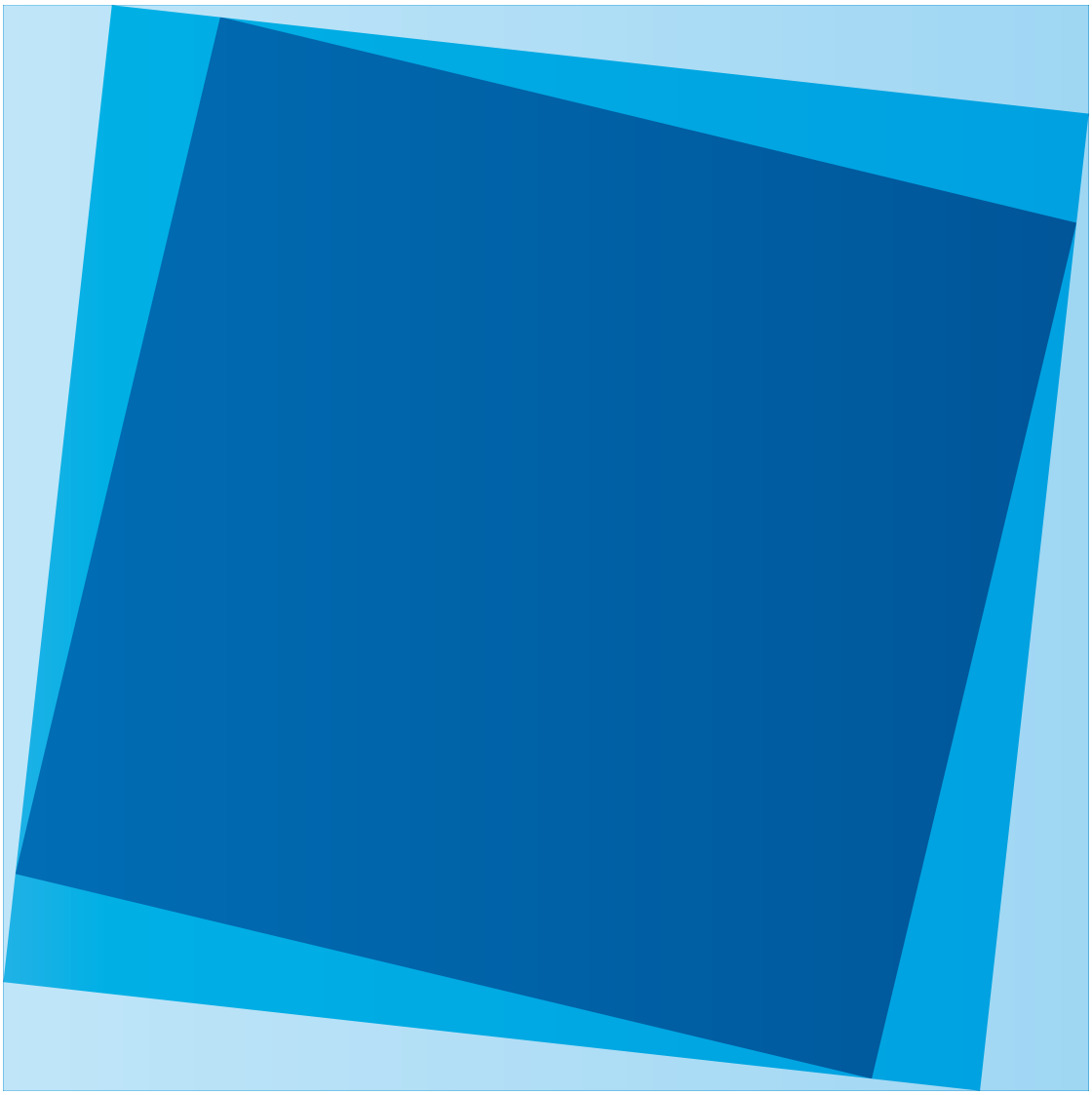
¿Hacia una nueva Ilustración? Una década trascendente



Ciberseguridad: un modelo de cooperación

Amos N. Guiora

Amos N. Guiora
SJ Quinney College of Law,
University of Utah

Amos N. Guiora es profesor en la Facultad de Derecho de Quinney, de la Universidad de Utah. Enseña Derecho Penal y Perspectivas Globales sobre Antiterrorismo y Religión y Terrorismo. Incorpora un innovador método basado en situaciones posibles para abordar problemas y dilemas de seguridad nacional e internacional. Asimismo, es investigador asociado de la Universidad de Oxford en el Instituto Oxford de Ética, Derecho y Conflictos Armados; investigador del Instituto Internacional Antiterrorismo del Centro Interdisciplinario en Herzliya, Israel; miembro de la escuela holandesa de Investigación sobre Derechos Humanos de la Facultad de Derecho de Utrecht y asesor en la Alianza por una Uta mejor. Ha publicado numerosos libros en Estados Unidos y Europa. Entre sus últimos títulos figuran: *Cybersecurity: Geopolitics, Law, and Policy* (Londres, 2017); *The Crime of Complicity: The Bystander in the Holocaust* (Chicago, 2017; traducido al chino y al neerlandés, segunda edición en preparación) y *Earl Warren, Ernesto Miranda and Terrorism* (Nueva York, 2018). Ha participado durante muchos años en negociaciones a dos vías en el conflicto israelí-palestino con un enfoque basado en la priorización como herramienta analítica.

Libro recomendado: Shoemaker, Dan y Conklin, W. Arthur (2012): *Cybersecurity: The Essential Body Of Knowledge* [Ciberseguridad: lo que hay que saber], Boston, Cengage.

El grado de gravedad que atribuyamos a las ciberamenazas es cuestión de perspectiva, experiencia, interacción y concienciación. Verlas como una acción delictiva, un acto terrorista o un híbrido de ambas cosas constituye un importante objeto de debate. Resolver este dilema ayuda a definir nuestra percepción de los responsables de los ciberataques y a decidir el castigo que merecen sus actos. Es una cuestión que atañe a la policía, los fiscales, los abogados defensores y la judicatura. Mi enfoque, como sugiere el título, se centra en la cooperación en ciberseguridad con objeto de minimizar el impacto de un ataque. La cooperación, como se verá, suscita reticencias en varios ámbitos. En algunos casos son legítimas y deben abordarse y recibir una respuesta convincente. El objeto del modelo de cooperación es ofrecer mecanismos institucionales para prevenir o, al menos, minimizar el daño que trae consigo la mera amenaza de un ciberataque y, por supuesto, un ataque real.

Que la ciberamenaza existe es hoy algo aceptado. El grado de gravedad que le atribuimos depende del punto de vista, la experiencia, las interacciones y el nivel de sensibilización de cada uno. Un punto importante a abordar es si la consideramos un acto delictivo, un acto terrorista o un híbrido entre ambas cosas.

Resolver esta cuestión ayuda a definir qué condición atribuimos a los responsables de los ciberataques y decidir el correspondiente castigo por sus actos. Es una cuestión que atañe a los cuerpos policiales, los fiscales, los abogados defensores y la judicatura, pero que también da pie a consideraciones morales en el contexto de la responsabilidad y la rendición de cuentas.

Otra realidad histórica a tener en cuenta es la falta de cooperación entre comunidades diferenciadas pero interconectadas que podrían beneficiarse mucho de unirse ante una amenaza grave. En este sentido, algunos objetivos potenciales de los ciberataques tienen el firme interés y la capacidad de minimizar la amenaza. Sin embargo, el análisis retrospectivo de cómo no llegan a unir fuerzas plantea un panorama desconcertante; un panorama que, en pocas palabras, refleja una falta de voluntad, derivada de múltiples razones, de reconocer las ventajas de una respuesta unificada ante los ciberataques.

Esta reticencia o vacilación no es una novedad de 2018, como dejan más que claro mis investigaciones anteriores en otros proyectos sobre ciberseguridad. Es decir, la falta de cooperación constatada en 2018 no es un fenómeno reciente, ni mucho menos. Una revisión de los datos, la literatura y la evidencia casuística pone de relieve, de un modo convincente, la aunsencia de cooperación institucionalizada (a falta de un término mejor). En cuanto a las diferentes razones del éxito de los ciberdelincuentes, su execrable impacto se ve intensificado por la incapacidad sistemática de sus blancos potenciales de reconocer las ventajas de adoptar un modelo cooperativo. Dados los esfuerzos persistentes, resueltos e incansables de los responsables del ciberterrorismo o los ciberataques, no adoptar por sistema un modelo de cooperación es tan destacable como preocupante.

Es destacable porque refleja un patrón coherente, y preocupante porque facilita el daño continuado a la sociedad (definida en términos amplios). Dicho patrón histórico explica, en parte, el éxito de los ciberataques. Refleja asimismo la incapacidad de desarrollar plenamente medidas defensivas que puedan aliviar, cuando no minimizar, el daño causado por los ciberataques. El análisis de las páginas siguientes se articula alrededor de dos realidades paralelas: (a) el análisis histórico de los problemas de ciberseguridad pone de relieve las consecuencias de la falta de cooperación; y (b) el desarrollo y la implantación de modelos de cooperación constituyen una medida positiva y muy necesaria para responder con más eficacia a una amenaza evidente.

La contextualización de un problema es importante para determinar qué recursos se dedican a contrarrestar, mitigar y minimizar las amenazas. De un modo similar, para concretar las medidas operativas aplicables contra el autor o los autores responsables de un ataque concreto es importante decidir resolver el dilema terrorismo-delito penal-híbrido. En todo caso, por importante que sea este debate, no será el que ocupe al presente capítulo, cuyo tema principal es, como indica el título, la cooperación en ciberseguridad con el fin de minimizar el impacto de los ataques. Como veremos, la cooperación suscita reticencias en varios ámbitos; reticencias que, en algunos casos, son legítimas y que deben abordarse y recibir una respuesta convincente.

Todo análisis de la ciberseguridad requiere una definición del término. Como suele ocurrir en estos casos, las mentes razonables pueden discrepar razonablemente; la discrepancia es una realidad y es comprensible.

Definimos ciberataques como «el uso deliberado y perverso de la tecnología con el propósito de dañar a las personas, las comunidades, las instituciones y los gobiernos». Pese a que esta propuesta de definición puede ser objeto de desacuerdo, se parte de la base de que sí hay amplio consenso respecto a lo que constituye «daño», con independencia de que un ataque haya tenido o no éxito.

