DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 124 | Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DEL EXCMO. SR. D. JOSÉ MANUEL GARCÍA-MARGALLO Y MARFIL

Sesión núm. 24

celebrada el jueves 13 de diciembre de 2018 en el Palacio del Senado

---

Página

ORDEN DEL DÍA

Celebración de las siguientes comparecencias:

---

cve: DSCG-12-CM-124

Se abre la sesión a las quince horas y treinta y cinco minutos.

COMPARECENCIAS:

— COMPARECENCIA DEL RESPONSABLE DE OPERACIONES DEL CENTRO EUROPEO DEL CIBERCRIMEN (EC3) DE EUROPOL, DON FERNANDO RUIZ PÉREZ, ANTE LA COMISIÓN MIXTA DE SEGURIDAD NACIONAL. (Número de expediente del Senado 713/001107 y número de expediente del Congreso de los Diputados 219/001522)
AUTOR: COMISIÓN MIXTA DE SEGURIDAD NACIONAL

El señor **PRESIDENTE:** Damos comienzo a la sesión de la comisión de hoy con la primera comparecencia de don Fernando Ruiz Pérez, responsable de operaciones del Centro Europeo del Cibercrimen de Europol, al que doy inmediatamente la palabra en un primer turno de exposición; intervendrán luego los portavoces de los distintos grupos; el compareciente tendrá un segundo turno; haremos un brevísimo turno también para que los portavoces digan si están satisfechos o no con la respuesta y cerrará el compareciente.

Tiene la palabra don Fernando Ruiz Pérez.

El señor **RUIZ PÉREZ** (responsable de operaciones del Centro Europeo del Cibercrimen (EC3) de Europol): Muchas gracias, señor presidente. **(El señor compareciente apoya su intervención con la proyección de diapositivas).**

En primer lugar, quiero dar las gracias por la invitación a presentar hoy aquí las actividades que realizamos por parte de Europol en la lucha contra la ciberdelincuencia. He preparado una presentación que, dada la estructura de la comisión, espero haber acabado en unos treinta minutos para dar tiempo luego a las réplicas. Por tanto, iré rápido, porque quería cubrir bastantes cosas.

Como no sé exactamente el conocimiento que tienen acerca del funcionamiento de Europol y sus funciones, en primer lugar voy a presentar brevemente la organización, posteriormente me centraré en el Centro Europeo de Lucha contra la Ciberdelincuencia, comentaré las principales tendencias en esta área, a lo que esperamos enfrentarnos en el próximo periodo y las dificultades que nos encontramos en la lucha contra esta cibercriminalidad y posteriormente presentaré algunos ejemplos de las operaciones e iniciativas que desarrollamos en Europol para luchar contra la ciberdelincuencia.

Europol es la agencia policial europea para la coordinación de investigaciones; tiene su sede en La Haya, Países Bajos, y el mandato de Europol es básicamente para prestar apoyo a las autoridades competentes de los Estados miembros en la lucha contra el crimen organizado, terrorismo y ciberdelincuencia, investigaciones supranacionales que afecten a más de dos Estados. ¿Cómo prestamos este apoyo? Básicamente a través de una serie de servicios y de productos. Nosotros no investigamos, nosotros no iniciamos nuestras propias investigaciones, nosotros no solicitamos entradas y registros, no realizamos detenciones, nuestra función es prestar apoyo a las policías de los Estados miembros. Estos apoyos son a través de una serie de servicios y funciones: primero, a través de conocimiento especializado. Tenemos algunos de los mejores especialistas en Europa en algunas áreas como pueden ser criptomonedas, análisis forense, análisis de equipos informáticos, análisis de *malware*. Cuando los Estados miembros tienen alguna dificultad, algún problema y requieren asesoramiento nos contactan y tratamos de apoyarles en ese sentido. También realizamos apoyo operativo, tanto en los países donde se desarrollan operaciones, donde podemos ser invitados a participar en las entradas y registros como apoyo en el análisis de los equipos que intervienen, eso es algo que a requerimiento de las autoridades nacionales podemos hacer. Facilitamos el intercambio de información entre las agencias policiales, tenemos unos sistemas de intercambio de información acreditados hasta SIE Confidencial, con lo cual son sistemas muy seguros a los que directamente las autoridades nacionales pueden acceder y realizar peticiones bilaterales o en las que pueden incluir a Europol.

Una de las principales funciones que realizamos, aparte de facilitar el intercambio de información, es analizar los datos que recibimos. Una de nuestras funciones es ser un repositorio de información operativa en relación a las investigaciones que están abiertas en diversos Estados, cruzar toda esa información y alcanzar una visión global de lo que es un determinado grupo criminal, una determinada estructura criminal y ayudar a los Estados a desarrollar una estrategia, identificando huecos de inteligencia y estrategias para desarrollar la investigación. Esto lo hacemos a través de reuniones que organizamos con los propios investigadores que van a nuestra sede y entre todos debatimos cuál es la mejor estrategia, involucrando no solo a autoridades policiales, sino también a autoridades judiciales: fiscales y jueces.

cve: DSCG-12-CM-124

Adicionalmente, Europol dispone de una red de oficinas de enlace, lo cual es uno de los principales beneficios de esta organización. Los Veintiocho Estados miembros y terceras partes con acuerdo operativo con la organización tienen una representación en nuestro edificio. Eso facilita muchísimo la colaboración. Cuando tenemos algunas dificultades o hay alguna duda en relación a los intercambios de información, en lugar de esperar a los intercambios de información telemáticos es tan sencillo como coger el ascensor e ir a Francia, ir a Reino Unido, ir a Croacia y preguntar a los oficiales de enlace qué ocurre con la investigación. Eso hace que el desarrollo de la coordinación sea muy fluido y es, sin duda, uno de los elementos significativos que tenemos en Europol. Aparte, la organización tiene sus propios oficiales de enlace, tenemos ahora mismo destacados oficiales de enlace en Interpol, tanto en Lyon como en Singapur y tenemos dos oficiales de enlace en Washington para facilitar los intercambios de información con las autoridades norteamericanas.

El Centro de Operaciones de Europol se estructura en cinco grandes bloques. Tenemos un centro operativo que es, digamos, la puerta de entrada a todas las solicitudes de información y a todos los intercambios, que está operativo continuamente, 24/7; tenemos un Centro de Crimen Organizado; un Centro de Lucha contra el Terrorismo; una red de información que apoya este flujo de información dando un apoyo horizontal genérico y tenemos el Centro Europeo de Lucha contra la Ciberdelincuencia.

El Centro Europeo de Lucha contra la Ciberdelincuencia empezó a operar en 2013 y fue creado como una respuesta europea a la lucha contra la cibercriminalidad. Cuando fue establecido recibió un mandado específico. Este mandato se estructura en tres funciones, básicamente en tres áreas criminales. Una de ellas está centrada en los fraudes *online*; otra, en ciberdelitos, ataques contra las infraestructuras críticas, *malware*, *ransomware*, *botnet*, y, la tercera, abuso sexual de menores *online*. Normalmente, recibo preguntas sobre por qué el abuso sexual de menores se considera dentro del paraguas del ciberdelito. En nuestra opinión, fue una decisión acertada. Como veremos posteriormente, la manera de operar de los abusadores sexuales, cómo intercambian material y cómo se relacionan está estrechamente relacionado con el desarrollo de las tecnologías. Por lo tanto, es bueno que el equipo que coordina, que da apoyo a esas investigaciones esté dentro del Centro Europeo de Lucha contra el Ciberdelito para beneficiarse de ese conocimiento que tiene el centro acerca de estas tecnologías.

El Centro Europeo de Lucha contra la Ciberdelincuencia está estructurado en tres grandes unidades. La primera es Operaciones, que es la que yo dirijo, en la que tenemos una serie de equipos, tres de ellos directamente relacionados con este triple mandato que acabo de referir. Tenemos un cuarto equipo, con funciones de ciberinteligencia, que, básicamente, se ocupa de recopilar información de fuentes abiertas, y tenemos especialistas en criptomonedas que apoyan al resto de equipos dentro del Centro de Lucha contra la Ciberdelincuencia, pero también a otros centros de Europol, como el Centro de Lucha contra el Terrorismo, el Centro de Lucha contra el Crimen Organizado. Recientemente, hemos creado un equipo, el Dark Web Team, para coordinar la lucha contra el uso criminal, la criminalidad dentro de la *dark web*, a lo que me referiré posteriormente con algunos detalles. Asimismo, coordinamos el J-CAT, el centro de coordinación de lucha contra la ciberdelincuencia, en el que están representados todos los Estados miembros. Posteriormente, facilitaré más información sobre esta iniciativa.

Tenemos una unidad forense que presta apoyo forense, digital y análisis informático de equipos y servidores intervenidos a requerimiento de los Estados miembros y siempre y cuando sea una investigación de relevancia en la que hayamos estado involucrados. No tenemos capacidad para ser la unidad de análisis forense de Europa, con lo cual damos apoyo cuando realmente hay necesidad de *expertise*, de conocimiento, del que los Estados pueden carecer en un momento determinado. También tenemos un grupo de análisis forense de documentos.

