Un libro blanco para la cooperación público-privada en ciberseguridad

Carlos Galán | Licenciado y doctor en Informática, licenciado en Derecho y abogado especialista en Derecho de las TIC, profesor de la Universidad Carlos III de Madrid, presidente de la Agencia de Tecnología Legal y miembro del Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

La cooperación es el hilo conductor que conecta, día a día, a agentes públicos y privados para hacer frente a los desafíos de la ciberseguridad. Un libro blanco facilitaría un debate estructurado para llevar a término dicha cooperación.

Resumen

Los libros blancos tienen por objeto analizar en profundidad un asunto o una política para asesorar a las partes interesadas, a los órganos legislativos o a los Gobiernos. En materia de ciberseguridad, el Estado es el primer y principal garante de la seguridad en el ciberespacio, pero la práctica totalidad del esfuerzo económico y operativo desplegado para anticipar y hacer frente a ciberataques, así como la innovación, provienen del sector privado, especialmente de aquellas empresas designadas operadores de servicios esenciales y de los operadores de infraestructuras críticas, cuyo funcionamiento es indispensable para el mantenimiento de los servicios públicos. Tanto la Ley de Seguridad Nacional de 2017 como la Estrategia Nacional de Ciberseguridad de 2019 respaldan la cooperación público-privada (CPP), pero su materialización precisa una reflexión previa y un debate en profundidad sobre sobre la visión, objetivos, prioridades, métricas y recursos necesarios de esa cooperación. Este ARI aboga por la elaboración de un libro blanco para para estructurar el debate conceptual y, de aprobarse mediante un acuerdo del Consejo de Ministros, facilitar el desarrollo de las normas jurídicas necesarias para materializar sus objetivos.

Análisis

El apoyo mutuo entre el Estado y el sector privado no solo es resultado de un mandato legal encuadrado en la regulación de la seguridad de las redes y sistemas de información (la transposición de la Directiva NIS), sino una manifestación de la necesidad de una estrecha cooperación entre lo público y lo privado. Entre las recomendaciones de la Comisión Europea sobre la implantación de CPP en ciberseguridad figura el informe de Enisa de 2011 "Cooperative Models for Effective Public Private Partnerships Good Practice Guide", el cual ofrece directrices para la formación de partenariados en ciberseguridad enfocados a diferentes propósitos junto

a ejemplos de buenas prácticas en las distintas regiones. Mas recientemente, en 2015, Enisa ha publicado el documento "EP3R 2009-2013 Future of NIS Public Private Cooperation", orientado a la cooperación en materia de resiliencia en el contexto de la Directiva NIS. Es también de obligada referencia el partenariado público-privado Contractual Public Private Partnership on Cybersecurity, iniciado en 2016 entre la European Cyber Security Organization (ECSO) y la Comisión Europea para el desarrollo de la industria de ciberseguridad europea mediante la financiación conjunta de proyectos en el marco del programa de investigación e innovación Horizonte 2020.

La práctica de los libros blancos en el sector público cuenta con varios precedentes en España, como son el Libro Blanco para la Reforma del Sistema Educativo de 1989 del Ministerio de Educación, Cultura y Deporte; los libros blancos para el diseño de títulos de grado adaptados al Espacio Europeo de Educación Superior, elaborados a principios de los años 2000 por una red de universidades españolas apoyada por la Agencia Nacional de Evaluación de la Calidad y Acreditación (Aneca); el Libro Blanco de la Sanidad, elaborado en 2018 por la Confederación Española de Organizaciones Empresariales (CEOE), o el Libro Blanco del Desarrollo Español de Videojuegos 2018, promovido por la Asociación Española de Empresas Desarrolladoras de Videojuegos (DEV) y el Instituto Español de Comercio Exterior (ICEX), también en 2018.