Para que una acción en el ciberespacio sea eficaz, no es necesario ni que sea un ataque ni que tenga éxito. Dada la omnipresencia del ciberespacio, el mero temor a un ataque de este tipo nos hace dedicar, individual y colectivamente, una cantidad significativa de recursos, tiempo y energía a minimizar su impacto potencial. De forma muy parecida a la política antiterrorista, se destinan medidas importantes tanto a la prevención de un ataque como, cuando ocurre uno, a responder a su impacto y consecuencias. Se nos plantean las preguntas siguientes: ¿Cuál es la mejor manera de protegernos? ¿Ya la estamos poniendo en práctica? ¿Existen mecanismos más eficaces y creativos? Podemos dar por hecho que son las mismas preguntas que, a la inversa, se plantean aquellos que se dedican a dañar deliberadamente a la sociedad civil (definida en términos generales o particulares). Es así, con independencia del paradigma que asignemos al ciberespacio. Como ya hemos subrayado, no se puede minimizar la importancia de definir y categorizar las acciones en el ciberespacio. Sin embargo, por mucha importancia que tenga y por poca que se le pueda negar, el presente capítulo se centrará en un aspecto diferente.

Nuestro objeto de análisis se resume en la cooperación entre diferentes objetivos potenciales de ataques y entre distintos organismos policiales, así como entre objetivos y organismos policiales. Sostenemos, en pocas palabras, que implantando modelos de cooperación destinados a ofrecer mecanismos institucionalizados se puede evitar o, por lo menos, minimizar el daño que representa la mera amenaza de un ciberataque o, más aún, un ataque que tenga éxito. Dadas las consecuencias de un ataque y los recursos necesarios para reducir al mínimo su impacto, el modelo de cooperación propuesto tiene el objetivo de reducir los costes, tanto directos como indirectos, de las acciones en el ciberespacio. El modelo se fundamenta en una premisa: prevenir un ataque o, en el peor de los casos, llevar a cabo un esfuerzo concertado y decidido es preferible a asumir los costes de un ataque exitoso.

Implantando modelos de cooperación destinados a ofrecer mecanismos institucionalizados se puede evitar o, por lo menos, minimizar el daño que representa la mera amenaza de un ciberataque o, más aún, un ataque que tenga éxito

Sé que hay grandes empresas que suscriben el argumento opuesto: es más rentable absorber un ataque que invertir en modelos de protección avanzados. Sin embargo no he conocido a directivos cuyas empresas hayan sido objeto de ataques exitosos y que se adhieran a dicha teoría.[1] Para mí, esta lógica refleja un pensamiento a corto plazo centrado en consideraciones económicas muy restringidas e indica una falta de conocimiento de las ventajas de una protección proactiva y de modelos de cooperación. Dichas personas también manifestaron sus inquietudes sobre la imagen pública, el nerviosismo de los consumidores y la ventajas que podría otorgar a la competencia. Desde una perspectiva estrictamente empresarial, este enfoque quizá es comprensible: era un argumento racional, no el producto de la impulsividad o la precipitación. Asimismo, las interacciones con mis interlocutores dejaban claro que consideraban que su enfoque correspondía a las prácticas de las mejores empresas.

Por tanto, no podemos descartarlo de un plumazo. No obstante, el enfoque refleja criterios tácticos limitados, de orientación interna y que no llegan a analizar el panorama general y las posibles ventajas a obtener. Aunque a los citados directivos se les presentó el intercambio de información para minimizar los daños como algo positivo, su perspectiva, centrada en aspectos internos, los conducía a percibir dicho intercambio como algo negativo, con un impacto notable en el producto y posición de la empresa.

Debemos añadir que los agentes de las fuerzas de la ley tenían una percepción positiva del modelo de cooperación como algo que los ayudaría en su labor, con una salvedad: una reticencia claramente manifestada de los agentes policiales federales a intercambiar información con sus homólogos estatales y locales. No queda claro si esta reticencia está institucionalizada o si se limita a determinadas personas; el análisis de esta cuestión no arrojó luz en un sentido u otro.

En el presente capítulo espero convencer a los lectores de la cortedad de miras de un enfoque como ese y subrayar las ventajas del modelo de cooperación que propongo. La pregunta es la siguiente: ¿Cuál es el modo más eficaz de mejorar la ciberseguridad?

Para convencer al lector de la viabilidad de una propuesta así, hay que analizar los costes de las acciones en el ciberespacio, tanto en forma de amenaza como de ataque. Es decir, debe atribuirse una ventaja a la adopción de un modelo de cooperación, de modo que el beneficio supere a los costes esperados; en caso contrario, la propuesta sería inviable desde el principio. De un modo similar, se deben disipar las dudas derivadas de considerar que la cooperación no es un «objetivo en sí misma», según las cuales la cooperación acaba teniendo consecuencias dañinas e involuntarias que reducen su valor.

La premisa de trabajo, como desarrollo más adelante, es que la cooperación es positiva, que así se debe considerar y que hay que desarrollar modelos para implantarla con éxito. No será tarea fácil, como ya me dejaron claro durante la redacción de mi libro *Cybersecurity: Geopolitics, Law, and Policy* [Ciberseguridad: Geopolítica, Ley y Regulación],[2] y confirmé cuando organicé un ejercicio de simulación.[3] Pese a los argumentos planteados (algunos comprensibles, otros que podrían caracterizarse como «difíciles de entender»), considero que el modelo de cooperación propuesto merece una atención detenida en un contexto caracterizado por ciberataques incesantes. Como suele decirse, «la mejor defensa es un buen ataque».

El análisis se dividirá en los cinco apartados siguientes: «Qué significa “cooperación”»; «Cooperación entre quiénes»; «Cooperación hasta qué punto»; «El bueno, el feo y el malo de la cooperación», y «Reflexiones finales».

Qué significa «cooperación»

El término «cooperación» tiene muchos significados y definiciones. El contexto, la época, la cultura y las circunstancias desempeñan un papel importante tanto en la definición del término como en su puesta en práctica real. La cooperación puede ser permanente, transitoria o situacional; se puede fundamentar en mecanismos formales y también en concepciones informales. La cooperación, ya sea bilateral o multilateral, alcanza su plenitud cuando las partes consideran que este tipo de relación les beneficia mutuamente.

Eso no significa que un mecanismo de este tipo, sea formal o informal, esté exento de costes. No lo está. Lo que es cierto es que en cualquier acuerdo vinculante se renuncia voluntariamente a determinadas «libertades» a cambio de un beneficio percibido. Basta con recordar las obras de Hobbes, Locke o Rousseau para reconocer los costes y beneficios de crear una comunidad y unirse a ella.[4]

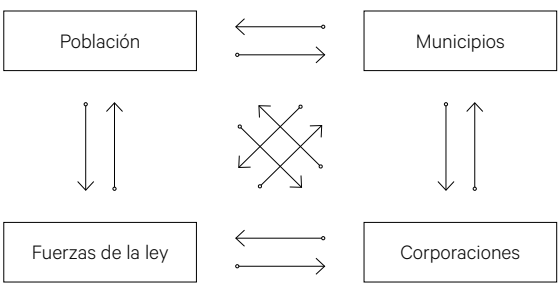
Esa es la esencia de la cooperación. Al entrar en una comunidad y cooperar con sus miembros, buscamos seguridad, estabilidad y protección, aspectos que se suelen percibir como positivos. A cambio, renunciamos al individualismo, a un cierto grado de libre albedrío y a parte de nuestra independencia. Para algunos, se trata de un coste inaceptable, no compensado por las ventajas derivadas de los aspectos positivos de la cooperación. Es razonable.

No obstante, la historia nos enseña que, por lo general, los beneficios de la cooperación superan a los costes percibidos o reales, aunque sin duda hay excepciones. Sin embargo, el concepto de «unir fuerzas» en una empresa o propósito común se suele considerar preferible a «intentarlo solo». Para facilitar o, incluso, mejorar la eficacia, un acuerdo de cooperación debe incluir:

1. Consenso acerca de los objetivos comunes.
2. Mecanismos para evaluar continuadamente los costes y beneficios.
3. Mecanismos para abandonar el acuerdo.
4. Unos parámetros para el acuerdo.
5. Unos mecanismos acordados de aplicación del acuerdo.

Huelga decir que el predicado subyacente es que las partes alcanzan el acuerdo voluntariamente reconocen la necesidad de este y admiten que la alternativa no es deseable. A medida que avanzamos en el análisis, estos principios sirven de base para nuestra recomendación de convertir la cooperación en un aspecto esencial de la minimización de las amenazas que plantean los ciberataques, con independencia de que sean considerados un delito, un acto de terrorismo o un híbrido entre los dos.

Para dar cuerpo a la presente propuesta, el modelo de cooperación que recomiendo beneficiaría tanto a las entidades privadas como a las públicas. De un modo similar, obligaría a las corporaciones que han sufrido un hackeo a institucionalizar unos mecanismos de notificación tanto a los organismos policiales como a sus clientes. Los vectores cruzados entre la población (en términos generales), los municipios, la policía y las corporaciones (coticen o no en el mercado de valores).



Esta complejidad refleja la multiplicidad tanto de las amenazas como de los objetivos vulnerables. Somos conscientes de que la puesta en práctica de la presente recomendación resulta contraria a la lógica para muchas de las partes interesadas, como las corporaciones (lo que no nos puede sorprender) y las fuerzas de la ley (lo que sí es sorprendente). En todo caso, el enfoque de dicha cooperación como un modelo de seguridad colectiva combinado con una componente de legítima autodefensa (en ambos casos derivados del derecho internacional) fue acogido con escepticismo.

La resistencia de las corporaciones reflejaba la preocupación por una potencial pérdida de ingresos y otras consecuencias involuntarias, en forma de ventajas para la competencia. Por otra parte, la reticencia de las fuerzas de la ley partía de dos lógicas diferentes: la falta de voluntad de los agentes policiales federales de cooperar con los agentes locales y la escasez de recursos para hacer frente a los ciberataques. La primera lógica no tiene salida, mientras que la segunda requiere admitir que la cibercriminalidad requiere una dotación de recursos suficiente para que la policía sea un colaborador más eficaz a la hora de minimizar la amenaza que plantean los malhechores (más adelante analizaremos la Ley de Intercambio de Información en Ciberseguridad o Cybersecurity Information Sharing Act, de 2015).

¿Cómo lograr el modelo corporativo? Existen varias alternativas y opciones, que en algunos casos representan medidas voluntarias y en otros son fruto de la imposición legislativa. En un mundo ideal imperaría la voluntariedad, pero, como quedó claro en numerosas conversaciones, se trata de un desenlace poco probable. De ahí la propuesta de modelos cooperativos por mandato legislativo que impongan un deber a los objetivos potenciales de ciberataques (la lista de objetivos potenciales se expone en el siguiente apartado 2).

Cabe una advertencia: sumar la intervención del Congreso de Estados Unidos a los requisitos existentes suscita grandes recelos, sobre todo en el sector privado. Asimismo genera preocupaciones de raíz ideológica, en especial entre los detractores acérrimos de la intervención del Estado, que rechazan con vehemencia este tipo de medidas. Ambos antagonismos constituyen obstáculos legítimos y poderosos para el avance de una legislación en la materia. Su poder se magnifica mediante la realidad de la política; en especial, en el contexto de polarización que caracteriza ahora mismo a Estados Unidos.