Por otra parte, tenemos una tercera unidad, que es la de estrategia. Fuimos el primer gran centro creado dentro del Departamento de Operaciones de Europol. Posteriormente, vinieron el Centro de Lucha contra el Terrorismo y el Centro de Lucha contra el Crimen Organizado, donde se encuentra el Centro de Lucha contra la Inmigración Ilegal. Desde un principio creamos la unidad de estrategia ya que, dentro de la lucha contra la ciberdelincuencia, la estrategia es fundamental. Hay muchas funciones estratégicas de las que no queremos que nuestro personal especializado en operaciones se tenga que hacer cargo. Quiero que mi personal de operaciones se dedique a lo que hace, que es dar apoyo operativo, analizar la información que recibimos de investigaciones desarrolladas por los Estados. No deseamos que este personal especializado invierta tiempo en otras funciones igualmente importantes, pero que requieren otro tipo de perfiles. Dentro de estrategia, coordinamos la cooperación con el sector privado; coordinamos los aspectos relacionados con *internet governance*, cómo las decisiones que se toman a nivel mundial sobre

cve: DSCG-12-CM-124

el funcionamiento de internet muchas de ellas afectan a nuestra capacidad de investigar. Por tanto, tenemos que estar presentes en esos foros para, por lo menos, informar sobre ciertas decisiones y cómo pueden afectar a las investigaciones. Esta unidad estratégica también coordina las funciones de formación y las relacionadas con la prevención. Por último, desarrolla el análisis estratégico, que es una función fundamental. Tenemos unos recursos limitados, por lo tanto, hay que priorizar dónde los invertimos y, para hacerlo de una manera coherente, debemos tener una buena visión de la amenaza, de qué es a lo que nos enfrentamos y qué es lo que requiere prioridad. Para ello, todos los años desarrollamos un documento, publicado a finales de septiembre principios de octubre de este año. El IOCTA es una valoración de la amenaza criminal en internet, es un documento con perspectiva policial, aunque bebe de distintas fuentes, también del sector privado, de fuentes policiales, de la academia, fuentes abiertas, porque toda la información es buena. Con ello, realizamos una previsión, valoramos lo que hemos visto hasta entonces y hacemos una previsión de lo que vamos a ver el año siguiente para, de este modo, ayudarnos a tomar decisiones e invertir nuestros recursos allí donde creemos que van a hacer más falta.

Estas son algunas de las amenazas que destacamos en este documento, que es público, está publicado en nuestra página web, a la que todo el mundo puede acceder.

Hay muchas más cosas, pero, simplemente, voy a dar una pincelada de algunas cuestiones importantes. La primera es *ransomware*, que es un *malware* que ataca a sistemas informáticos y que, básicamente, encripta la información de los usuarios o de los equipos y pide un rescate, por ejemplo pide que se pague un dinero, o a través de criptomoneda o a través de otros medios de pago, para poder facilitar la clave de esa incriptación de esos archivos y que así el usuario pueda recuperarlos. El año pasado vimos dos grandes ataques a nivel internacional relacionados con *ransomware* y esperamos seguir viéndolos, porque los criminales siguen obteniendo un beneficio económico. Por lo tanto, seguiremos viendo campañas de *ransomware.*

Ataques de DDOS, denegación de servicios, que es otra de las grandes amenazas que estamos viendo y vamos a seguir viendo en el futuro. Después les explicaré alguna operación que hemos coordinado recientemente en la lucha contra este tipo de ataques que pueden tener distinta motivación, pueden buscar una extorsión, pueden pedir dinero a empresas a cambio de no ser atacadas por este tipo de ataques, o pueden ser de otro tipo ideológico con distintas motivaciones.

Fraude en los medios de pago con y sin tarjeta presente, fraude *online*, negocio *online*, *e-commerce* crece y, por tanto, el fraude en esta área va a seguir creciendo también; también el fraude a través de *skimming*, que se hace con tarjeta presente, la copia de los datos de la banda magnética de las tarjetas es algo en lo que sigue habiendo un elevado fraude. Posteriormente explicaré algo acerca de este tipo de criminalidad.

Esto sí que es novedoso: hemos visto cómo los usuarios de criptomonedas y los *exchangers,* aquellas empresas que cambian criptomoneda por moneda corriente, son atacados para robar, precisamente, estas criptomonedas. Ahora mismo es uno de los principales objetivos criminales, porque saben que a través de este modo pueden obtener grandes ganancias.

El *cryptojacking* son ataques; básicamente es el uso de ancho de banda o capacidad de procesamiento para generar precisamente criptomonedas. También hay algunos debates; puede no ser considerada incluso una actividad criminal, pero cuando los criminales jaquean páginas web de otras personas para beneficiarse de su ancho de banda o de la capacidad de procesamiento de los usuarios, entonces estamos hablando de actividad criminal.

Ingeniería social como uno de los mecanismos más importantes a la hora de facilitar la ciberdelincuencia, lo cual hace ver que todavía se requiere muchísima educación. Pensamos que para ser ciberdelincuente hace falta tener grandes conocimientos y hacer uso de muy sofisticadas herramientas informáticas, muchas veces pura ingeniería social como recuperar información acerca de una empresa y a través de un correo electrónico, unas llamadas, cuando se tiene la información adecuada, quién está llamando, cuándo está llamando, aparentando ser alguien de una empresa, pues vemos que tienen información o facilitan incluso transacciones económicas, y todo esto es a través de lo que se llama ingeniería social.

El uso criminal de la *dark web*, a lo cual me voy a referir posteriormente, es algo en lo que llevamos centrando nuestra atención durante mucho tiempo, pero ahora lo estamos haciendo con más coordinación, lo cual era muy necesario y la producción de material de uso sexual de menores, que seguimos viendo que continúa.

cve: DSCG-12-CM-124

En la lucha contra la ciberdelincuencia nos enfrentamos a algunas dificultades a nivel policial: la primera es la falta de datos. Cuestiones como la retención de datos no es homogénea en algunos países de nuestro entorno; en la Unión Europea el periodo de la retención de datos es muy corto y en algunos casi inexistente, lo cual hace que la atribución de las direcciones IP, que es una de las principales herramientas que tenemos los investigadores para investigar, no hay tiempo suficiente desde que se tiene conocimiento hasta que el servidor identifique quién es el usuario,hay un proceso, y si ese proceso se alarga, cuando se pide esa información, esos datos ya se han borrado, con lo cual dificulta mucho la investigación. El uso de la incriptación es cada vez más frecuente tanto la incriptación de archivos como la incriptación de las comunicaciones; el uso de criptomonedas dificulta también mucho el seguimiento de las transacciones económicas relacionadas con las actividades criminales.

Carrier Grade NAT es una herramienta utilizada por los servicios de acceso a internet para que a través de una misma dirección IP muchos usuarios puedan acceder a internet, con lo cual cuando nosotros identificamos una actividad criminal y la relacionamos con una dirección IP específica, esta dirección IP no está asignada a una persona en concreto, puede ser compartida por muchas personas y, si no hay una información específica que podamos aportar para que veamos quién de estas muchas personas comparten esta dirección son los usuarios finales, no podemos identificarlos o proceder con la investigación; es una herramienta utilizada por los servicios de acceso a Internet precisamente por la falta de direcciones IP disponibles para facilitar los servicios.

En la *dark web*, tanto los usuarios como los contenidos *online* son anónimos, con lo cual, si no sabemos dónde está ubicado eso conlleva problemas de investigación y de jurisdicción, y lo mismo ocurre con el almacenamiento en la nube cuando hay varias países o jurisdicciones involucradas en el almacenamiento de la información.

En cuanto a los marcos legales, a pesar de que en la Unión Europea tenemos un marco legal similar, todavía hay diferencias considerables, sobre todo a la hora de realizar investigaciones *online*. En el año 2015 en España se modificó la Ley de Enjuiciamiento Criminal y se actualizó la capacidad de investigar *online* y lo que se puede hacer con un agente encubierto *online*. Muchos países de nuestro entorno todavía no disponen de herramientas para realizar este tipo de investigaciones, lo cual es una dificultad.

Respecto de la cooperación internacional, en concreto, el intercambio de comisiones rogatorias internacional aún es un proceso muy lento. En un entorno en el que los cibercriminales pueden cambiar infraestructura criminal de un país a otro en cuestión de minutos, el intercambio de comisiones rogatorias es un proceso que lleva semanas, meses en el mejor de los casos, con lo cual hay una gran diferencia en velocidad. Por tanto, se ha demostrado que no es una herramienta que nos pueda facilitar intercambio de información lo suficientemente rápido como para ayudar al desarrollo de las investigaciones. A nivel europeo hay distintas iniciativas dentro del IE, el paquete de intercambio de evidencias digitales, que se está actualmente debatiendo en el Consejo y en el Parlamento. Vamos a ver lo que tarda en implementarse y cómo resulta; por lo menos se está abordando este tipo de problemas.

Y, por último, el entorno cambiante. La tecnología está en continuo desarrollo y eso requiere una continua formación de los investigadores para saber cómo funcionan las tecnologías, cómo funcionan las herramientas y las plataformas. Es una formación continua que requiere esfuerzo e inversión.