En materia de ciberseguridad, cabe señalar el estudio monográfico "Ciberseguridad: la cooperación público-privada", publicado en 2017 por el Instituto Español de Estudios Estratégicos del Ministerio de Defensa y el Departamento de Seguridad Nacional. Aborda la cooperación público-privada desde cuatro vertientes: (1) el advenimiento de la transformación industrial y las tecnologías facilitadoras; (2) el análisis, intercambio de información y modelo integral de respuesta a las ciberamenazas desde el sistema de seguridad nacional; (3) la protección de las infraestructuras críticas, y (4) la cultura, capacitación y nuevos perfiles profesionales.

Aunque no se pueden considerar libros blancos, la CPP cuenta con dos referencias centrales. En su "Aproximación española a la ciberseguridad", el Centro Criptológico Nacional señala tres objetivos para la construcción de una comunidad basada en la cooperación público-privada: (1) el intercambio de información sobre vulnerabilidades y ciberamenazas, (2) la promoción de la cooperación con sectores de la industria o servicios de ciberseguridad para la mejora de las capacidades de detección, prevención, respuesta y recuperación, y (3) el impulso de estándares[1].

La segunda referencia es la reciente Estrategia Nacional de Ciberseguridad 2019, que define algunas líneas de acción específicas para fomentar la CPP con el objeto de (1) garantizar la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas, , (2) promover el compromiso de los proveedores de servicios de internet (ISP) y de servicios digitales para la protección del ecosistema empresarial, social y de los ciudadanos, y (3) promover la creación del Foro Nacional de Ciberseguridad con el objetivo de potenciar y crear sinergias público-privadas,

[1] En el terreno práctico, el Centro proporciona las Guías CCN-STIC sobre normas, instrucciones y recomendaciones para la mejora de organizaciones, junto con el Sistema de Alerta Temprana del CCN, al servicio de las Administraciones y empresas de interés estratégico para el país.

particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio. Esta tercera línea demandará una mayor estructuración de los distintos agentes del sector privado con el objetivo de consolidar la representatividad en su interlocución con el sector público.

Elementos para la reflexión y el debate

Como se ha mencionado, los libros blancos son tanto más necesarios cuanto más complejo es el problema por tratar. En el caso español, la CPP en materia de ciberseguridad puede observarse desde distintas ópticas. Primero, desde una perspectiva estratégica y política, porque la ciberseguridad es una parte de la seguridad nacional. Segundo, desde la perspectiva de los actores económicamente involucrados en su desarrollo y utilización (fabricantes, usuarios, compradores y vendedores de productos, soluciones o servicios de ciberseguridad, etc.). Tercero, desde una visión ética y jurídica, porque la respuesta a las ciberamenazas exige contemplar medidas de naturaleza jurídica amparadas en el respeto a unos principios éticos esenciales. Cuarto, desde un punto de vista sociológico, porque los nuevos métodos de defensa frente a las ciberamenazas pueden tener un impacto significativo en el comportamiento de las sociedades. Finalmente, el académico y de investigación, porque no es posible construir una adecuada ciberseguridad sin el concurso de las actividades de I+D+i y la presencia de la academia en tales investigaciones.

Además de estas dimensiones, un libro blanco para la CPP en materia de ciberseguridad debería satisfacer alguno de los siguientes objetivos esenciales. Debe elaborar una clara definición del alcance de tal cooperación y señalar hasta dónde debe llegar una cooperación efectiva, capaz de salvaguardar al mismo tiempo los intereses particulares de las empresas privadas (en materia de propiedad intelectual e industrial, por ejemplo) y los intereses generales del Estado y sus ciudadanos. También debe señalar cuáles son las garantías que pueden ofrecerse para asegurar que el intercambio de información entre las empresas privadas y las Administraciones gubernamentales no va a usarse posteriormente para otros propósitos. Otro de los objetivos es la clarificación del marco legal —y ético— en el que podrán desenvolverse las actividades de los investigadores en ciberseguridad; por ejemplo, a la hora del desarrollo de políticas responsables de revelación coordinada de vulnerabilidades. Y ya que, por definición, el ciberespacio no conoce fronteras físicas, las medidas que el sector público adopte para disuadir a terceros de atacar los sectores públicos y privados nacionales debe legitimarse mediante un consenso internacional.