El deber de notificar, como ilustra la Ley Sarbanes-Oxley de 2002,[5] es la bestia negra de muchos líderes corporativos. Un directivo dijo que la legislación era fuente de cargas, costes y obligaciones engorrosas para las empresas. En su opinión, en su equipo había más directivos dedicados a supervisar el cumplimiento de la ley que responsables de producción.

Sin duda, ello impone costes indeseados y, en ocasiones, injustificados. Sin embargo, los riesgos y amenazas que representan los ciberataques justifican la búsqueda de mecanismos que impongan la cooperación. Esto es, si la cooperación voluntaria no es posible, se debe ampliar el debate a la posibilidad de que la cooperación sea obligatoria.

La Ley de Intercambio de Información sobre Ciberseguridad (S. 754), presentada por Richard Burr, senador republicano por Carolina del Norte, y promulgada por el presidente Obama, el 18 de diciembre de 2015, era una medida importante porque «autoriza el intercambio de información sobre ciberseguridad entre el sector privado, los gobiernos estatales, locales, tribales y territoriales, y el gobierno federal».[6] Esta ley tiene cuatro objetivos importantes:

> — Requiere al gobierno federal que publique periódicamente un documento de buenas prácticas. De este modo las entidades podrán utilizar las buenas prácticas para defender mejor su infraestructura cibernética.
> — Identifica los usos de indicadores de ciberamenaza y las medidas defensivas permitidas al gobierno federal, al tiempo que restringe la revelación, retención y uso de la información.
> — Autoriza a las entidades a intercambiar indicadores de ciberamenaza y medidas defensivas, entre sí y con el Departamento de Seguridad Nacional, con la consiguiente protección ante riesgos legales.
> — Protege la información identificable personalmente (IIP), al exigir a las entidades que retiren toda la IIP de la información transmitida al gobierno federal. Estipula que cualquier organismo federal que reciba ciberinformación que contenga IIP debe proteger la IIP de toda difusión o uso no autorizado. El fiscal general de Estados Unidos y el secretario del Departamento de Seguridad Nacional publicarán unas directrices para ayudar a cumplir este requisito.[7]

En el mismo sentido, el 6 de julio de 2016, el Parlamento Europeo adoptó la Directiva relativa a las redes y sistemas de información (Directiva RSI), que proporciona medidas legales para mejorar el nivel general de ciberseguridad en la UE, al garantizar:

> — La preparación de los Estados miembros, al exigirles unos dispositivos apropiados al respecto; por ejemplo, una red de equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) y una autoridad nacional competente en redes y sistemas de información (RSI).
> — La cooperación entre todos los Estados miembros mediante la creación de un grupo de cooperación a fin de respaldar y facilitar la cooperación estratégica y el intercambio de información. También deberán crear una Red de CSIRT, con el objetivo de promover una cooperación operacional rápida y eficaz ante incidentes de ciberseguridad específicos e intercambiar información sobre riesgos.
> — Una cultura de la seguridad en diferentes sectores que resultan vitales para nuestra economía y sociedad y, por añadidura, dependen en gran medida de las tecnologías de la información y la comunicación (TIC), como la energía, el transporte, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad y la infraestructura digital. Las empresas de dichos sectores que sean identificadas por los Estados miembro como operadoras de servicios esenciales deberán adoptar las medidas de seguridad adecuadas y notificar los incidentes graves a la autoridad nacional correspondiente. Asimismo, los proveedores de servicios digitales clave (motores de búsqueda, servicios informáticos en la nube y mercados en línea) deberán cumplir los requisitos de seguridad y notificación de la nueva Directiva.[8]

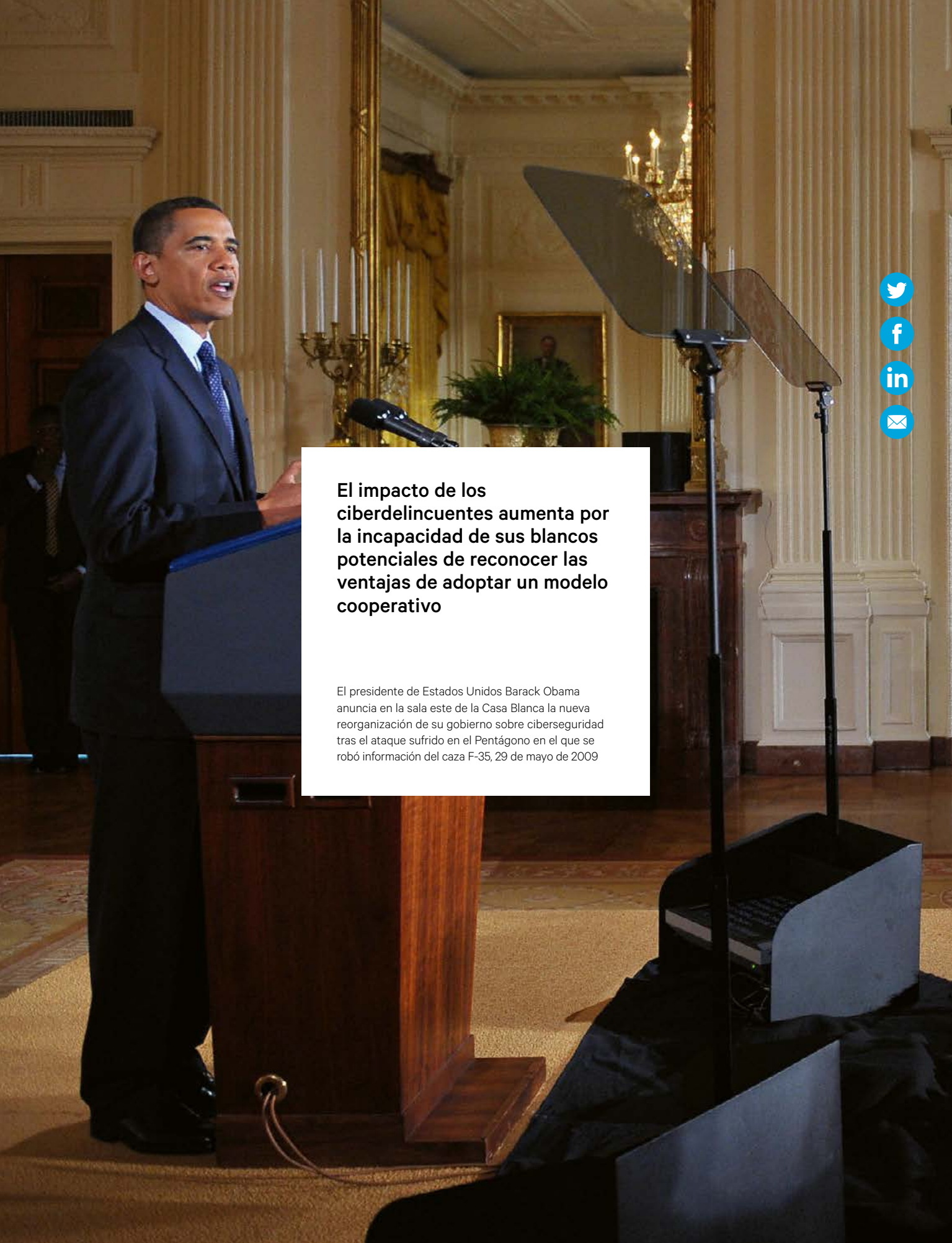
La clave está en basarse en estas dos importantes medidas e incrementar los niveles de cooperación entre diferentes comunidades, creando así una infraestructura que minimice con la máxima eficacia las posibles consecuencias de un ciberataque. Para conseguirlo, es necesario integrar sectores, vectores y grupos de interés; y, para lograrlo con mayor solvencia, hay que reconocer que las medidas de cooperación existentes, por bienintencionadas que sean, se quedan cortas. El «porqué» nos lo dejaron claro; el desafío, a medida que avanzamos en este debate, radica en determinar qué cooperación, entre quiénes, es la que se debe institucionalizar con mayor efectividad.[9]

El apartado siguiente se centra en esta cuestión.

Cooperación entre quiénes

En el reino de la ciberseguridad, los blancos de los ciberataques (con independencia de que lleguen o no a sufrirlos) pueden ser (de lo general a lo específico, sin afán de exhaustividad):

1. Personas como objeto de un robo de identidad.[10]
2. Personas cuya intimidad está en peligro cuando, por ejemplo, los centros sanitarios sufren un hackeo.
3. Empresas (de todos los tamaños) cuyos datos se ven comprometidos.
4. El sector financiero, incluidos los bancos, las empresas de inversión y los mercados de valores.
5. Municipios cuyas infraestructuras (por ejemplo, la señalización de tráfico y los sistemas de agua) se ven amenazadas.
6. Hospitales, cuando se pone en peligro el bienestar de los pacientes y la seguridad y protección de las historias médicas.



El impacto de los ciberdelincuentes aumenta por la incapacidad de sus blancos potenciales de reconocer las ventajas de adoptar un modelo cooperativo

El presidente de Estados Unidos Barack Obama anuncia en la sala este de la Casa Blanca la nueva reorganización de su gobierno sobre ciberseguridad tras el ataque sufrido en el Pentágono en el que se robó información del caza F-35, 29 de mayo de 2009

El 6 de julio de 2016 el Parlamento Europeo adoptó la Directiva RSI que proporciona medidas legales para mejorar el nivel general de ciberseguridad en la UE

Cables de fibra óptica y de cobre de Ethernet. El Departamento de Cultura, Comunicación y Deportes junto al Ministerio del Interior británico trabajan en un libro blanco que obligue a los gigantes tecnológicos a revelar cómo gestionan el material ofensivo e ilegal que publican sus usuarios

7. Las fuerzas armadas, al resultar amenazados los sistemas de armamento.
8. Las líneas aéreas y los sistemas de control del tráfico aéreo.
9. Los organismos y oficinas gubernamentales.

Esta lista, pese a que no es exhaustiva, basta para mostrar la amplitud del abanico de objetivos potenciales de un ciberataque. Pone el acento en el número significativo de personas, instituciones, corporaciones e infraestructuras críticas que corren peligro. El concepto de «peligro» es esencial en el debate sobre la cooperación: a falta de un peligro potencial, el impulso para llegar a un acuerdo se debilita significativamente, cuando no se desvanece por completo.[11]

No obstante, en realidad la ciberseguridad es un mundo de amenazas claras pero desconocidas, ocultas e indistinguibles hasta que se produce el verdadero ataque. La ciberamenaza se debe formular en términos de «cuándo se producirá un ataque», y no «si se produce un ataque».