La pregunta es cómo afrontamos las investigaciones en este escenario y cómo logramos llevarlas a buen puerto desde un punto de vista policial. Pues bien, se hace a través de la colaboración con todos los actores que participan en este entorno. Nuestro principal socio en Europol, el Centro Europeo de la Ciberdelincuencia, es una *taskforce* en la que reunimos a los jefes de unidades de delincuencia tecnológica de los Veintiocho Estados miembros. Nos reunimos habitualmente, varias veces al año, y hablamos sobre cuáles son sus necesidades, qué tipo de productos necesitan, si el servicio que estamos prestando va en la línea de lo que sus investigadores demandan, etcétera. Por tanto, repito, es nuestro principal interlocutor.

Tenemos un Programme Board, una serie de agencias, organizaciones con las que nos reunimos también periódicamente con el fin de debatir iniciativas y alinear estrategias. Dentro de este grupo tenemos el consejo, la comisión, Interpol, Cepol, European External Action Service, Eurojust, etcétera, una serie de agencias y organismos con los que debatimos también el desarrollo y la estrategia del centro.

Tenemos también una serie de grupos de asesoramiento. Ahora tenemos principalmente tres centrados en seguridad en internet, proveedores de servicios y servicios financieros. Básicamente esta es nuestra forma de relacionarnos con el sector privado. Son grupos no muy grandes, porque en las reuniones que mantenemos de forma periódica, si hay muchos miembros no es posible mantener un

cve: DSCG-12-CM-124

diálogo fluido. Empezamos creando una red de personas con las que queríamos trabajar pero queríamos hacer algo más que hablar; queríamos debatir sobre las tendencias y los problemas que nos encontramos desde un punto de vista policial o del sector privado. Es decir, queremos hacer cosas con ellos, con lo cual lo que desarrollamos con estos tres grupos de asesoramientos son planes de trabajo; todos los años realizamos un plan con actividades específicas, como desarrollar conjuntamente documentos, desarrollar soluciones, campañas de prevención o, en algunos casos, apoyar de manera operativa. Ha demostrado ser una buena herramienta de trabajo y hemos alcanzado con algunos de ellos un elevado nivel de confianza; la confianza es una de las palabras clave en cuestiones de colaboración internacional y a nivel de colaboración policial también lo es.

Podemos tener las mejores herramientas de intercambio de información, pero si no existe confianza entre los socios no las van a utilizar, hace falta generar esta confianza a través del conocimiento de los socios. Ese fue el objetivo que planteamos cuando empezamos esta iniciativa, que es única a nivel mundial. Es un grupo de ciberespecialistas de distintos Estados miembros y terceras partes que trabajan juntos en Europol no solo representando a los Estados miembros, sino trabajando como un equipo. No existe un grupo como este a nivel mundial en el que estén representados todos los países relevantes en la lucha contra la ciberdelincuencia y ha demostrado ser un mecanismo muy positivo a la hora de desarrollar investigaciones. De hecho, hay iniciativas para replicar este modelo en otras áreas, como en el área de inmigración ilegal o terrorismo. Nosotros llevamos operando con ellos cuatro años y me atrevería a decir que hay pocas o ninguna gran investigación a nivel internacional, a nivel global, cuando estamos hablando de tumbar grandes *botnets* o grandes campañas de *ransomware*, que estén fuera de la coordinación de este grupo. España está representada por dos fuerzas de seguridad: Policía Nacional y Guardia Civil.

Voy a mostrar algunas de las investigaciones y de las iniciativas que hemos desarrollado recientemente en las tres áreas relacionadas con nuestro mandato. La primera área de nuestro mandato, como ven en la presentación y que he citado al iniciar la presentación, los ataques, ciberataques contra infraestructuras, sistemas de información y que conllevan muchos de tipos de delincuencia. Hay algo que quisiera destacar en relación con este tipo de criminalidad, el concepto de crimen como servicio. Para ser un ciberdelincuente hay quien piensa que hace falta tener unos conocimientos muy sofisticados, muy elevados, grandes conocimientos informáticos, y eso no es cierto. Hoy en día para llevar a cabo actividades criminales dentro de lo considerado ciberdelincuencia basta con buscar los servicios criminales que otros delincuentes ofrecen. Un ejemplo de este tipo de crimen como servicio es el desarrollo de ataques en acción de servicio. Este tipo de ataques son realizados cuando una gran cantidad de usuarios quieren acceder al mismo servicio *online*. Se crea un cuello de botella y este servicio no puede dar una respuesta. Por lo tanto, cuando los usuarios legítimos intentan acceder, se quedan en la cola y nunca acceden. De esta manera se puede tumbar una página web u otro de tipo de servicios *online*. Es un ataque muy común que puede ser desarrollado a través de un gran *botnet*, si tienes un *botnet* controlas muchos equipos o dispositivos y cuando les ordenas a todos acceder a un mismo recurso *online* lo saturas y se cae el servicio. Si alguien quiere atacar un recurso concreto o una página *online* no hace falta que disponga de un gran *botnet* o de un control de dispositivos, basta con acudir a un servicio de ataques DDOS y contrata el ataque. Pagando una pequeña cantidad, 15 dólares, se puede atacar una página web, el precio varía dependiendo del tipo y la intensidad del ataque, con ese ataque esa página es tumbada. Se ofrece como un servicio criminal a otros criminales. Es una muestra de crimen como servicio a otros criminales.

Hemos desarrollado recientemente una investigación con la Policía holandesa, en colaboración con otras agencias policiales, en la que conseguimos identificar a los administradores y desmantelar la infraestructura del principal servicio de ataque DDOS que había *online*. Cuando buscaba alguien a través de los servicios que hay en internet, en cualquier buscador, ataque DDOS o facilitador de ataques DDOS era el primero que salía. Fue una investigación coordinada por la Policía holandesa y conseguimos identificar al administrador y tumbar la infraestructura y se subió esta página informando a quien quisiera acceder de la intervención de este servicio por las autoridades policiales.

Vimos el año pasado dos grandes ataques a nivel internacional: WannaCry y NotPetya. En Europol quisimos dar una respuesta lo más rápida y ágil posible a nuestros socios, a las autoridades policiales. Creemos, eso nos dijeron, que hicimos un buen trabajo, pero, aun así, hicimos una valoración de nuestra respuesta, cómo lo hicimos, qué hicimos bien, qué hicimos mal.

Hicimos una valoración y vimos que muchas de estas cuestiones eran mejorables, con lo cual, lanzamos una iniciativa, que expusimos en colaboración con el trío de Presidencia —Estonia, Bulgaria y

cve: DSCG-12-CM-124

Austria—, para crear un protocolo de respuesta policial de emergencia en el caso de este tipo de ataques, para que cuando ocurra, y volverá a ocurrir —esperemos que más tarde que pronto—, estemos mejor preparados a nivel policial, para saber cómo intercambiar la información policial —y reitero lo de policial— cuando esto esté ocurriendo. Todos estos ciberataques son actividades criminales. Por lo tanto, la Policía, desde un primer momento, tiene que estar involucrada en la coordinación de la respuesta. Este protocolo europeo ha sido recientemente aprobado por el Cosic, que facilita también la colaboración con el sector privado. Uno de los principales problemas que vimos cuando coordinamos nuestra respuesta con WannaCry y NotPetya fue que nuestros socios del sector privado nos dijeron que habían recibido muchas peticiones de muchos países preguntando qué sabíamos de esto o cómo les podíamos ayudar. A través de este protocolo, nosotros coordinamos esta información, garantizamos que el flujo se dirija a todas las autoridades competentes de los países y exista un flujo rápido de información y limpiamos todo el ruido que hay, porque cuando ocurren estos ciberataques hay mucho ruido y se genera mucha información que no es relevante o que no es precisa. Nuestra función es limpiar toda esa información y facilitar la información precisa lo más rápido posible para dar una respuesta adecuada. Y este protocolo se incardina dentro de otros protocolos a nivel europeo relacionados con la ciberseguridad. Nosotros nos centramos en la respuesta policial y en cuál va a ser la contribución policial a estos protocolos europeos.

Delitos relacionados con fraude en línea, como he dicho anteriormente, fraudes con o sin tarjeta. Una muestra de alguna de las iniciativas que desarrollamos desde hace algunos años es los Días de acción contra el fraude en el sector de las aerolíneas. Básicamente, vimos que había una gran cantidad de fraude en relación con la compra de billetes de avión y no se estaba haciendo mucho. Por tanto, nos pusimos en contacto con las operadoras, con los bancos y con los emisores de tarjeta para ver cómo se podía abordar este fenómeno. Desarrollamos un protocolo de comunicación que, en cuanto las turoperadoras o las agencias de las aerolíneas detectan la compra, presuntamente, fraudulenta de billetes de avión, lo comunican al sector bancario, a los emisores de tarjeta, los cuales confirman si la compra ha sido o no fraudulenta y puedan decir: Efectivamente, mi cliente no ha comprado este billete, con lo cual, esta es una compra fraudulenta. Esa información se transmite de manera rápida a la Policía, que está desplegada en los aeropuertos esperando a la persona que va a utilizar el billete de avión comprado de forma fraudulenta. Esa persona es interrogada, se puede registrar su equipaje y, dependiendo de las circunstancias, puede ser hasta detenida. La última operación de este tipo fue desarrollada en junio de este año. Durante una semana, participaron 226 aeropuertos a nivel mundial. Es un dispositivo global, en el que tenemos centros de coordinación en Europa, que los coordinamos en nuestro centro de control de La Haya con centros de Estados Unidos, Canadá, con el de Ameripol para Latinoamérica e Interpol en el área asiática. Al final, se realizaron 141 detenciones y, a lo largo de los años, hemos visto cómo, a través de esta iniciativa —así nos lo han comunicado las aerolíneas—, ha habido un descenso en la compra fraudulenta de billetes de avión.