En función de todo ello, se pueden señalar algunas cuestiones que deberían estar presentes en un libro blanco sobre la cooperación público-privada en materia de ciberseguridad.

Investigación, intercambio de datos e inteligencia

Los vectores de ataque de muchas de las amenazas conocidas siguen el mismo patrón, con independencia de su objetivo final, y los procedimientos, tácticas y técnicas usados en un ataque de ciberespionaje contra una empresa privada no difieren gran cosa de otro realizado contra una institución pública. Con los ataques provenientes de las organizaciones delincuenciales sucede otro tanto. Hasta ahora, la respuesta ha sido parcial y, en consecuencia, poco eficiente, por lo que parece cada vez más necesario

que los sectores público y privado aúnen esfuerzos para afrontar un problema común, y una manera efectiva de hacerlo es compartir inteligencia, información y datos que permitan una respuesta eficaz y sistémica y que no comprometa las metodologías (inteligencia pública) ni las fuentes de los datos (privacidad).

Cuestiones sobre la cooperación en inteligencia:

- ¿Cuál debe ser el papel del sector público a la hora de compartir y promover la difusión de información e inteligencia sobre amenazas?
- ¿Cómo deben compartirse datos entre el sector privado y el sector público? ¿Y entre actores privados? ¿La compartición debe ser obligatoria o voluntaria? ¿Cuál debe ser el modelo de compartición de datos de las organizaciones multinacionales?
- ¿Cuál debe ser el tipo de información que puede compartirse? ¿Cómo han de ser los mecanismos para el intercambio: automáticos, manuales, mixtos?
- ¿Puede permitirse una compartición parcial o debe ser completa?
- ¿Debe eximirse de responsabilidad a las entidades privadas por compartir datos personales de sus clientes o usuarios? ¿Debe regularse?
- ¿Cuál sería el coste de compartir grandes volúmenes de datos? ¿Quién debería asumir tal coste?

Las vulnerabilidades de día cero en los productos de software (o de hardware)

Como es sabido, una vulnerabilidad de día cero (*zero-day*) hace referencia a una brecha de seguridad —accidental o intencionada— no conocida públicamente en un producto de *hardware* o, más frecuentemente *software* y para la que no se han desarrollado las acciones correctoras correspondientes. Por su parte, los denominados *exploits* de día cero (*zero-day exploits*) son herramientas usadas para aprovechar dichas vulnerabilidades desarrolladas por todo tipo de actores, desde *hackers* a grupos delincuenciales, pasando por los propios Estados, y que se pueden adquirir en foros *underground* o en la Internet profunda (*deep web*). El descubrimiento de tales vulnerabilidades puede tener lugar en dos momentos diferentes: antes de un ataque, como consecuencia del trabajo de grupos de investigación pertenecientes o ajenos a la empresa desarrolladora del *software* vulnerable, o tras un ataque. Obviamente, cuanto mayor es el tiempo que permanece una vulnerabilidad sin ser reparada, mayor será el riesgo de que terceras partes puedan descubrirla y servirse de ella para propósitos dañinos. Aunque la garantía no es absoluta, una adecuada metodología de desarrollo puede ayudar a limitar la introducción de vulnerabilidades en el *software*.[2]

[2] Tales como las patrocinadas por el Open Web Application Security Project (OWASP) o el National Institute of Standards and Technology (NIST). Security Considerations in the System Development Life Cycle. Gaithersburg, MD: U.S. Dept. of Commerce.

Cuestiones sobre las vulnerabilidades de día cero:

- ¿En qué medida debe participar el sector público en la investigación, desarrollo y "adquisición" de vulnerabilidades y *exploits* de día cero?
- Cuando tiene constancia de ello, ¿hasta qué punto debería el sector público compartir estas vulnerabilidades con el sector privado y con quién (fabricante del producto de *hardware* o *software* vulnerable, terceras empresas, ciudadanos, etc.)? Tal compartición, ¿debería estar regulada legalmente? ¿Deberían existir penalizaciones o sanciones para los fabricantes que, tras habérseles comunicado una vulnerabilidad, no la solucionan en tiempo y forma?
- ¿Es necesario imponer legalmente la obligación de usar metodologías adecuadas en el desarrollo de *software*? ¿Cómo evaluar, auditar y, en su caso, certificar los productos evaluados? En este escenario, ¿es razonable limitar la importación de productos que no estén certificados o limitar las subvenciones públicas a desarrollos no evaluables?