La lista anterior refleja el amplio abanico de objetivos potenciales de un ataque, además de poner de manifiesto el alcance de su impacto en términos de víctimas secundarias. También subraya la importante cuestión de «ante quién hay que rendir cuentas». La cooperación no se puede considerar algo «que está bien», sino un medio necesario para proteger a las víctimas, tanto deliberadas como accidentales, de un ciberataque. Para señalar lo que es obvio: el número de personas afectadas por el hackeo de cualquiera de las entidades enumeradas antes es asombroso. No solo tiene un coste económico extraordinario, también paraliza el municipio, afecta al hospital, pone en peligro a los viajeros aéreos y tiene consecuencias abrumadoras para las personas que requieren de los servicios públicos. Por sí solo, esto justifica la cooperación entre las partes implicadas.

Lo que propongo es que consideremos la presente propuesta desde la óptica, por extrapolación, del derecho internacional. De este modo podremos analizar la cooperación en cuanto autodefensa, pero también como iniciativa de seguridad colectiva. En el contexto de la cooperación entre las víctimas potenciales de un ciberataque, esta dualidad proporciona un marco intelectual y, en ocasiones, también práctico. Pone de relieve dos realidades importantes: la necesidad de autodefensa y el reconocimiento de que unir fuerzas constituye un medio eficaz de mejorar la protección.[12]

La cooperación o seguridad mutua no implica un acuerdo sobre todas las cuestiones ni indica una confluencia perfecta de intereses, valores y objetivos. Sin embargo sí refleja el reconocimiento de que determinadas amenazas, a tenor de sus posibles consecuencias, justifican la búsqueda de una postura común aun cuando las partes tengan intereses contrapuestos. Los dos principios (autodefensa y seguridad colectiva) se pueden considerar complementarios. Por una parte, la acción individual está justificada; por otra, se reconoce que determinados casos requieren de cooperación para facilitar la protección.

El artículo 51 de la Carta de las Naciones Unidas establece que:

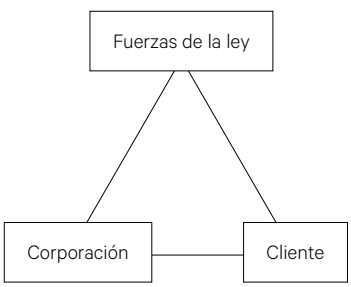
> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, en tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales.[13]

Según el artículo 5 del Tratado de la Organización del Tratado del Atlántico Norte (OTAN):

> Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales.[14]

Aplicados a la cibernética, los dos principios reflejan un enfoque integrado que nos permite responder al que debería ser el interés principal de los objetivos potenciales de un ciberataque: evitarlo, si es posible, o, en caso de ataque consumado, minimizar su impacto. Desde el punto de vista de la víctima potencial (por ejemplo, el cliente de una gran empresa financiera), un enfoque de este tipo reflejaría reconocer el deber de proteger y la aplicación de las consiguientes medidas. De un modo bastante análogo, los gobiernos tienen la obligación de proteger a su población civil.

En el combate contra el ciberterrorismo, la concepción del «cliente como colaborador» —en virtud de la cual se crea una relación triangular entre la empresa, el cliente y las fuerzas de la ley— es mucho más eficaz que la minimización innecesaria o la misma negación de la amenaza.



Para una empresa, resulta más barato responder a un hackeo o gestionar sus consecuencias que invertir en sistemas de defensa y protección.[15] El número de empresas que, tras un hackeo (consumado o no) se sinceran inmediatamente y admiten «nos han hackeado, somos vulnerables y debemos aprender de ello» es mínimo. Es una oportunidad perdida tanto para la empresa como para otras partes interesadas, al tiempo que representa una doble victoria para los piratas informáticos:[16] la intrusión ha tenido éxito y las empresas son incapaces de aprender las unas de las otras. Pese a que las diferentes compañías tienen intereses que proteger, las similitudes y los valores comunes que las unen justificarían que aceptaran y facilitaran el intercambio de información frente a una intrusión o un intento de intrusión. Pero lo cierto es que la mayoría de las empresas son muy reticentes a dar un paso adelante y reconocer que han sufrido un hackeo. En ese sentido, no son francas con sus clientes, sus accionistas o las fuerzas del orden público. Además, impiden o evitan que otras empresas se protejan. Tal vez les avergüenza ser vulnerables pese al enorme gasto en cortafuegos y equipos de TI (tecnologías de la información). Sin embargo, dado el carácter malintencionado de los

ciberagresores y el daño causado, las empresas deberían dejar de lado la vergüenza y ser mucho más transparentes.

Para tal fin, es recomendable definir la falta de transmisión de información como un acto delictivo. El marco establecido por la Ley de Intercambio de Información en Ciberseguridad ofrece un punto de partida para hacerlo. A continuación se articulan las razones de esta recomendación:

— *Teniendo en cuenta a los clientes*

Como cliente de una empresa que ha sido hackeada, usted desea saber *de inmediato* si su intimidad está en peligro. Tiene el derecho a saber que «alguien a quien no autorizó» tiene acceso a su número de la seguridad social, su información sanitaria y otros datos de carácter muy personal. Las empresas deben tener la *obligación* inmediata de notificar a sus clientes.

— *Teniendo en cuenta a los accionistas*

Para los accionistas hay en juego intereses económicos considerables. Dicho esto, existen factores económicos importantes a tener en cuenta a la hora de determinar cuándo y cómo informar a los accionistas de un ciberataque, haya tenido o no éxito. Claramente, las corporaciones sopesan con cuidado el impacto de una respuesta negativa, pero, en cualquier caso, deben asumir la responsabilidad absoluta de ofrecer a sus accionistas la máxima información y de un modo inmediato.

— *Teniendo en cuenta a las fuerzas de la ley*

Cuanto menos se tarde en transmitir a las fuerzas de la ley la información de un ciberataque, con mayor eficacia podrán iniciar el proceso de identificar al responsable. A primera vista, a la empresa agredida le interesa ayudar a la policía. No obstante, los reiterados retrasos en la transmisión de información indican la existencia de un conflicto al respecto, pese a las ostensibles ventajas que se derivarían de una notificación y una transmisión de información inmediatas.

Con vistas a un proceso de notificación institucionalizado, el apartado siguiente se centra en la mejora de la cooperación entre partes afectadas por un ciberataque contra una empresa.

¿Cooperación hasta qué punto?

La complejidad de esta cuestión queda patente en un comentario y una respuesta del ejercicio mencionado en la introducción. El diálogo se puede resumir del modo siguiente:[17]

—Amos N. Guiora (ANG): ¿Cuándo informa a sus clientes de que le han hackeado, con la consiguiente potencial violación de su intimidad?

—CEO: Solo cuando el problema está resuelto; nunca mientras estamos enfrentándonos al posible hackeo.

—Participante: Me gustaría saberlo tan pronto como ustedes (la empresa); de este modo podría tomar medidas para protegerme.

—CEO: Me centraré en resolver el problema antes que en informar a los clientes.

—Cliente: ¿Y eso significa que no me permitirán proteger mi intimidad, aunque consideren que puede estar en peligro?

—CEO: Así es.

—ANG: ¿Informaría usted a la competencia (del mismo sector) de que su empresa ha sido hackeada?

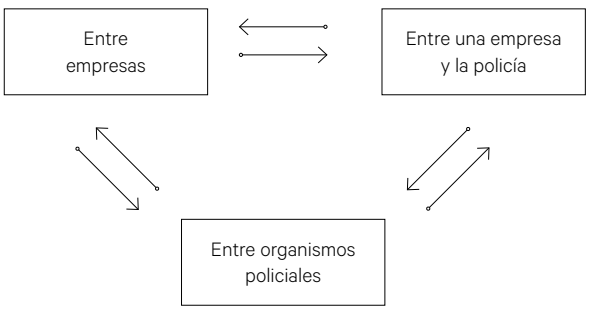
—CEO: No.

—ANG: ¿Por qué?

—CEO: Lo usarían en su propio beneficio, de modo que debilitarían mi posición financiera.
—ANG: ¿Informaría a las fuerzas de la ley, ya fueran locales o nacionales?
—CEO: No sería una prioridad.

Me impresionó el CEO por su franqueza; además, quedaba claro que el ciberprotocolo de su empresa era avanzado y fruto de mucha reflexión y conocimiento. Pero también me asombró la falta de voluntad (bien argumentada) de cooperar con tres actores diferenciados: los clientes, la competencia y las autoridades policiales. Sus respuestas reflejaban un enfoque de «hacer las cosas solos». Esta sensación se acrecentó cuando un participante me explicó lo siguiente: un director de seguridad de la información afirmó que durante un ataque solo compartiría información con aquellas entidades empresariales que conociera y en las que confiara personalmente.

A menudo se alude a los motivos corporativos, los intereses financieros, la competencia y los secretos industriales como razones de este enfoque. Por otra parte, el pensamiento estratégico a largo plazo indica que es esencial adoptar una perspectiva distinta para contrarrestar con éxito los ciberataques. Este enfoque más estratégico y a largo plazo se fundamenta sobre todo en el reconocimiento de un «enemigo común» y de que «aunar fuerzas» mejorará notablemente el desarrollo de contramedidas más eficaces. El modelo de cooperación propone la colaboración entre empresas, y entre estas y fuerzas policiales.



La interacción con agentes de policía puso de relieve la falta de cooperación en materia de ciberseguridad y en tres ámbitos distintos: entre una empresa y otra, entre una empresa y la policía, y entre distintos organismos policiales.

¿Qué deberían hacer las empresas al descubrir que ha habido una intromisión?:

— Efectuar una evaluación sincera del «daño causado».
— Tomar todas las medidas posibles para proteger los datos existentes.
— Informar a los clientes lo antes posible.
— Informar de inmediato a las autoridades policiales y colaborar estrechamente con estas para minimizar los daños.
— Informar al público.
— Cooperar con otras empresas, con el objetivo tanto de minimizar los daños internos como de evitar ataques futuros.