Otra muestra de colaboración dentro de los fraudes *online* es lo que llamamos la acción europea contra las mulas. La mula es un intermediario dentro del camino criminal, que recibe el efectivo a través de una transacción fraudulenta y lo manda a otros criminales. Es un elemento necesario dentro de este camino de la ciberdelincuencia. Hace un par de años, empezamos una acción pequeña con algunos países para tratar de abordar esta criminalidad en colaboración con los bancos. Los bancos, al igual que las aerolíneas, tienen sus mecanismos para detectar transacciones que, presuntamente, son fraudulentas o pueden estar dirigidas a unas mulas. Esta información se facilita a las agencias policiales, y estas la elaboran y la investigan para, en un momento dado, realizar las intervenciones o las investigaciones. En este caso, es una iniciativa que hemos desarrollado durante un periodo de tres meses, en el que las autoridades competentes han realizado investigaciones, y a lo largo de esos tres meses se han identificado más de 1500 mulas, 140 organizadores, gente que controla a otras mulas, y se han producido 168 detenciones.

Junto con estas acciones operativas, siempre buscamos la posibilidad de realizar campañas de prevención. La prevención es un aspecto fundamental en la lucha contra la ciberdelincuencia y puede estar dirigida bien a potenciales víctimas o bien a potenciales criminales. Ser una mula es ofertado como un trabajo, como un trabajo falso, y hay gente que incluso puede pensar que es un trabajo legítimo. Vemos que son estudiantes o gente que puede pensar que es una forma legítima de obtener dinero. Les informamos acerca de que es una actividad criminal, de las consecuencias que conlleva y de las actividades policiales en este sentido.

cve: DSCG-12-CM-124

La acción coordinada contra el uso de la criminalidad en la *dark web*. En Europol llevamos coordinando investigaciones contra el uso criminal en la *dark web* desde hace bastante tiempo, especialmente en el área de abuso sexual de menores, a la cual me voy a referir posteriormente. La *dark web* es una red dentro de internet creada básicamente para hacer a sus usuarios y sus contenidos anónimos. Los elementos que tradicionalmente utilizamos para identificar a estos usuarios, como son las direcciones IP dentro de la *dark web*, no son válidos para hacer una investigación. Básicamente no sabemos quiénes son, no sabemos dónde están alojados estos contenidos, lo cual es un terreno perfecto para los cibercriminales para alojar contenidos y para alojar páginas web en las que se intercambian todo tipo de sustancias ilegales. Alphabay era una de las principales, era una especie de mercado *online* donde se podía acceder y encontrar cualquier tipo de contenido criminal. Se podían vender armas de fuego, se podían vender drogas, se podían vender herramientas de *malware.* Cualquier tipo de actividad criminal. Solo había que buscar lo que uno necesitaba y comprarlo, y los pagos se realizaban a través de una criptomoneda, lo que también nos dificultaba mucho las investigaciones policiales, porque era casi imposible identificar quiénes eran, tanto los vendedores como los compradores. Y Hansa era otro de los grandes mercados que facilitaban el intercambio de todo tipo de sustancias ilegales.

A través de una acción coordinada, el año pasado conseguimos identificar a los administradores y tumbar la infraestructura de estos dos grandes mercados en la *dark web*. Fue una acción coordinada en la que el FBI básicamente tumbó una de estas páginas web, lo cual creó una gran confusión dentro de este entorno criminal porque no dijeron nada; nadie sabía qué había pasado. Los criminales pensaban que el administrador había huido con los beneficios, y como digo, eso creó una gran confusión. ¿Y qué ocurrió? Que muchos de estos criminales fueron al siguiente mercado, que era Hansa, y Hansa estaba entonces controlado por la Policía holandesa, que tenía monitorizado y controlado este mercado, con lo cual empezó a ver quiénes eran todos esos usuarios que llegaban y a recopilar información sobre este tipo de actividad criminal, y al cabo de unas semanas se cerró. Con esta información se trababa de identificar tanto a los vendedores, como a los compradores, y en las páginas web en las que estaban alojados se subió un mensaje que decía que dichas páginas habían sido intervenidas por las autoridades policiales. Y ello envió un fuerte mensaje a los criminales, que pensaban que las autoridades policiales no tenían ni el conocimiento ni la coordinación ni la estrategia para realizar este tipo de operaciones.

Toda esta coordinación se llevó a cabo a través de Europol, que celebró diversas reuniones y conferencias semanales para coordinar estas acciones. Y este es el tipo de apoyo que nosotros prestamos. Estas dos operaciones por sí solas hubieran sido grandes operaciones; combinadas dieron lugar a una con un impacto mucho mayor. Y eso es lo que tenemos que buscar a nivel estratégico.

Abuso sexual de menores. Los abusadores sexuales de menores también llevan utilizando la *dark web* durante mucho tiempo. Es un entorno perfecto para ellos, para encontrar otros abusadores con los que hablar e intercambiar las imágenes y videos que producen. Dentro de estos foros en la *dark web* en la que ellos se sienten anónimos, los administradores crean una zona vip, y para entrar a esas zonas tienes que demostrar que eres un abusador y que tienes acceso a niños, es decir, tienes que demostrar que puedes producir material, con lo cual para entrar tienes que mandar al administrador ese material: fotografías de los niños siendo abusados y violados. Entonces, el administrador lo ve; ve que eso ha sido producido para ese grupo y te da el acceso a la zona vip, donde te relacionas con otros abusadores con acceso a niños. Pero, además, para mantenerte en esa zona vip tienes que subir material todos los meses; de lo contrario, te echan. Ese es el tipo de gente con la que tratamos. Y no estamos hablando de un pequeño grupo. Este en concreto es un servicio que fue tumbado en el marco de una operación que coordinamos, y tenía 80 000 usuarios registrados. No todos estaban en la zona vip, pero, insisto, tenía 80 000 usuarios registrados. Y este tipo de servicios no es algo que encuentras si no lo estás buscando; no es algo que puedas encontrar por casualidad en internet. Tienes que saber lo que estás buscando y registrarte. ¿Qué ocurre cuando conseguimos, a pesar de las dificultades, identificar a los administradores e intervenir todo el material que está en estos servicios? Pues que accedemos a una gran cantidad de material de abuso sexual de menores, fotografías y vídeos nuevos que no han sido analizados nunca por la comunidad policial internacional. Y material nuevo quiere decir abuso que ha tenido lugar recientemente, es decir, no es material histórico que lleva circulando por internet durante años. Son abusos que pueden estar siendo cometidos en cualquier lugar del mundo, con lo cual tenemos la obligación y la responsabilidad de examinar este material lo antes posible. Para eso organizamos lo que llamamos fuerzas de identificación de víctimas. Es algo que llevamos haciendo en Europol durante un tiempo. Básicamente reunimos en la organización a los mejores investigadores especialistas en

cve: DSCG-12-CM-124

identificación de víctimas a nivel mundial y durante un periodo de dos semanas analizamos, con el uso de la mejor tecnología disponible —lo cual es necesario para facilitar el gran volumen de material que tenemos—, elementos que nos ayuden, en primer lugar, a identificar el lugar de origen, es decir, dónde está siendo cometido este abuso, dónde está este niño o dónde está este abusador. Si lo logramos, creamos un paquete de inteligencia con todas las pistas y con todos los elementos de que disponemos y lo mandamos a ese país. Si creemos que es en Alemania le mandamos un paquete y la policía alemana abre una investigación para saber por qué está en su país. Lo mismo si ocurre en cualquier lugar del mundo, mandamos un paquete de inteligencia para que abran la investigación.

Este año hemos realizado la quinta *taskforce* de identificación de víctimas. En relación con esta actividad, hemos conseguido identificar y rescatar a 241 víctimas, lo cual es un número elevadísimo. Aun así, estamos lejos de estar satisfechos porque existe una gran cantidad de *backlog*, de material que todavía está pendiente de ser analizado por las agencias policiales. Hay mucho más de lo que tenemos capacidad de analizar, no solo Europol, sino que cualquier agencia policial del mundo tiene el mismo problema. Hay mucho más. Hay pocos especialistas en abuso sexual de menores e identificación de víctimas. Es una especialidad compleja y requiere mucha más inversión y mucha más colaboración para analizar estas identificaciones.