Responsabilidad por las vulnerabilidades

Al tiempo que las sociedades occidentales son cada vez más dependientes de sus sistemas de información, la importancia del *hardware* y, muy especialmente, del *software* sobre el que se sustentan ha crecido de forma pareja. Muchas actividades actuales relacionadas con la economía, el trabajo, la salud, las relaciones o el ocio se apoyan en unas tecnologías que deberían garantizar su seguridad y su correcto funcionamiento. Desafortunadamente, esto no siempre es así. La celeridad que el mercado impone a los fabricantes provoca que muchos productos tecnológicos se comercialicen con graves vulnerabilidades, que obligan a los destinatarios a estar permanentemente atentos y adoptar las medidas de remedio más adecuadas en cada caso o a las que tienen acceso. Frente a esta realidad, los fabricantes han venido esquivando su responsabilidad por la presencia de vulnerabilidades en sus productos, que, en ocasiones, ponen en grave peligro el normal desenvolvimiento de las sociedades. Por otro lado, la desaparición de empresas, la obsolescencia de la tecnología, la preocupación por el desarrollo de nuevas versiones —y el olvido de las anteriores— o la falta de continuidad en la generación de parches incrementan significativamente estos riesgos.

Cuestiones sobre vulnerabilidades:

- ¿Cuál debe ser la actitud de los poderes públicos en materia de vulnerabilidades? ¿Es necesaria una regulación que determine el alcance de la responsabilidad de los fabricantes?
- ¿Quién es responsable de los perjuicios de una vulnerabilidad en un producto de *hardware* o *software*? ¿Es algo que puedan negociar las partes en todos los casos? ¿Es igualmente responsable un proveedor de *software* abierto que uno que sea propietario? ¿En qué casos un integrador podría ser responsable por un *software* de terceros? ¿Cabe la misma responsabilidad en un *software* comercial que en *software* como servicio?
- ¿Quién es responsable de eliminar una vulnerabilidad una vez descubierta?
- ¿Cuál es la responsabilidad de los usuarios en implementar los parches cuanto antes?

La atribución de los ciberataques

Es sabido que atribuir la autoría de un ciberataque a un actor concreto puede ser, en muchos casos, una tarea extraordinariamente compleja. Lo mismo cabe señalar de los supuestos "colaboradores" o cómplices de los atacantes: la ocultación, el enmascaramiento o las llamadas *acciones de falsa bandera* contribuyen a ello. La complejidad de la atribución aumenta en relación con la oportunidad y el alcance de la respuesta: mientras que una respuesta inadecuada podría causar incidentes y réplicas contraproducentes, la ausencia o tibieza de respuesta podría aumentar el número de ataques y el descrédito de las instituciones.

A falta de una regulación o acuerdo internacional sobre atribución, las acciones de disuasión en sus vertientes pasiva (poner dificultades a los atacantes) o activa (responder ante los ataques, lo que se ha dado en llamar *defensa activa*) ya forman parte de los contenidos de las estrategias nacionales de seguridad modernas, porque son los Gobiernos los responsables del ejercicio de las acciones de respuesta. No obstante, la CPP deberá precisar el papel del sector privado en la atribución de los ciberataques, tal y como refleja el cuadro siguiente.

Cuestiones sobre atribución:

- ¿Cómo deben involucrarse los Gobiernos cuando el sector privado alega públicamente que un actor concreto es responsable de un ciberataque?
- ¿Hasta dónde debe involucrarse una entidad privada en la atribución de un ciberataque?
- ¿Cómo deben verificar los Gobiernos la verosimilitud de una supuesta atribución? ¿Cómo abordar el problema cuando las víctimas son organizaciones multinacionales? ¿Cómo debe manejarse públicamente una situación como esta?