Adoptar estas medidas requiere sofisticación, trabajo en equipo y la capacidad y voluntad de analizar las vulnerabilidades internas, lo cual exige, a su vez, contar con las herramientas necesarias y también con un equipo humano competente. La voluntad, por importante

que sea, debe ir acompañada de unas determinadas destrezas. La capacidad de reacción inmediata, que exige la integración del trabajo en equipo, la competencia y buena disposición, minimiza daños futuros. No obstante, lo primero que se desprende del análisis de cómo reaccionan las empresas ante un hackeo es la falta de una respuesta rápida. Queda por saber si es deliberada o no. En todo caso, demuestra las dificultades que entrañan tanto la incapacidad para identificar rápidamente la intromisión como la no transmisión de información al cliente. Uno de los lectores de un borrador anterior comentó ambos problemas (las dificultades y la información al cliente) y manifestó lo siguiente:

> En la actualidad nos enfrentamos a amenazas de piratas informáticos decididos y con talento, muy capaces y motivados y que cuentan con el tiempo y el apoyo de Estados nación para ejercer su oficio (el hackeo) contra un blanco determinado. Sí, puede haber dado la impresión de que algunas empresas no se tomaban este asunto con seriedad, pero ello se debe en parte a cómo se dan las noticias. En las noticias no se habla de cómo una empresa gestiona sus cambios internos, sus problemas de vulnerabilidad o sus recursos (los equipos informáticos físicos y los programas) o los procesos de seguridad en las TI, por ejemplo [...] estas entidades constituyen unidades separadas o compartimentalizadas que deben unirse para responder a un hackeo. Además, tras algunos hackeos recientes, los responsables de la amenaza ocultan sus actividades para evitar ser detectados. Se adelantan a cualquier sistema que alerte de su actividad; superan con creces la protección antivirus porque simulan ser un usuario normal de la red, de modo que a veces pasan desapercibidos para la protección antivirus.
>
> En cuanto a informar o no a un cliente mientras la investigación está en curso es un arma de doble filo. Hasta que se determine el alcance del peligro, informar a los clientes puede entorpecer la investigación; en especial, si quieres ver si el pirata informático todavía está activo en el sistema, que es una manera de atraparlo. Además, la empresa debe determinar antes hasta qué punto se han visto expuestos sus clientes. Como hemos visto con Equifax (que sufrió una violación de datos en 2017), tuvo que informar al público una y otra vez con más detalles sobre el hackeo.[18]

En cuanto a los requisitos normativos sobre el sector financiero, en la actualidad se está decidiendo cuánto se puede esperar antes de informar al público de un hackeo y si se «debería» notificar a los clientes antes que a la prensa o la población. Las consecuencias son significativas: prolongación de la vulnerabilidad; prolongación de la amenaza contra los clientes; responsabilidad civil potencial en el contexto de una protección insuficiente de la información o la privacidad del cliente, y responsabilidad por no notificar al cliente de la vulneración y de sus consecuencias.

Pese a que es comprensible que la atención se centre en las posibles demandas judiciales, las cuestiones más importantes radican en las omisiones de protección y de información por razones claras:

— Los clientes potenciales serán reticentes a «hacer negocios con nosotros» cuando descubran la omisión de proteger o de informar.
— Los clientes existentes podrían irse a la competencia si llegan a la conclusión de que no se tomaron todas las medidas razonables para proteger su intimidad.
— La población en general tendrá una mala imagen de la empresa en cuanto a su incapacidad para eliminar los ciberataques y minimizar los ciberriesgos, aunque su crítica más potente será la relativa a la *omisión de la verdad*.

Por lo tanto, ¿qué significa esto para las empresas? Siendo escuetos, deben ser mucho más transparentes. En mi opinión, reconocer públicamente que ha sufrido un hackeo tiene beneficios claros para una empresa. Aunque justo después de notificar el ataque, el público se mostrará preocupado, la reacción más a largo plazo será de aprecio por haber «dicho la verdad».

Además, la información sobre cómo se produjeron la violación o intromisión podría evitar vulneraciones futuras a otras compañías. Este cambio de comportamiento puede tener un efecto considerable y positivo en millones de consumidores.

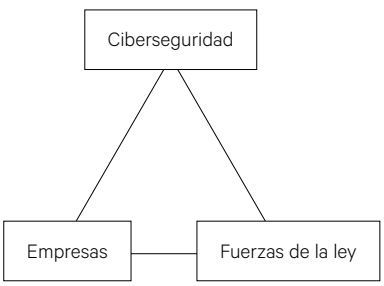
Revelar la verdad debe incluir los pasos siguientes:[19]

— Admisión de la intromisión.
— Una lista de medidas tomadas para afrontar de inmediato la intromisión con vistas a proteger a los clientes.
— Una lista de medidas para proteger a los clientes en un futuro.
— Contactar con otras empresas en el marco del «intercambio de información».
— Aplicación de contramedidas cibernéticas agresivas.

Este enfoque «abierto» entraña riesgos. Sin embargo, desde una perspectiva de coste-beneficio, las ventajas acaban por imponerse a las desventajas. Pese a que la transparencia y la sinceridad traen consigo vulnerabilidad, un enfoque que ponga el acento en la aplicación de medidas para evitar ataques futuros combinado con la sinceridad refleja: (1) una mayor protección de los clientes; (2) una mayor protección de las infraestructuras críticas, y (3) una mayor protección del «interés general».

La mayoría de las empresas son muy reticentes a dar un paso adelante y reconocer que han sufrido un hackeo. En ese sentido, no son francas con sus clientes, sus accionistas o las fuerzas del orden público

Mitigar riesgos mediante la sinceridad y la proactividad es beneficioso en todos los sentidos. Desde una perspectiva jurídica (porque minimiza el impacto potencial de las demandas civiles), una política de transparencia basada en el mensaje de «tomamos medidas para minimizar la exposición de la información personal, aprendemos de ello y trabajamos en estrecha colaboración con los clientes», reducirá la probabilidad de demandas judiciales contra las empresas. Un enfoque de este tipo transmite una voluntad por parte de la empresa de llegar a públicos diferentes; en particular a los clientes y a las autoridades policiales.



Para que las autoridades policiales puedan proteger a las empresas con eficacia es necesario un cambio fundamental en el contexto y el concepto de la cooperación. Una mayor eficacia policial en la protección de las empresas requerirá que estas sean más transparentes con los cuerpos policiales.

Sin embargo, un lector planteó la advertencia siguiente:

> ¿Cree que hay en los «cuerpos policiales» talento necesario en materia de cibernética para descubrir vulnerabilidades y cómo solucionarlas? ¿Cuáles podrían hacerlo? ¿Los locales, los estatales o los federales? Cuando la policía interviene se plantean los siguientes problemas: A la policía le interesa, sobre todo, encontrar al responsable del hackeo, mientras que la empresa quiere retomar su actividad empresarial; son prioridades contrapuestas. Una de las razones por las que no se alerta de inmediato a las autoridades es que la empresa quiere hacer su trabajo sin la distracción la intervención policial supone. Por otra parte, que sean policías no garantiza que dispongan del talento necesario en materia de ciberseguridad. Además, dependiendo de la empresa de que se trate, podría tener que interrumpir su actividad y sus servicios mientras dura la investigación.[20]

La cooperación ayudará a las fuerzas de la ley a comprender dónde se produjo el hackeo y dónde radicaba la vulnerabilidad de la empresa, además de contribuir a solucionarla. Sin embargo, para ello es necesario que las empresas sean mucho más transparentes. En este sentido, la pelota está en su tejado. La falta de una colaboración estrecha con los cuerpos policiales impide el desarrollo y, todavía peor, la aplicación de un modelo avanzado de cooperación entre el mundo empresarial y la policía. Y dadas las consecuencias de un ciberataque para la vulnerabilidad para las personas, urge adoptar enfoques diferentes de los actuales en lo referido a la aplicación de la ley.[21]

La cooperación ayudará a las fuerzas de la ley a comprender dónde se produjo el hackeo y dónde radicaba la vulnerabilidad de la empresa, además de contribuir a solucionarla

No obstante, la puesta en práctica de estos nuevos enfoques depende de la disposición de las compañías a considerar a los cuerpos policiales como colaboradores de pleno derecho, tanto en el plano preventivo como en el reactivo. A tal efecto, es necesario un modelo de gobernanza corporativa de la seguridad, todavía pendiente, cuyo desarrollo corresponde a las compañías mismas. Por otra parte, las autoridades policiales han manifestado repetidamente su disposición a colaborar en el desarrollo y la aplicación de dicho modelo, que pondría el acento en:[22]

— Identificar las amenazas.
— Minimizar las vulnerabilidades.
— Establecer prioridades en los recursos.
— Efectuar análisis coste-beneficio.
— Proteger los activos.
— Comprender mejor los puntos de vulnerabilidad.
— Minimizar el impacto de los ataques futuros.

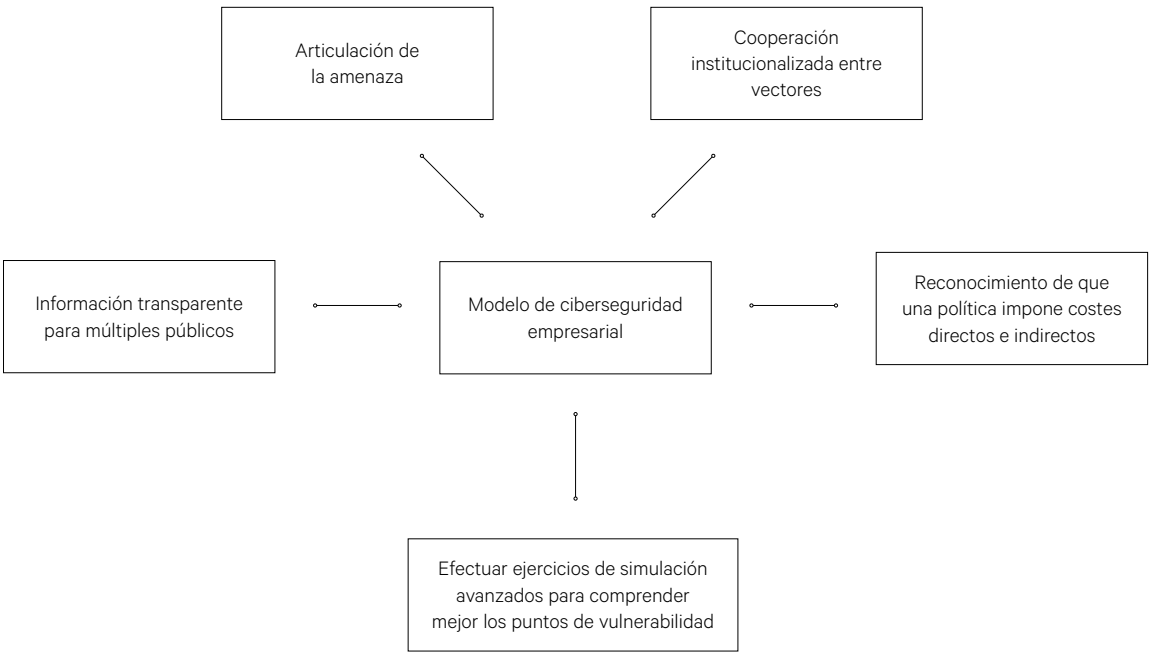
El ex consejero delegado de Equifax, Richard Smith, se prepara para declarar ante el Comité de Bancos, Vivienda y Asuntos Urbanos del Senado de Estados Unidos el 4 de octubre de 2017. Smith dimitió tras hacerse público que unos piratas informáticos habían atacado la firma de solvencia crediticia y se habían llevado información sobre casi 145 millones de estadounidenses

Por consiguiente, ¿qué deben hacer las empresas?