¿Qué ocurre cuando a pesar de nuestros esfuerzos tenemos una serie de imágenes y de vídeos en los que vemos a niños siendo abusados y no tenemos elementos que identificar, ni siquiera el país donde eso sucede? Pues después de mucho debate decidimos lanzar una iniciativa para pedir el apoyo del público. Básicamente, lo que hacemos es extraer objetos, piezas de estas imágenes y de estos vídeos y las subimos a nuestra página web y pedimos a la gente que nos ayude por si reconocen algún objeto, alguna marca o el entorno y si saben dónde puede estar. Lo llevamos haciendo un año y la respuesta del público ha sido excelente. Hemos recibido más de 20 000 indicios de gente diciendo que eso era en su país o que eso se vende en su región o que conocen esa marca, y eso nos ayuda a centrar los esfuerzos. En algunos casos lleva hasta una localización directa, como este, donde se ve una habitación de hotel y preguntamos si alguien sabía dónde era. El mismo día recibimos una fotografía diciendo que era una habitación de un hotel en Taiwán. Entonces, cogemos esa información, realizamos un paquete de inteligencia y lo mandamos a las autoridades taiwanesas para que abran una investigación y saber por qué ese abuso ha sido cometido en ese país. Dentro de nuestra página web actualizamos los objetos de manera habitual y, a través de esta iniciativa —tenemos varios números, como pueden ver en la presentación, y es mucho trabajo analizar todas las pistas recibidas— hasta ahora hemos conseguido identificar a ocho víctimas que, de otra manera, no habrían sido identificadas y rescatadas, con lo cual, desde nuestro punto de vista, la iniciativa tiene éxito y seguiremos invirtiendo nuestros esfuerzos en ella.

Por último, respecto a las actividades relacionadas con la prevención, como he dicho, ante cualquier investigación y cualquier iniciativa siempre nos planteamos desde el punto de vista de la prevención qué podemos hacer. No More Ransom es una iniciativa que desarrollamos junto con el sector privado y básicamente pretende ofrecer soluciones a las víctimas de *ramsomware.* Cuando un usuario ha sido víctima y sus archivos han sido encriptados tiene dos opciones: perderlos o pagar al criminal y esperar que le mande la clave para recuperar su archivo, lo cual rara vez ocurre. A través de esta iniciativa, con la colaboración del sector privado, tenemos herramientas que los usuarios se pueden descargar, primero, para limpiar sus equipos y, segundo, para tratar de desencriptar estos archivos. A través de las investigaciones que coordinamos accedemos a claves de desencriptación que subimos a la plataforma y puede ser que ayuden a las víctimas a recuperar sus archivos. Es una iniciativa que ha dado muy buen resultado. Tenemos una gran cantidad de socios del sector privado asociados a esta iniciativa y sigue creciendo.

Del mismo modo, tenemos iniciativas dirigidas al abuso sexual de menores para orientarles sobre los peligros que pueden tener cuando interactúan de manera *online* y ciertas medidas de seguridad que deben implementar. También hay consejos de seguridad en relación con el *malware* para dispositivos móviles y otros consejos.

Básicamente, esta es mi presentación. Si tuviera que resumir cómo se puede afrontar la ciberdelincuencia con cierto éxito, el único camino es a través de la continua colaboración de todos los actores involucrados. No solo son las autoridades policiales las que tienen que ocuparse de ello, hace falta una colaboración muy estrecha y muy fluida con el sector privado, con la academia, con otras entidades, con todo aquel que tenga algo con lo que contribuir en esta lucha. En este sentido, estamos desarrollando nuestra estrategia y nuestras iniciativas.

Eso es todo por mi parte.

cve: DSCG-12-CM-124

El señor **PRESIDENTE:** Muchas gracias.

Me comunican que los grupos han llegado a un acuerdo para que intervenga en primer lugar la representante del Grupo Popular.

Señora Vázquez, tiene la palabra.

La señora **VÁZQUEZ BLANCO:** Gracias, señor presidente.

Agradezco a los grupos que me haya permitido intervenir en primer lugar para poder realizar un viaje parlamentario. Yo lo hablé con dos, no sé si alguno más faltaba. Discúlpenme. Si hay algún problema, lo siento.

Agradezco al compareciente la brillante exposición que acaba de realizar, sin lugar a dudas, muy práctica y muy interesante. Entre las últimas comparecencias que hemos escuchado, esta es de las mejores, sobre todo, desde el punto de vista práctico.

Simplemente, quiero felicitarle, en primer lugar, en nombre del Grupo Parlamentario Popular, por el trabajo que están desarrollando y más en un mundo tan complejo como es el del ciberespacio, que no entiende de fronteras, no entiende de nombres y en el que es tan difícil, tal como usted nos ha explicado, dar con los auténticos autores, los ciberdelincuentes.

Le voy a formular una serie de preguntas y, si me permite, después leeré sus contestaciones, como le he dicho anteriormente, en el *Diario de Sesiones,* por lo que le pido disculpas de antemano.

¿Qué medidas operativas y de coordinación se están discutiendo actualmente para mejorar la ciberseguridad en dos sectores, en concreto, el sanitario y el de la automoción? ¿Considera adecuada la respuesta que se está dando para mejorar la ciberseguridad de estos dos sectores? Me refiero al sanitario, porque recuerdo cómo el WannaCry, en el mes de mayo, afectó al Reino Unido, sobre todo en el ámbito sanitario. ¿En qué situación se encuentra el desarrollo de taxonomías comunes para todos los cuerpos policiales en materia de lucha contra la ciberdelincuencia? ¿Cómo valora los programas europeos de gamificación para la detección de talento en materia de ciberseguridad? ¿Nos puede comentar alguna experiencia que usted considere positiva y que se pueda aplicar en nuestro país? Nosotros hemos hablado muchas veces aquí de la creación de una ciberreserva o la figura del cibercooperante. Hay otros países en los que para la detección del talento se utilizan otras formas. Me gustaría que nos contara algo al respecto. ¿Se está trabajando en la generación de equipos pluridisciplinares, no estrictamente técnicos, para combatir eficientemente el cibercrimen en la Unión Europea? ¿Podría trasladarnos alguna experiencia relevante que fuera de especial conocimiento para nosotros para mejorar nuestro país? ¿Cómo valora los códigos de intercambio de información respecto a las distintas fuerzas y cuerpos policiales que hay dentro de Europol? ¿Propondría alguna mejora respecto a esa coordinación? ¿Puede valorar el impacto de la nueva regulación del ICANN en cuanto al acceso de datos de los dominios registrados en materia de investigación de los ciberdelitos? ¿Qué nos puede aconsejar respecto a esto para la trazabilidad en la transferencia de los antedichos dominios?

Agradezco a los compañeros que me hayan permitido intervenir en primer lugar y cuando ellos tengan también un problema, lo resolveremos. Voy con una comisión del Congreso y del Senado a Azerbaiyán, de jóvenes parlamentarios, y entre los temas que se van a tratar hay uno de ciberseguridad. Por eso voy allí.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, buen viaje.

Tiene la palabra el señor Yanguas.

El señor **YANGUAS FERNÁNDEZ:** Muchas gracias, señor presidente.

Quiero darle la bienvenida a esta comisión, señor Ruiz Pérez, y agradecerle su amplia y clara explicación. La verdad es que a mí me ha aclarado bastantes cosas y en su última explicación incluso me han impresionado algunas de las que ha dicho y que yo desconocía.

Se me ha ocurrido alguna pregunta al hilo de su intervención. No sé si lo ha dicho, pero ¿cuántas personas trabajan en Europol directamente relacionadas con el ciberdelito? ¿Ustedes actúan o pueden actuar como expertos o como peritos en juicios? Porque veo que tienen un *expertise* impresionante. No sé si hay alguna recomendación más que tenga que dar a España. Usted ha hablado de más inversión, desde luego de más profesionales —también es cierto— y al final ha terminado hablando de la colaboración que, como usted, creo que es importante. ¿Tiene alguna recomendación más? **(El señor vicepresidente, Jiménez Tortosa, ocupa la Presidencia).** Le animo a seguir trabajando con la excelencia que nos ha mostrado. Ha sido usted muy claro y muy conciso.

Muchas gracias.

cve: DSCG-12-CM-124

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Gracias, señor Yanguas.

Tiene la palabra el señor Castellana.

El señor **CASTELLANA GAMISANS:** Muchas gracias.

Le felicito por la cantidad de información categorizada y bien identificada de su presentación. Seguramente profundizar en el tema nos daría para muchas sesiones como esta, pero yo probaré con tres preguntas muy concretas que nos pueden dar más pistas.

En primer lugar, ha hablado de un seguimiento a la *internet governance*, y querría saber, en relación con su trabajo y con este seguimiento, si tiene propuestas que mejoren la seguridad de los usuarios a la vez que faciliten la persecución del cibercrimen y de los cibercriminales. En segundo lugar, ¿qué magnitud más o menos estimada tienen los grupos criminales, teniendo en cuenta que son grupos transnacionales? Ha hablado de las grandes *botnets*, lo digo para hacernos una idea de la magnitud de los enemigos a los que nos enfrentamos, y su conexión con otras fórmulas más clásicas de criminalidad. Y finalmente, cuando ha hablado del crimen como servicio, teniendo en cuenta que ha habido ataques por parte de potencias extranjeras a organismos internacionales denunciadas por algunos Estados y que hay una alta competición, para decirlo de una manera muy suave, entre estas potencias, querría saber si han detectado la externalización de servicios de agencias de ciberdefensa de potencias equis con esas redes de crimen como servicio.