Ataques generados por botnets

Un *botnet* es un conjunto (generalmente extenso) de dispositivos previamente infectados —que pueden ir desde ordenadores personales a dispositivos de *IoT*, *wearables*, etc.— utilizados por los agentes de amenazas para generar ciberataques (ataques de denegación de servicio o de propagación de *ransomware*, por ejemplo). Cuanto mayor sea el número de dispositivos comprometidos por un *botnet* en cualquier parte del mundo, mayor será el efecto de tales ataques, y es ahí donde se difuminan las consideraciones en torno a actores o fronteras terrestres. La prevención y respuesta frente a los *botnets* es otro componente importante de la CPP.

Cuestiones sobre *botnets*:

- ¿Qué deben hacer los sectores público y privado para prevenir la proliferación de *botnets* y cómo deberían cooperar?
- ¿Cómo deberían investigarse y estudiarse los *botnets* existentes? ¿Existe alguna limitación en cuanto a las entidades que pueden investigar o a los métodos de investigación usados? ¿Cómo articular la cooperación público-privada en la investigación de *botnets*?
- ¿Cómo deberían desmantelar las *botnets* los actores de todo el ecosistema? ¿Cómo gestionar los riesgos asociados a la comercialización de los productos y a la reputación de los fabricantes? ¿Cómo compaginar el derecho a la privacidad de los usuarios con el desmantelamiento de *botnets*?
- ¿Qué responsabilidad deben asumir los actores involucrados (fabricantes, distribuidores o usuarios) en el caso de dispositivos vulnerables no parcheados?

Monitorización o supervisión de los ciberataques

La monitorización o supervisión de datos e informaciones —comunicaciones, esencialmente— forma parte del arsenal de trabajo de los investigadores en ciberseguridad. Dichas informaciones pueden ser parte de las relaciones entre un empresario y sus trabajadores, entre un ISP y sus clientes o entre una plataforma tecnológica (pública o privada) y sus usuarios. No obstante lo anterior, no es menos cierto que la monitorización o supervisión de las comunicaciones exige, como así lo señalan las regulaciones sustentadas en los principios del Estado de derecho de todo el mundo, un escrupuloso respeto a los derechos fundamentales de los individuos, en concreto a su privacidad.

Cuestiones sobre la monitorización/supervisión:

- ¿Quién debe estar facultado para monitorizar/supervisar qué tipo de información?
- ¿Hasta dónde ha de alcanzar la monitorización: a los mensajes, a los metadatos…? ¿Es necesario regular con mayor profundidad las excepciones legales a la monitorización de contenidos?

La gobernanza de la ciberseguridad

En la actualidad, y por lo que respecta a España, la gobernanza de la ciberseguridad está distribuida entre distintas entidades, entre las que cabe destacar: órganos de coordinación y asesoramiento (Consejo Nacional de Ciberseguridad y Departamento de Seguridad Nacional, respectivamente), organismos públicos ejecutivos (Centro Nacional de Inteligencia-Centro Criptológico Nacional, Instituto Nacional de Ciberseguridad, Centro Nacional de Protección de Infraestructuras y Ciberseguridad, Mando Conjunto de Ciberdefensa) y otros organismos públicos y privados gestores de CSIRT o centros de operaciones de ciberseguridad (SOC). El futuro libro blanco deberá seleccionar aquellos ámbitos en los que centrar la cooperación CPP, así como promover objetivos y líneas de acción establecidas en las referencias mencionadas. Entre estas, cabe mencionar la manera de articular el ecosistema y la interlocución de los agentes privados, la forma de identificar los nuevos ámbitos de la ciberseguridad por regular y el modo de hacerlo, la necesidad de enmarcar el modelo de cooperación en ámbitos clave

de la seguridad nacional tales como la Ley PIC o el modelo que seguir para el fomento de la investigación, entre otras. Una adecuada gobernanza de la ciberseguridad exige la mayor coordinación entre las diferentes entidades y, quizás, la creación de un Centro Nacional de Ciberseguridad.