Los líderes corporativos pueden reunirse y debatir sin fin sobre sus puntos débiles, pero el mecanismo más eficaz para entender de verdad estos puntos es realizar ejercicios de simulación, ya sea interno o con expertos.

Recomiendo encarecidamente que los cuerpos policiales tengan un sitio en la mesa de reuniones con las corporaciones y otros representantes públicos. De lo contrario, el ejercicio se quedará en una mera cámara de resonancia, en gran medida ineficaz a la hora de concebir y aplicar una política de ciberseguridad. Soy muy consciente de que, para muchos dirigentes del mundo empresarial, la idea de una cooperación institucionalizada con los cuerpos policiales, las entidades del gobierno y otras compañías o competidores es alarmante[23] y lo respeto.

Sin embargo, dados el coste, el impacto y la perversión de los piratas informáticos, no atisbo otra alternativa que reformar el modelo de ciberseguridad empresarial.



A continuación planteo las preguntas a considerar para comprender la naturaleza y el alcance de la cooperación:[24]

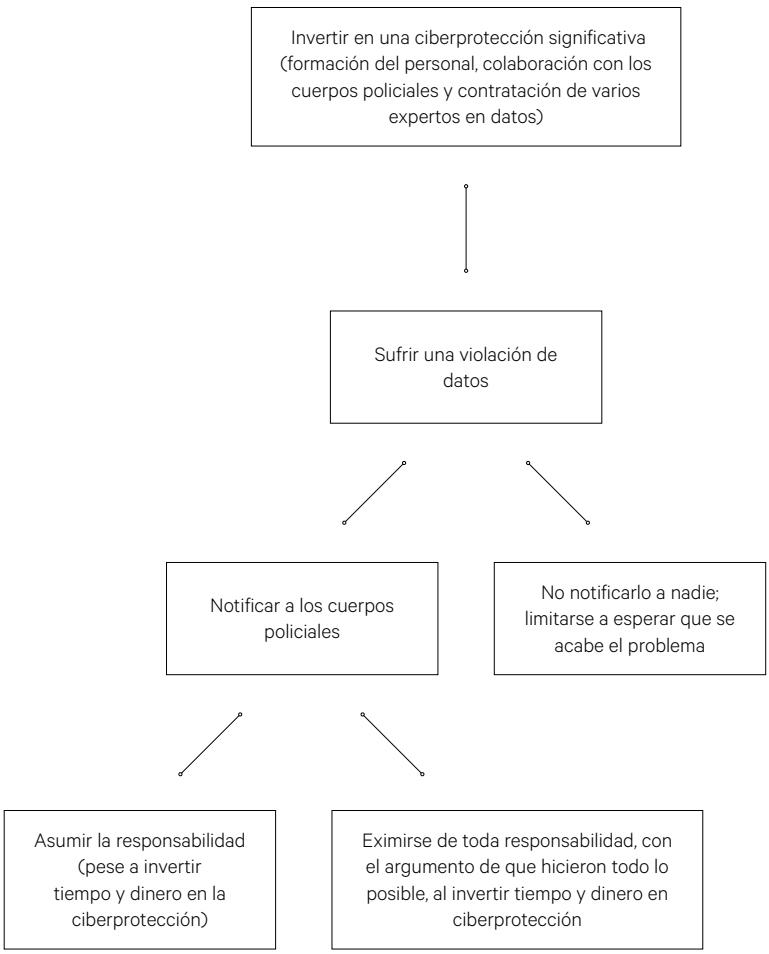
— ¿Las empresas deben ser responsables de su propia ciberseguridad?
— ¿El gobierno debe obligar a las empresas a tener una política de ciberseguridad?
— ¿Se debería exigir a las empresas que compartan la información de ciberseguridad relevante con otras empresas, incluidas sus competidoras?
— ¿Se debería exigir a las empresas que informen a los cuerpos policiales cuando sufran un ataque?
— ¿Tienen las empresas el deber de informar a sus accionistas de un ciberataque?

Como ilustran los apartados anteriores, la cooperación no se puede «dar por supuesta», ni mucho menos. Sin embargo, descartarla de entrada sería demasiado fácil. El reto radica en crear modelos factibles y funcionales que generen un equilibrio adecuado; que protejan a las distintas partes interesadas sin causar un daño económico involuntario a una entidad que coopere. En otros términos: a la hora de determinar el alcance de la cooperación, el desafío consiste en convencer a las empresas de que la colaboración (con clientes, cuerpos policiales y competidores) es beneficiosa, tanto táctica como estratégicamente.

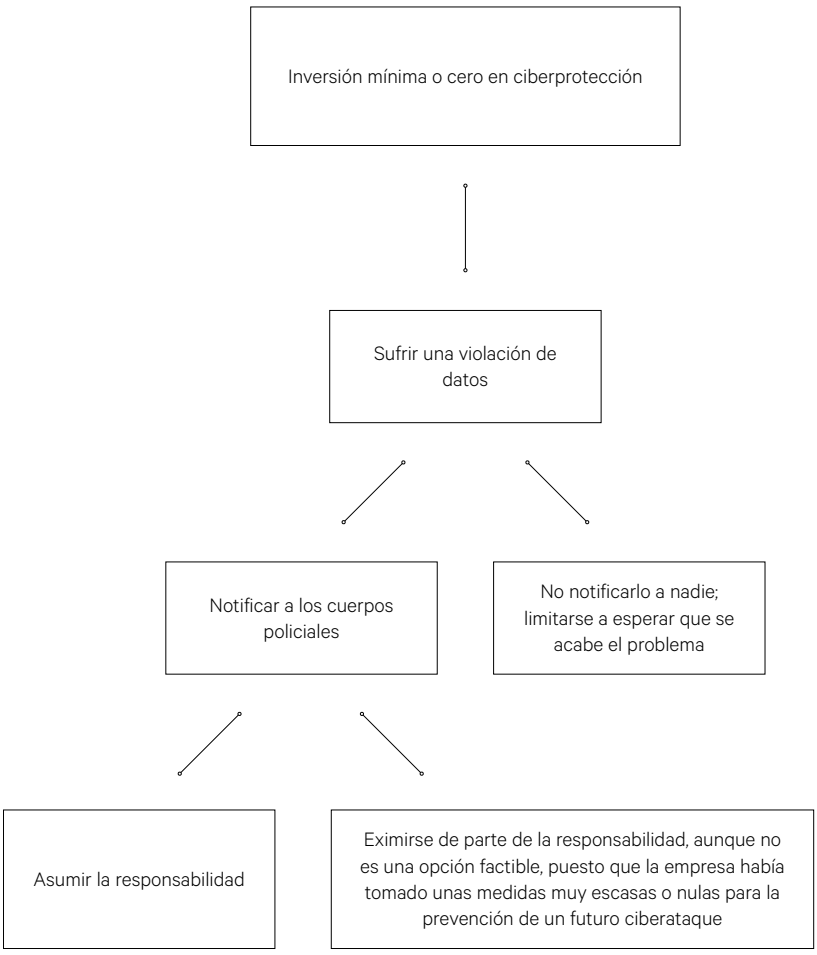
Las ventajas tácticas representan un beneficio a corto plazo, mientras que las estratégicas lo hacen a largo. No tienen por qué ir unidas; de hecho, pueden ser mutuamente excluyentes. En todo caso, al considerar la adopción de un modelo de cooperación, el dilema se puede plantear como un experimento intelectual sobre coste-beneficio.

Para avanzar es fundamental considerar cuatro tipos distintos de empresa: los dos gráficos siguientes tienen el objetivo de ilustrar la relación de las empresas con la cooperación.

Vulneración de datos en una empresa (empresa con una protección significativa)



Violación de datos en una empresa
(empresa sin una protección significativa)



Empresa A La empresa A asume una gran responsabilidad por la cantidad de información a la que tiene acceso. Por consiguiente ha invertido una cantidad significativa de tiempo y dinero en ciberprotección. Colabora estrechamente con los cuerpos policiales, proporciona la formación correspondiente al personal y recurre a expertos en datos para protegerse de un ciberataque.

Ahora, pese a sus denodados esfuerzos, la empresa A ha sido hackeada. De un modo similar a Target o eBay (que sufrieron violaciones de datos en 2013 y 2014, respectivamente), más de cien millones de clientes se han visto afectados por esta intromisión. Se plantean, pues, las preguntas siguientes: ¿qué hacer a continuación?; ¿quién es el responsable del ataque? Sin embargo, como la empresa A tomó medidas considerables para protegerse de un ciberataque, la pregunta pasa a ser la siguiente: ¿la compensación o castigo deberían ser distintos porque la corporación tomó medidas para evitar el incidente?

Sea como fuere, lo primero que debe ocurrir cuando una empresa sufre un ciberataque es que se notifique a las fuerzas policiales. Pese a que las empresas quizá no querrán informar a las autoridades por miedo a las repercusiones o a la pérdida de confianza entre los clientes, hacerlo debe ser una obligación legal. Sin notificación a los cuerpos policiales, estos no podrán deducir patrones o algoritmos que puedan evitar futuros ataques.

El siguiente aspecto a tomar en consideración es si la empresa A está eximida de responsabilidad porque tomó las precauciones necesarias; sufrió un ciberataque, pero no fue por su culpa. Es una cuestión difícil de dirimir y que no tendrá una respuesta definitiva hasta que se promulgue la legislación correspondiente.

Empresa B La empresa B, como la A, es una de las mayores corporaciones de Estados Unidos. Como tal, asume una gran responsabilidad por la cantidad de información a la que tiene acceso. Sin embargo, la corporación B no ha invertido en ciberprotección una cantidad significativa ni de tiempo ni de dinero. Por el contrario, su consejo de administración, consciente de las amenazas contra la ciberseguridad, votó a favor de suspender cualquier inversión económica o de personal en medidas de ciberprotección, dado que son caras y la corporación tiene el objetivo de ganar dinero. Este problema es el máximo exponente del debate entre la protección y los beneficios.

Imaginemos ahora que la corporación B ha sufrido un hackeo.

De una manera parecida los casos de Target o eBay, más de cien millones de clientes se han visto afectados. Como en el caso A, se plantean, pues, las preguntas siguientes: ¿qué hacer a continuación?; ¿quién es el responsable del ataque? Como se ha dicho, el gobierno de Estados Unidos podría decidir asumir la responsabilidad de intervenir cuando el problema implique a empresas de una cierta magnitud, y lo ha hecho en el pasado.