Muchas gracias.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, señor Castellana.

¿Por el Grupo Ciudadanos? **(Pausa).**

Por el Grupo Confederal Unidos Podemos-En Comú Podem-En Marea, tiene la palabra el señor Comorera.

El señor **COMORERA ESTARELLAS:** Muchas gracias. Muchas gracias, señor Ruiz Pérez, por su exposición.

Voy a confesarles a los demás miembros de la comisión que ya tenía el gusto de conocerle porque, como miembro de la Asamblea Parlamentaria de Control de Europol, estuve visitando con la delegación española la sede de Europol. Aunque no lo ha dicho usted, lo diré yo: me llevé una grata sorpresa al comprobar que el personal español es el segundo en número dentro de Europol y que está muy pero que muy bien valorado. No lo ha dicho usted, lo digo yo.

Uno de los problemas que ha expresado usted, tanto aquí como en alguna entrevista suya que he leído, es, cómo no, la *dark web*, más que nada porque no se puede controlar. Siendo imposible de controlar, ¿cómo cree usted que desde el ámbito legislativo podríamos limitar, dentro de lo posible, ese descontrol? Si es posible a través de determinadas medidas que pudiéramos darle a Europol o a las policías nacionales para limitar ese peligro, dado que somos conscientes de que el patrullaje activo dentro de un mundo inabarcable como este es prácticamente imposible.

Otro de los problemas crecientes va a ser el internet de las cosas. Usted ha dicho que lo peor está por venir todavía. Sobre todo con la llegada del 5G vamos a tener una menor latencia que permitirá utilizar prácticamente cualquier aparato a distancia por internet, desde coches, lavadoras, cualquier electrodoméstico. A este respecto —creo que usted lo ha dicho en alguna de sus intervenciones—, vemos que no tenemos ninguna regulación para que los fabricantes de elementos informáticos impidan o hagan más difíciles las instrucciones. Y la pregunta es: ¿Cree que deberíamos legislar con urgencia respecto a esas instrucciones?

En relación con este mismo tema, le preguntaría cómo llevan ustedes la colaboración con el sector privado. Ha dicho que sí tienen colaboración, pero la pregunta es si tendría que ser mejor o si es suficiente la que hay.

Otro problema evidente con el que se encuentran es el de la transversalidad de los delitos al utilizar las nuevas tecnologías, su internacionalización o la colaboración entre las partes y la dificultad de tener que solicitar información a empresas tecnológicas, sobre todo, radicadas en el extranjero. Con el marco legal que tenemos actualmente, tanto a nivel legislativo español como a nivel comunitario, ¿cree que es suficiente para hacer su trabajo o necesitaríamos dar algún paso más? **(El señor presidente ocupa la Presidencia).**

Desde el punto de vista legislativo, lo normal es que vayamos tarde en relación con los avances de la tecnología. Y uno de los temas que también preocupa es la escasez de regulación en lo que se refiere a

cve: DSCG-12-CM-124

las criptomonedas, lo que imagino que es un hándicap importante en sus investigaciones: Los ICO, el *cryptojacking*, los que surgen cada día y los que posiblemente surgirán mañana. Le pregunto si legislativamente tendríamos que regular esta cuestión.

Y para acabar, ayer mismo, el director del Centro Nacional de Inteligencia, el general Félix Sanz Roldán, desveló que cada día se detectan dos o tres ciberataques en España de peligrosidad muy alta para los intereses del país. Y manifestó que sus autores son con frecuencia otros Estados, pidiendo medidas legislativas para frenar a los responsables de los ciberataques. Mi pregunta es si ha detectado usted ciberataques por parte de algún Estado.

Le agradezco de nuevo su magnífica exposición. Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, senador Comorera.

Tiene la palabra el señor Álvarez.

El señor **ÁLVAREZ VILLAZÁN:** Muchas gracias, señor presidente.

Para empezar, quiero agradecerle la magnífica y clara exposición que nos ha realizado de toda la problemática que estamos tratando. Asimismo, quiero manifestarle mi preocupación porque, de todo lo que usted ha expuesto y dado el malestar que podríamos tener por todos estos problemas, no me queda la tranquilidad de saber que se está haciendo todo lo que se debería. En ese sentido, mi pregunta fundamental, que le planteo al principio, es si cree usted que se está haciendo todo lo posible y necesario para avanzar en esta cuestión.

Es evidente que las amenazas *online* se vienen detectando desde hace tiempo como complejas y problemáticas y que, a medida que pasa el tiempo, se han incrementado. Por eso mismo, desde que en 2013 la Comisión Europea crea el Centro Europeo contra el Cibercrimen, hemos visto una serie de medidas que usted ha señalado aquí perfectamente, indicando cuál es el organigrama, cuáles son los objetivos o qué es lo que pretenden; así, detener todas esas acciones delictivas como son las estafas *online*, los negocios fraudulentos y otro tipo de delitos, persiguiendo los delitos que causen perjuicio a la víctima, como son los delitos de explotación sexual y pornografía infantil. Me ha parecido realmente importante, interesante y digno de elogio que le hayan dado la importancia que usted ha señalado que se le está dando. O las acciones para prevenir los ataques a infraestructuras y sistemas de información críticos, que pueden afectar a instalaciones vitales para un país o para sectores importantes de la población.

Por su exposición, por su exposición y por lo que podemos leer en los medios de comunicación, me queda la impresión de que nos estamos enfrentando a grupos muy organizados, que hemos abandonado ya la idea del *hacker* que se encerraba en su habitación y que era muy difícil de localizar porque era una persona anónima, solitaria, y que estamos hablando de grupos muy organizados, con unos fines lucrativos muy importantes y muy difíciles, muy difíciles de combatir. Estamos hablando de grupos terroristas, de grupos criminales, y la preocupación es si realmente estos grupos no nos están ganando en velocidad o en rapidez de innovación —no sé cómo llamarlo—; es decir, me queda la duda de si las instituciones públicas, los países y todos los organismos que están dedicados a combatirlos no estamos yendo siempre un poquito por detrás, de forma, que en vez de prevenir, sencillamente actuamos ya para intentar evitar el daño, pero cuando el daño se ha producido. Es la duda que tengo.

También me preocupa la colaboración. Creo que fue a finales de 2017 cuando el vicepresidente responsable del Mercado Único Digital hacía unas declaraciones en las que resaltaba que ningún país puede hacer frente por sí solo a los retos de ciberseguridad —usted lo ha señalado también—, pero, claro, yo creo que volvemos a hablar del mismo problema: que sigue sin existir esa colaboración decidida, sincera de todos los países para evitarlo.

Que algo no ha ido bien desde 2013 lo prueba que en 2017 la misma Comisión Europea propone al Parlamento y al Consejo de Europa otro conjunto de medidas, de numerosas medidas en materia de seguridad, probablemente porque percibe lo que todos estamos percibiendo: que estos ataques se van incrementando, que surgen nuevos riesgos, que no nos adelantamos a detectar estos nuevos riesgos y que los delitos cada vez son mayores y más diversos. En ese sentido, vemos cómo se aprueba la estrategia del Mercado Único Digital en 2015 o en 2016 —no lo recuerdo bien ahora—; se aprueba la Agencia Europea de Seguridad, que no sé exactamente si está en pleno funcionamiento en estos momentos o todavía no; también se adopta una comunicación para el refuerzo del sistema de ciberseguridad en Europa y se reclaman nuevos instrumentos legislativos —creo que ha sido el portavoz

cve: DSCG-12-CM-124

de Podemos, que me ha precedido en el uso de la palabra, quien ha señalado la necesidad de nuevos instrumentos legislativos—.

Pero con todas estas medidas hemos visto los incidentes tan graves de seguridad que usted ha señalado también, los ataques híbridos o las campañas cibernéticas ofensivas contra determinados intereses de países desde otros países fuera de la Unión Europea, con lo cual le vuelvo a señalar otra vez la preocupación de si realmente estas medidas están siendo lo suficientemente eficaces que deberían ser. No sabemos si estas medidas están sirviendo para afrontar la progresión de la ciberdelincuencia en la comisión de delitos o actos terroristas, o si se están afrontando adecuadamente con estas medidas los retos que plantean —también se ha señalado aquí por algún otro portavoz antes de mí— el internet de las cosas, la digitalización de la industria, la industria 4.0 o la economía digital de los datos.

Todos manifestamos nuestra preocupación en materia de ciberseguridad, pero vemos que hay unos vacíos operativos o jurídicos que plantean las nuevas tecnologías y vemos que la eficacia de las medidas de acciones no legislativas que se están adoptando quizá es limitada. Cito también al presidente de la Comisión Europea que, a finales de 2018, en el discurso sobre el estado de la Unión, decía: Europa sigue sin estar adecuadamente equipada para defenderse de los ciberataques. Y el comisario de Seguridad de la Unión Europea añadía poco después: Hemos subestimado la escala del cibercrimen. Y añado a estas declaraciones de alarma unas de usted, creo que de marzo de 2018 —se han señalado también aquí—, en las que decía: Con el 5G los ataques informáticos serán mucho más peligrosos.