Cuestiones sobre gobernanza:

- ¿Cuál debe ser el modelo de gobernanza de la ciberseguridad?
- ¿Qué entidades y organizaciones públicas deben ser responsables de asumir qué competencias nacionales en materia de ciberseguridad?
- ¿Bajo qué esquemas deben participar las entidades privadas en este modelo de gobernanza?
- ¿Es necesaria una Ley de Ciberseguridad Nacional capaz de articular todo ello?

El acceso a datos cifrados

Las técnicas criptográficas y, en concreto, el cifrado de la información constituyen los mecanismos más útiles a la hora de proteger la información que se transmite o se almacena, por lo que podemos concebir la criptografía como un recurso que forma parte de los derechos y la libre iniciativa de los usuarios de los medios tecnológicos. Sin embargo, la criptografía también está al alcance de quienes se aprovechan de sus características para perpetrar ataques (ocultación de identidad, inclusión de código dañino o *malware* en los contenidos trasmitidos, etc.), que, de no ser descubiertos a tiempo, pueden comportar daños importantes para los sistemas de información de las víctimas.

Así las cosas, y admitiendo que el cifrado es un derecho, los cuerpos policiales de Europa han venido solicitando la presencia de mecanismos legales y la estrecha colaboración de operadores de comunicaciones electrónicas, proveedores de plataformas de Internet (OTT) y fabricantes de terminales con el fin de descifrar las comunicaciones cifradas (criptoanálisis) o acceder a información cifrada en el dispositivo del usuario y en las plataformas de servicios. Esta colaboración se practica en circunstancias regladas y sin conculcar derechos fundamentales, como el derecho a la privacidad o el secreto de las comunicaciones, pero ha abierto el debate en torno a los llamados *mecanismos de cifrado fuerte* (más robustos y cuya ruptura exige los mayores recursos tecnológicos) frente a un *cifrado débil* (menos robusto y con puertas traseras, lo que lo hace más vulnerable al criptoanálisis).

Cuestiones para la reflexión y el debate:

- ¿Quién debería poder acceder a datos y comunicaciones cifradas y en qué supuestos?
- ¿Es conveniente o útil diferenciar *cifrado fuerte* de *cifrado débil*? ¿Quién debería determinar qué algoritmos de cifrado débil podrían usarse? ¿Cuál sería la responsabilidad del sector público en asegurar la inviolabilidad de las puertas traseras de tales algoritmos?
- ¿Debe regularse la obligación de usar técnicas de cifrado en determinadas comunicaciones, incluso en el sector privado? ¿Qué tipo de cifrado: débil o fuerte?
- ¿Cómo cohonestar el derecho al cifrado con la responsabilidad de las instituciones públicas competentes en la prevención e investigación de los delitos?

Conclusiones

La articulación de un libro blanco sobre la cooperación público-privada en materia de ciberseguridad ofrecería un marco conceptual adecuado para potenciar la cooperación y la priorización de áreas donde sea más necesaria. En particular, proporcionaría un análisis sobre la necesidad de normas jurídicas, estándares o esquemas de certificación que faciliten la consecución de los objetivos establecidos.

En este sentido, la Estrategia Nacional de Ciberseguridad 2019 establece unas líneas de acción específicas para el estímulo de la cooperación público-privada, en concreto la creación de un Foro Nacional de Ciberseguridad orientado a la identificación entre todos los agentes de las oportunidades y amenazas prioritarias para la ciberseguridad.
Con el ánimo de propiciar un debate muy preliminar sobre los contenidos que abordar en un posible libro blanco sobre la cooperación público-privada, este ARI ha señalado distintos elementos y puntos de vista desde donde puede observarse el problema de la ciberseguridad, así como cinco objetivos de carácter general y ocho elementos significativos que considerar, sobre los que se exponen distintas cuestiones abiertas a debate.