Los cuerpos policiales han de estar en las reuniones de corporaciones y representantes públicos. De lo contrario, el ejercicio se quedará en una cámara de resonancia, en gran medida ineficaz a la hora de concebir y aplicar una política de ciberseguridad

Sin embargo, como la corporación B no tomó medidas considerables para protegerse de un ciberataque, que finalmente se produjo, la pregunta pasa a ser la siguiente: ¿la compensación o castigo deberían ser mayores porque la corporación no tomó medidas? Una vez más, lo primero que debe hacer una empresa cuando sufre un ciberataque es notificarlo a los cuerpos policiales. La mayoría deciden no hacerlo, ya sea por miedo a la pérdida de confianza entre los accionistas, a la percepción de los accionistas o a otras repercusiones. No obstante, la notificación debe ser una obligación legal. El paso siguiente es determinar si la corporación B tiene una mayor responsabilidad a causa de su negligencia.

A diferencia de la corporación A, no puede ser eximida de responsabilidad, puesto que no tomó las precauciones necesarias. Pese a que es probable que el director de inteligencia u otros empleados de la corporación recomendaran lo contrario, la corporación B eligió los beneficios en detrimento de la protección y se convirtió en un blanco fácil. Cabe entonces preguntarse si la negligencia debería repercutir en la compensación o protección posterior al ataque. Es una cuestión que deberá dirimir la legislación por venir.

Empresa C La empresa C, a diferencia de A y B, es una de las más pequeñas de Estados Unidos; es un negocio de ciudad pequeña, controlado con mano firme por algunos miembros de una familia. En consecuencia, asume una responsabilidad notablemente inferior, puesto que tiene acceso a mucha menos información.

Sin embargo, al igual que la empresa A, la empresa C ha invertido una cantidad significativa de tiempo y dinero en ciberprotección. Asimismo, colabora estrechamente con los cuerpos policiales, proporciona al personal la formación correspondiente y recurre a expertos en datos para protegerse de un ciberataque.

Pese a los denodados esfuerzos de la empresa C, ha sufrido un hackeo, pero, al contrario que A y B, dicha violación no afecta a más de cien millones de clientes, ni mucho menos: solo a 5.000 personas. De nuevo, se plantean las preguntas siguientes: ¿qué hacer a continuación?; ¿quién es el responsable del ataque? Cabe suponer, sin miedo a equivocarse, que el gobierno de Estados Unidos sería menos proclive a intervenir cuando la violación es tan reducida que ante las crisis de las corporaciones A y B.

Con todo, se nos plantea la pregunta siguiente: dado que la empresa C tomó medidas considerables para protegerse de un ciberataque, aunque no pudo evitarlo, ¿tendría que recibir algún tipo de compensación o de apoyo? ¿Dicho apoyo tendría que ser superior al asignado a una empresa que no hubiera tomado medidas de protección ante un ciberataque?

La empresa C, pese a su pequeño tamaño en comparación a las A y B, debe estar sujeta también a la obligación legal de informar a los cuerpos policiales de que han sufrido un ciberataque. La pregunta siguiente es si la empresa C debe ser eximida de responsabilidad por tomar las precauciones necesarias y haber sido víctima de un ciberataque pese a no haber cometido falta alguna.

Empresa D La empresa D, al igual que C y a diferencia de A y B, es una de las más pequeñas de Estados Unidos, al tratarse de un negocio de ciudad pequeña, controlado con mano firme por algunos miembros de una familia. En consecuencia, asume una responsabilidad notablemente inferior puesto que tiene acceso a mucha menos información. Sin embargo, como B, la empresa D no ha invertido una cantidad significativa de tiempo ni dinero en la ciberprotección.

En su lugar, decidió suspender cualquier inversión económica o de personal en medidas de ciberprotección porque son caras y está centrada en ganar dinero. Este problema, como quedó patente con el caso de la corporación B, es el máximo exponente del debate entre protección y beneficios.

A causa de su falta de inversión en ciberseguridad, la empresa D ha sido objeto de un hackeo. Sin embargo, a diferencia de los casos de las corporaciones A y B, esta violación no afecta a más de cien millones de clientes, solo a 5.000 personas. El razonamiento y los factores a tener en cuenta son muy similares a los expuestos en el caso de la corporación C. Se nos siguen planteando, pues, las preguntas siguientes: ¿qué hacer a continuación?; ¿quién es el responsable del ataque?

Podemos afirmar, sin miedo a equivocarnos, que es menos probable que el gobierno de Estados Unidos intervenga, puesto que, en comparación con los hackeos de las corporaciones A y B, el impacto es mínimo. No obstante, habida cuenta de que la empresa D no tomó medidas significativas para protegerse de un ciberataque, que al final sufrió, ¿la compensación o castigo deberían ser menores o mayores?

La empresa D, pese a su pequeño tamaño comparada con las corporaciones A y B, debe tener también la obligación legal de informar del ciberataque. A continuación debemos reflexionar sobre su responsabilidad: A diferencia de las corporaciones A y C, no hay justificación para eximirla de responsabilidad, porque no adoptó las precauciones necesarias.

Pese a que es probable que el director de inteligencia u otros empleados de la corporación recomendaran lo contrario, la empresa D eligió los beneficios en detrimento de la protección y se convirtió en un blanco fácil. Cabe entonces preguntarse si la negligencia debería repercutir en la compensación o protección posterior al ataque. Es una cuestión que deberá dirimir la legislación por venir.

El bueno, el feo y el malo de la cooperación

Es más fácil de decir que de hacer.

Esta máxima tan repetida se aplica al modelo corporativo en que se basa el presente ensayo. Una empresa no está exenta de costes. En este sentido, existe una preocupación comprensible por la vulnerabilidad, la exposición y los riesgos injustificados, quizá acompañados por unas ventajas mínimas.

La concisión del CEO citado en el apartado 3 hablaba por sí sola: para él, colaborar no era una opción. Otros líderes corporativos me habían manifestado esta misma actitud, pero, para mi sorpresa, era el mismo mensaje de los agentes policiales federales cuando les pregunté si colaborarían con sus homólogos locales. La respuesta fue tajante y embarazosa: «No cooperamos con los cuerpos policiales locales». Esta respuesta breve y rotunda era embarazosa porque iba dirigida a autoridades policiales locales presentes en la reunión. Sin embargo, pese a lo escueto del mensaje, ponía de manifiesto una cuestión tan vital como preocupante: que los cuerpos policiales cooperan poco entre sí y mucho menos con entidades externas.

Esta salida me pareció en su momento —y aún me lo parece— un signo de arrogancia cortoplacista que antepone «proteger el territorio propio» al bien común. En una reunión reciente con agentes policiales federales me aseguraron que una respuesta así sería acogida con gran desagrado por los altos mandos. Eso espero.

Más allá de las garantías que den las autoridades, es importante que la cooperación entre agentes locales, estatales y federales se institucionalice y no se deje al capricho y la voluntad de los policías implicados. Dicha institucionalización contribuiría al interés público y el bien común, velar por ellos constituye la principal obligación de los cuerpos policiales. Sin embargo, institucionalizar la cooperación entre las diversas partes interesadas requiere tiempo, dedicación y recursos. Asimismo, la puesta en marcha inmediata de protocolos que faciliten la cooperación no está exenta de problemas cuando están representadas diferentes culturas, normas y costumbres. Requerirá de un esfuerzo concertado.

Para implantar la cooperación hay que asignar recursos, encontrar un lenguaje común, identificar objetivos comunes y mitigar problemas tan comprensibles como las reticencias, las vacilaciones y el escepticismo. Ello exige un esfuerzo dedicado de todos los implicados, que centre su motivación en el bien general y no en los costes y cargas temporales. En caso contrario, el proyecto no llegará a buen puerto.

Por otra parte, los aspectos positivos de la cooperación compensan con creces los conflictos y tensiones, como se hace patente en términos de seguridad pública. Francamente, esta debe ser la consideración más importante al sopesar la adopción de un modelo de cooperación.

Reflexiones finales

El tema de la cooperación ha constituido el punto central del presente ensayo; y no es casualidad.

Antiguo centro de vigilancia de la organización de la Agencia de Seguridad Nacional estadounidense (NSA) en Bad Aibling, al sur de Múnich. Las revelaciones sobre programas de vigilancia masiva de la NSA hechas por Edward Snowden en junio de 2013 pusieron en jaque las relaciones diplomáticas entre Estados Unidos y sus socios europeos

Fui asesor legal en un grupo de trabajo del Congreso de Estados Unidos reunido bajo los auspicios del Comité de Seguridad Interior de la Cámara de Representantes, dedicado a la política de seguridad interior de Estados Unidos. Para mí, el principio de cooperación debía prevalecer en el desarrollo e implementación de un sistema eficaz de contramedidas de seguridad cibernética. La argumentación del presente ensayo quiere ayudar al lector a comprender la necesidad de desarrollar la cooperación institucionalizada y, al mismo tiempo, reconocer las dificultades que entraña un empeño de este tipo.

Las razones son diversas: las hay de índole financiera, como en el caso de las empresas; otras derivan del empeño por defender el «territorio» y el presupuesto propios, como me explicaron unos agentes de policía. En todo caso, las consecuencias son fáciles de predecir. El beneficiario de una falta sistemática de cooperación es el malhechor y el perjudicado, sus numerosas víctimas. Dicha falta de cooperación fue un tema recurrente durante la redacción de mi libro y se repitió durante el ejercicio de simulación. En los tres ámbitos (el Congreso de Estados Unidos, la investigación para el libro y la simulación), la actitud de las personas con las que estuve en contacto respecto a la cooperación, ya fuera de tipo proactivo o reactivo fue idéntica: no encajaba en su «modelo». Fue un mantra repetido numerosas veces.

Esto contrasta de manera frontal con una reunión que tuve en Israel con un importante ciberexperto. La conversación fue muy reveladora y arrojó mucha luz sobre la intersección entre la seguridad nacional y la ciberseguridad. Y, lo que es más importante, dejó claro el papel clave que el gobierno puede y debe desempeñar frente a las ciberamenazas. La conversación se centró en cuestiones legales y regulatorias; los aspectos técnicos, pese a su indudable importancia, no tuvieron un papel destacado. Lo que más me admiró, por lo que respecta a la cooperación, es el enorme beneficio derivado de la cooperación y la unión de fuerzas entre los sectores público y privado.

Con ello no quiero quitar hierro a las inevitables tensiones, rivalidades y competición entre ambos. Pero la diferencia respecto a mis conversaciones con los agentes de policía estadounidenses era evidente. Lo distinto de los enfoques era desconcertante y tenía unas consecuencias obvias. De ahí el papel central de la cooperación en mi libro *Cybersecurity: Geopolitics, Law, and Policy*.

El principio de cooperación debe prevalecer en el desarrollo e implementación de un sistema eficaz de contramedidas de seguridad cibernética

Muchos hemos sido víctimas de daños, ya sea en el ámbito personal, profesional o de social. Nuestra vulnerabilidad ante el ciberdelito está bien documentada y no es necesario reiterar la letanía de incidentes ocurridos, que van desde los meramente molestos a los catastróficos.