Ante todo esto, le vuelvo a reiterar mi pregunta inicial: si realmente, según su criterio, faltan medidas legislativas para afrontarlo, faltan medidas operativas o si no cree que la superposición o proliferación de todas estas iniciativas que ha habido en la Unión Europea están dispersando la atención, los recursos y las prioridades que debería haber para actuar contra la ciberdelincuencia.

Termino manifestando también otra preocupación —llevo toda mi intervención preocupándome— por informaciones que veía en prensa en las que parece que España está a la cabeza del cibercrimen y sobre las dudas que generaba también si las leyes actuales —me parece que me reitero—, la legislación actual, está siendo lo suficientemente efectiva para ello.

Sin más, agradeciéndole vez más su exposición, creo que ya he intervenido suficiente. ¿No, señor presidente?

Muchas gracias.

El señor **PRESIDENTE:** Me ha parecido muy bien. Gracias, señoría.

Señor Ruiz Pérez, tiene usted la palabra.

El señor **RUIZ PÉREZ** (responsable de operaciones del Centro Europeo del Cibercrimen (EC3) de Europol): Voy a ver si consigo dar respuesta a todas las preguntas.

Para empezar —porque es algo común y puedo contestar a muchas de las preguntas—, la ciberseguridad y la lucha contra la ciberdelincuencia es algo complejo porque intervienen muchos actores. Tenemos varias esferas: la ciberseguridad, la cibercriminalidad y la ciberdefensa. Vemos que estas esferas cada vez se están acercando más, hay muchos elementos comunes, con lo cual lo primero que hay que hacer es conseguir que todos los actores involucrados, en vez de actuar de forma aislada, aúnen esfuerzos. Algunas de las preguntas iban en ese sentido y lo desarrollaré a continuación.

La primera pregunta, ciberseguridad en el sector sanitario y automoción —en relación con el ataque de WannaCry que vimos el año pasado—. Es cierto que algunos sectores están mejor preparados para hacer frente a ciberataques; por ejemplo, el sector bancario está bastante bien preparado porque desde hace tiempo sabe que es una gran amenaza y son un objetivo, con lo cual están mejor preparados para una respuesta y para prevenir estos ataques.

El sector sanitario, como vimos en Reino Unido y por eso tuvo un gran efecto WannaCry, estaba muy desfasado, tanto los sistemas de seguridad como los sistemas informáticos que tenían no estaban actualizados, básicamente, y no porque la vulnerabilidad que utilizó WannaCry no fuera conocida, sí era conocida y fue publicada, así como la actualización, el parche para solventarla, que estaba publicada hacía meses. ¿Qué ocurre? Que en estas grandes infraestructuras, como el sector sanitario, si no hay una inversión suficiente no hay una capacidad de actualizar toda esa infraestructura y parchear estas vulnerabilidades tan pronto son publicadas; esperan un tiempo, acumulan parches y luego consiguen actualizar. Esto no ocurrió en Reino Unido, había una gran vulnerabilidad que, a pesar de ser conocida, no había sido parcheada y por eso el ataque que se originó en un punto concreto se pudo distribuir y tuvo un gran impacto.

cve: DSCG-12-CM-124

Yo creo que tanto el sector sanitario como cualquier otro sector han tomado nota de la necesidad de estar actualizados, de considerar la ciberseguridad y la seguridad de sus sistemas como una prioridad, y especialmente el sector sanitario no solo por el efecto que pueden tener estos ciberataques en la dejación de sus servicios —en Reino Unido casi se tuvieron que cerrar hospitales, se dejaron de realizar operaciones—, sino porque los datos sanitarios son un objetivo también para los cibercriminales; los datos personales que tienen las entidades sanitarias son un objetivo que tienen un valor y esos objetivos también tienen que protegerlos adecuadamente. Lo mismo pasa con la automoción.

La siguiente pregunta estaba relacionada con la taxonomía. Existen muchas taxonomías, similares pero distintas. Desde el punto de vista policial, y esto es algo que quiero dejar claro desde el principio, mi respuesta es una respuesta desde el punto de vista de la cibercriminalidad. Podría haber otras respuestas si quien se sentara en este lugar fuera alguien representando la esfera de la ciberseguridad; la mía es una visión policial. Desde el punto de vista policial, tratamos de solventar este problema creando una taxonomía común junto con la Agencia Europea de Seguridad de las Redes y de la Información, Enisa, que ahora se está reconvirtiendo en la Agencia Europea de Ciberseguridad, fijando una taxonomía común tanto para la policía como para los centros de seguridad, que está vigente y la única cuestión es cómo es utilizada y cómo es implementada. Pero, efectivamente, hay muchas taxonomías y en un momento dado esto puede ser una dificultad.

Respecto a la búsqueda de talento para cuestiones relacionadas con la ciberseguridad, hay iniciativas a nivel europeo: Enisa realiza una serie de concursos, de desafíos, a los que se pueden presentar talentos; si vemos que estos talentos responden positivamente, que es gente con grandes capacidades, se trata de promoverlos. Esto lo hace Enisa, no lo hace Europol. En relación con el talento, lo que trato de hacer por mi parte, desde luego, es contratar a los mejores cuando intentan entrar en Europol; tenemos unos procedimientos de selección muy duros, se reciben muchas aplicaciones para los puestos que ofertamos y, básicamente, tratamos de reclutar a los mejores. Por eso tenemos a los mejores especialistas, como mínimo a nivel europeo, en algunas áreas, porque han demostrado ser los mejores dentro de su área.

Equipos multidisciplinares. Efectivamente, tal y como he dicho en mi presentación, es algo necesario. La lucha contra la ciberdelinecuencia y la ciberseguridad es parte de muchos actores y la coordinación no siempre es fácil. Por nuestra parte, queremos extender J-CAT, esta iniciativa de ciberespecialistas que tenemos en Europol —que colaboran a nivel policial para que el flujo de información sea más rápido y más fluido—, también al sector privado. Es una iniciativa que tenemos abierta y estamos esperando la oportunidad para incluir a representantes del sector privado, con el fin de que colaboren con este grupo de policías en relación con investigaciones o iniciativas concretas; que durante un periodo de tiempo trabajen con nosotros y tratemos de explotar esta interacción. En otras iniciativas, como la de seguridad en los aeropuertos, ya tenemos una colaboración con el sector privado, pero es algo que continuamente tratamos de explorar y de explotar porque lo consideramos una necesidad.

Respecto a los códigos de intercambio de información de Europol —ha sido una pregunta muy concreta—, tenemos una serie de códigos y esto es esencial para nosotros. Toda la información de la que dispone Europol en nuestras bases de datos —desde un teléfono, hasta un nombre, hasta una IP—, todo pertenece alguien, Europol no es el dueño, pertenece bien a la policía española, bien a la policía francesa, bien a la americana, a quien aporta esa información y ha contribuido a esa información. Cuando la aportan, con cada dato adjuntan un código de manejo; ese código de manejo nos dice lo que podemos hacer con la información: hasta qué punto se puede distribuir a una tercera parte; hasta qué punto, si hay un cruce con esa información, hay que preguntar al dueño antes. Eso es algo esencial para nosotros porque, como he dicho antes, la confianza es un elemento fundamental a la hora de cooperar y a la hora de compartir información. Si no implementamos los mecanismos adecuados para garantizar el correcto uso de la información, nuestros socios no van a confiar en nosotros. Hasta ahora nunca hemos tenido un problema con los códigos de manejo, y es una de las grandes virtudes de Europol. Quien facilita una información y asigna un código de manejo sabe que eso va a ser respetado y tiene total control sobre esa información.

Sobre ICANN y el problema con Whois es, efectivamente, un problema actual consecuencia del reglamento de protección de datos: una información que antes era pública ahora deja de serlo, porque infringiría —aunque hay cierto debate— el reglamento de protección de datos. ¿Qué ocurre? Que esta información relacionada con los registros de los dominios, que antes era fácilmente accesible de cara a una investigación policial, pero también desde el punto de vista de la seguridad, ya no lo va a ser. En Europol hemos tratado de llegar a un acuerdo con ICANN para facilitar un portal de acceso a esta información, porque los registros están dispuestos a facilitar esta información dentro de una investigación

cve: DSCG-12-CM-124

policial —no es pública, pero se puede facilitar—. Nosotros no hemos podido facilitar este portal para acceder porque la interpretación de nuestro reglamento que hemos recibido nos lo impide. Sin embargo, tras conversaciones que hemos mantenido, sabemos que ICANN está desarrollando un portal para poder dar acceso, al menos a las agencias policiales, a esa información que es clave para desarrollar investigaciones. Es un portal, una herramienta técnica en la que estamos prestando asesoramiento, y esperemos que sea implementada por lo menos a medio plazo.

Respecto al personal que trabaja en el Centro Europeo de Ciberdelincuencia, somos unos 85; dentro de la unidad que yo dirijo, que es la de operaciones, somos entre 45-50. Si me preguntan, siempre diré que somos pocos; si recibiera otros 50, otros 500, tendrían trabajo todos inmediatamente porque tenemos mucho. Pero hay que tener en cuenta que hay muchas prioridades y tenemos otros centros dentro de Europol: el departamento de operaciones, el centro de lucha contra el terrorismo, el centro de lucha contra el crimen organizado y, dentro de él, el centro de lucha contra la inmigración ilegal, dos prioridades que ahora mismo son muy importantes. Por tanto, a la hora de repartir los recursos hay que atender todas las prioridades.