No hay duda de que hay grupos de individuos en todo el mundo dedicados a buscar modos de utilizar la tecnología del ciberespacio en su favor y en nuestra contra. En ciberseguridad hay, sin duda, un «nosotros» y un «ellos». Los daños causados por los ciberdelincuentes y los ciberterroristas son notables, pero todavía deben preocuparnos más los daños futuros que, con toda seguridad, planean infligir a la sociedad.

Existe una profunda falta de consenso respecto a la intervención gubernamental. Quizá por mis antecedentes en las fuerzas de defensa de Israel, me desconcierta la vacilación que he percibido una y otra vez en Estados Unidos en este sentido. En mi opinión, los ciberataques deben considerarse similares a las agresiones físicas.

La consecuencia de ello, para mí, está clara: un ataque a una corporación estadounidense justifica una respuesta del gobierno. Cierto es que para ello es necesaria la cooperación antes explicada, pero las ventajas, tanto a corto como a largo plazo, compensan con creces cualquier consecuencia negativa de un «exceso» de intervención. Hay demasiado en juego como para recurrir a clichés gastados y mantras irrelevantes sobre derecho a la intimidad. Ello no equivale a infravalorar la importancia de la privacidad (las filtraciones de la NSA constituyen un perturbador recordatorio del carácter real de la intrusión gubernamental), sino a proponer que las ciberamenazas exigen un enfoque equilibrado y matizado. Descartar de entrada la intervención del gobierno resulta corto de miras y, en última instancia, contraproducente.

Hablar de la intervención del gobierno implica hablar también de autodefensa y la autodefensa colectiva. Hoy en día son inseparables.

La autodefensa es crucial en el debate sobre el ciberespacio. Se trata de dirimir la cuestión de si los Estados nación tienen deberes para con las empresas y las personas víctimas de un ciberataque. No es un problema abstracto, sino concreto.

Imponer la responsabilidad de «responder a un ciberataque» al Estado nación comporta grandes riesgos. Solo es posible si se adopta un modelo cooperativo. Si, por el contrario, todos los objetivos potenciales irreales de un ciberataque se «estancan» en un paradigma de no colaboración, solo salen ganando, sin duda alguna, las fuerzas del mal.

En cualquier caso, los sectores privado y público han presentado una oposición tan intensa y sistemática a la cooperación que en algún momento tendrán que parar. Esta oposición, sin duda acompañada de escepticismo, es legítima y no se puede desestimar, por mucho que nos pese.

Porque, pese a todo, la amenaza continuada que plantean los ciberataques potenciales, por no hablar del impacto real de un ataque exitoso, justifican el examen detenido de cualquier propuesta de imponer legalmente unos requisitos y obligaciones de cooperación. La cooperación entre las diferentes partes implicadas que propone este ensayo podría minimizar las consecuencias de un ataque determinado.

Y, en el peor de los casos, la cooperación contendría las consecuencias de un ataque, al dar la posibilidad a otras entidades afectadas (sí, las de la competencia) de aplicar medidas proactivas de protección y al garantizar la implicación plena de cuerpos policiales nacionales y locales en la atenuación de los daños colaterales.

Existen diversos mecanismos para determinar la viabilidad de una iniciativa de este tipo. Como me dejaron claro en el ejercicio de simulación, la comunicación y el diálogo son un excelente punto de partida. Reunir a las partes interesadas, analizar cómo responder y, con suerte, minimizar los daños colaterales de un ataque es un paso importante. Es recomendable que un ejercicio de este tipo incluya a un amplio abanico de participantes, como parlamentarios, miembros de los cuerpos de policía (local, estatal y nacional), directivos (de empresas pequeñas y grandes, que cotizan o no en los mercados de valores), funcionarios o cargos municipales, representantes de grupos de defensores del consumidor y miembros de la población general.

Una iniciativa de este tipo permitirá a la comunidad (tanto en un sentido restringido como amplio) determinar cuál es el mejor mecanismo para garantizar la cooperación frente a un ciberataque.

Es un debate que debemos entablar. Posponer el análisis de los modelos de cooperación no está exento de costes; al contrario, supone costes importantes. Las medidas existentes representan una plataforma eficaz como punto de partida, pero el desafío es grande y debemos abordarlo ya.

Agradecimientos

Debo expresar mi profundo agradecimiento a las personas siguientes, que tuvieron la amabilidad de leer los borradores previos y hacer perspicaces comentarios y sugerencias que han mejorado notablemente el producto final (huelga decir que todos los errores y omisiones son responsabilidad mía): Anne-Marie Cotton, profesora titular en Gestión de la Comunicación, Universidad de Artevelde, Gante (Bélgica); Jessie Dyer, doctoranda (obtención del título de doctora previsto para 2019), S. J. Quinney College of Law, Universidad de Utah; Brent Grover, presidente, Brent Grover & Co.; profesor Daniel Shoemaker, catedrático en la Universidad de Detroit Mercy, y Judy A. Towers, directora de Inteligencia ante Ciberamenazas, SunTrust Bank.

Notas

1. El lector de un borrador anterior indicó que esta afirmación es aplicable al 99% de los directivos corporativos con los que ha tratado.
2. Guiora, Amos N. (2017): *Cybersecurity: Geopolitics, Law, and Policy*, Londres, Routledge.
3. Debido a las normas «Chatham House», no se puede tomar nota de la identidad de los participantes ni de sus comentarios; el ejercicio estuvo auspiciado por la organización National Cyber Partnership.
4. Para un análisis concienzudo del contrato social, ver https://www.iep.utm.edu/soc-cont/
5. https://www.investopedia.com/terms/s/sarbanesoxleyact.asp
6. https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/
7. https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/
8. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
9. https://www.us-cert.gov/ais
10. Problemas nacionales: no solo el robo de identidad, también de propiedades, como ilustra este anuncio: https://www.youtube.com/watch?v=_CQA3X-qNgA
11. Un lector de un borrador anterior señaló que: «Muchos dirían que la ciberseguridad no es más que gestión de riesgos» correo electrónico, archivos del autor.
12. Como ilustra este anuncio de una agencia belga: https://www.youtube.com/watch?v=jop2I5u2F3U
13. http://www.un.org/en/sections/un-charter/chapter-vii/
14. https://www.nato.int/cps/ic/natohq/official_texts_17120.htm
15. Un lector de un borrador anterior planteó los comentarios y preguntas siguientes: ¿De acuerdo con qué pruebas? ¿Qué hay del impacto negativo en la reputación? ¿Pérdida de confianza? Son intangibles, frente a las cifras económicas de rediseñar los «cortafuegos» […]. Sin embargo, el valor de marca también se ha convertido en un elemento importante.
16. Un lector de un borrador anterior señaló que: «[…] desarrollado maravillosamente por Andrew Ehrenberg (London School of Economics) en su teoría de la doble penalización aplicada a la dicotomía entre empresas grandes y pequeñas. Las empresas de pequeño tamaño son dos veces «víctimas» de su tamaño: aunque las pequeñas inviertan, las grandes invierten más, de modo que, en proporción, las primeras tienen que invertir X más que las segundas para obtener un resultado inferior […]».
17. De acuerdo con las normas «Chatham House».
18. Intercambio de correos electrónicos con un lector; correo electrónico, archivo del autor.
19. Véanse los artículos de Finn Frandsen, Timothy Coombs, Robert Heath y Winni Johansen sobre este tema; por ejemplo, «Why a concern for apologia and crisis communication?». Frandsen y Johansen acaban de publicar sus últimas propuestas teóricas en: *Organizational Crisis Communication: A Multivocal Approach*.
20. Intercambio de correos electrónicos con un lector; correo electrónico, archivo del autor.
21. Un lector de un borrador anterior hizo la advertencia siguiente: «Además de la sensibilización, esto también lleva mucho tiempo […] No hemos hecho más que empezar a generar el talento [necesario], y los miembros de la policía rara vez tienen el "ancho de banda" necesario para asumir otro conjunto de competencias»; correo electrónico, archivo del autor.
22. Un lector de un borrador anterior señaló que es una buena propuesta, pero no ha visto agentes de la ley lo bastante duchos en materia empresarial como para poder poner en práctica los elementos de la lista. Ahí es donde entran los reguladores del sector, aportando conocimientos para llevar a efecto dichos elementos; no los agentes de la ley. Además, están asesorando al Departamento de Seguridad Nacional, porque están estableciendo los mismos criterios de la lista.
23. Un lector de un borrador anterior señaló que, en este momento, esto ya se está haciendo en el sector financiero; y que las empresas eran sinceras en los «porqués» de sus procesos de reparación, mientras que todos los que representamos a los reguladores o la policía estábamos esperando a que nos explicaran las cosas. Asimismo, una empresa puede tardar días en determinar que ha habido un hackeo y no solo un fallo del sistema, en especial si el autor de la amenaza ha modificado los registros del sistema y borrado su código, acciones o pasos. Hacer que parezcan problemas normales del sistema es propio de un pirata informático avezado. Esperemos que esta capacidad no sea fácil de adquirir para cualquier pirata informático «corriente y moliente».
24. Un lector de un borrador anterior señaló que estas preguntas ahora las responden los reguladores del sector. A saber, el Estado de Nueva York estableció estos requisitos para cualquier empresa cuya razón social estuviera en este estado antes del final de 2018; el Estado empezará a auditar estas empresas para garantizar que se ha trabajado en la ciberseguridad. Una vez más, no debemos olvidar qué ocurre cuando las empresas trabajan solo para cumplir unos requisitos básicos. Si los criterios a cumplir no se actualizan, una empresa puede cumplirlos y satisfacer a los reguladores pese a no ser cibersegura. La mayoría de las empresas que han sido hackeadas hoy cumplen los criterios del regulador, pero el regulador ya no está al día. Es un escenario con umbrales evolutivos: las empresas cumplirán solo con el mínimo requerido, porque ir más allá cuesta dinero.

OpenMind

ESCUCHA EL AUDIO DE ESTE CAPÍTULO

ACCEDE AL LIBRO COMPLETO

- ¿Hacia una nueva Ilustración? Una década trascendente
- Towards A New Enlightenment? A Trascendent Decade

ACCESO AL ARTÍCULO EN INGLÉS

Cybersecurity: A Cooperation Model

CÓMO CITAR ESTE ARTÍCULO

Guiora, A. N., "Ciberseguridad: un modelo de cooperación",
en ¿Hacia una nueva Ilustración? Una década trascendente, Madrid, BBVA, 2018.

ARTÍCULOS RELACIONADOS

LEER MÁS SOBRE #TECNOLOGÍA #MUNDO DIGITAL

- Ciberataques

C@mbio: 19 ensayos clave acerca de cómo Internet está cambiando nuestras vidas, Mikko Hypponen

- La Ciberseguridad y el nuevo modelo de gobernanza

- Inteligencia Artificial en ciberseguridad: retos

TODOS LOS TÍTULOS DE LA COLECCIÓN OPENMIND