¿Si podemos actuar como peritos en juicio? Sí, lo hemos hecho a requerimiento. Desarrollamos algunos informes y podemos ser requeridos para participar en el juicio oral como peritos y ratificar el informe que hemos desarrollado.

Recomendaciones en este sentido. Mi recomendación sería realizar más intercambio de información. Europol es una agencia que está para servir, está financiada por los Estados miembros y ofrecemos un servicio, ofrecemos servicio a quien nos los solicita. Si no nos piden este servicio, si no comparten información con nosotros, si no nos utilizan como vehículo para coordinar investigaciones internacionales, no podemos facilitar este tipo de apoyo, y si no lo hace una agencia de un país lo va a hacer la del otro. Con lo cual, yo animaría a que se facilitara toda esta información, porque en el marco de cualquier investigación relacionada con ciberdelincuencia es difícil no encontrar un elemento internacional. En ese sentido, hay que lanzar un mensaje para que se utilicen más los recursos que están disponibles. Luego tendremos que realizar una función para dar prioridad al que más tenga, pero que se utilicen los servicios que ahora mismo están a su disposición; algunos países podrían intercambiar más información, podrían utilizar mejor estos recursos que están disponibles.

En cuanto a *internet governance,* había otra pregunta: qué se podría mejorar dentro de *internet governance* en cuanto a la seguridad del usuario. Uno de los aspectos sobre el que hemos llamado la atención es la información relacionada con los registros, que no siempre es tan aceptada o tan precisa como debería ser. Por parte de los registros se tendría que asegurar que la información aportada es fidedigna, adecuada y que no son informaciones falsas aportadas por los criminales para realizar registros. Esto es algo que se puede mejorar. Sabemos que hay *policies* en este sentido para que se mejore, pero es algo que hemos resaltado en el pasado y que hemos comunicado al grupo de seguridad de *internet governance* acerca de este problema que supone a la hora de la investigación.

Respecto a los grandes grupos criminales, a su estructura, a las conexiones de la cibercriminalidad con otras formas de criminalidad, es algo que hemos visto cuando he hablado del uso de la *dark web*; son herramientas técnicas, posibilidades técnicas que pueden utilizarse por cualquier criminal. La venta de drogas o de drogas peligrosas a través de la *dark web* son investigaciones que llevan nuestros compañeros de tráfico de drogas. ¿Qué ocurre? Que ello conlleva unos conocimientos técnicos hasta cierto punto que ellos no tienen ni tienen por qué tener. Luego lo que tenemos que hacer desde el Centro Europeo de Ciberdelincuencia es asegurarnos que estos compañeros reciben el asesoramiento técnico cuando lo necesitan para desarrollar sus investigaciones, ya que nosotros, el Centro Europeo de Ciberdelincuencia, no podemos desarrollar investigaciones relacionadas con tráfico de armas o de drogas a través de internet. Tenemos especialistas y esos especialistas requieren el asesoramiento y la formación adecuada hasta cierto nivel para entender cómo funcionan estas tecnologías. Esto es un problema, porque cada vez más estamos viendo cómo la tecnología facilita otros hechos criminales y hay que incrementar de cierta manera los niveles de conocimiento técnico de toda la base policial. No puede ser que solo los técnicos, la gente que trabaja en unidades de nuevas tecnologías, tengan ciertos conocimientos; pueden tener los más elevados, pero hay varios niveles de conocimiento y el básico lo deben tener todos los policías en Europa, por lo que debería formar parte de los currículums de formación de todos los policías; a un segundo nivel puede haber compañeros que de forma habitual se relacionen con nuevas tecnologías y pueden tener una formación más específica, y en la pirámide es donde tendrían que estar los especialistas únicos, con conocimientos que nadie más tiene.

cve: DSCG-12-CM-124

Ámbitos legislativos en relación con el uso criminal de la *dark web*. *Dark web* es una red dentro de internet que tiene usos muy legítimos —nunca diremos que es algo malo, tiene usos muy legítimos y hay países donde hay censura, pero hay gente que necesita ser anónima porque puede estar amenazada—, el problema es el uso criminal de la *dark web*. Más que buscar soluciones legislativas a este fenómeno, que es una cuestión técnica, lo que sí que habría que buscar son herramientas legislativas para tener información que de algún modo esté relacionada con la *dark web;* tengo que decir que se están buscando soluciones, se están desarrollando soluciones a nivel europeo. El intercambio de información a nivel internacional, el proceso de comisiones rogatorias, la lentitud de este proceso y cómo esto es un impedimento para desarrollar investigaciones, es algo que está siendo abordado actualmente. Hay una propuesta de la Comisión que ahora está siendo debatida por el Consejo y por el Parlamento, que es el paquete de evidencias digitales. Cuando se consiga llegar a un acuerdo y entre en vigor, facilitará las peticiones directas de autoridades judiciales europeas a empresas que ofrecen servicios en Europa, independientemente de donde tengan sus sedes; pueden ser empresas que están establecidas en Estados Unidos, pero si esto se sigue desarrollando en el camino que se prevé, estas empresas deberán designar un representante en Europa, que recibirá directamente esa petición y tiene que responder en un breve espacio de tiempo. Cuando entre en vigor va a facilitar mucho la velocidad en el intercambio de información y va a evitar tener que realizar intercambios de comisiones rogatorias. Esto, que puede ser una herramienta muy útil, veremos cómo se conjuga con las iniciativas, por ejemplo, con parte de Estados Unidos, que están regulando lo mismo a nivel nacional: tratan de limitar el acceso a la información de las empresas con sede en su país, con lo cual hay mucho debate. Se llama Cloud Act, está ya en vigor y veremos cómo se conjugan estos dos elementos legislativos y cómo se consigue llegar a un acuerdo, porque desde luego hay cierta fricción.

Respecto a internet de las cosas, efectivamente, es algo muy positivo: mayor conectividad, como ya he dicho, ofrece mayores servicios, etcétera. Pero todos estos dispositivos conectados a la red son también vectores de ataque para las cibercriminalidades, y la base de vectores de ataque cuando todo esté conectado —si no lo está ya, mucho más no lo va a estar— va a suponer una gran base para estos ataques. Pero las medidas de seguridad de muchos de estos dispositivos no son las adecuadas; en el pasado no se ha invertido lo suficiente, no se ha legislado o no se ha requerido la suficiente seguridad mínima en estos dispositivos. Se está abordando esta actuación: a la agencia europea de ciberseguridad, Enisa —cuyo mandato, si la última información que tengo es correcta, está siendo debatido ahora mismo por el Consejo y el Parlamento—, se le va a asignar una certificación, que ya veremos si es obligatoria o recomendable, pero una certificación para que este tipo de dispositivos la adopten, para que los productores de estos dispositivos cumplan con unas mínimas normas si quieren vender, comercializar sus productos dentro de Europa.

También ha habido otra pregunta sobre la colaboración con el sector privado. Como he mostrado en la presentación, efectivamente, es una obligación, es una necesidad y muchas de las iniciativas que estamos desarrollando en Europol, pero también a nivel nacional, sabemos que involucran al sector privado. Hay diversos países en los que las unidades de ciberdelincuencia tienen establecidas unidades de acción en las que colaboran de manera habitual y regular con el sector privado —puede ser con el sector financiero, con agencias de seguridad—, y yo creo que hoy en día todas las autoridades policiales de Europa son conscientes de la necesidad de colaborar con el sector privado.

Respecto a más colaboración con empresas extranjeras, creo que ya he contestado a través de la pregunta relacionada con el paquete de evidencia digital que se está desarrollando actualmente a nivel europeo.

La regulación de las criptomonedas. Efectivamente, está habiendo un incremento en su uso y es difícil regular la criptomoneda en sí; lo que se puede regular son los *exchanges*, que son las entidades que cambian criptomoneda por moneda de curso legal. La mayoría de estos *exchanges* colaboran con las autoridades y tienen una política de conocimiento de sus clientes adecuada; piden suficiente información cuando alguien quiere abrir una cuenta en esos *exchanges:* piden información, fotografías, copias de documentos de identidad, etcétera, antes de crear una cuenta y facilitar estas transacciones entre criptomonedas y monedas de curso legal. Pero hay algunos otros que no, y con que haya unos cuantos que no lo hacen, ya pueden ser utilizados por los delincuentes y, por lo tanto, son vías para blanquear beneficios y para traducir beneficios que obtienen a través de criptomonedas en moneda de curso legal.

Por lo tanto, sí, es un punto en el que hemos llamado la atención en el pasado en el sentido de que es necesario regularlo porque esto solo va a crecer.

cve: DSCG-12-CM-124

En relación con los ciberataques y la posibilidad de que Estados estén detrás de estos ciberataques, desde Europol es difícil que lleguemos a decir: detrás de este ciberataque está este país en concreto o este otro. Esa atribución es, probablemente, política; nosotros nos centramos en una atribución técnica. Nosotros realizamos un apoyo técnico a las investigaciones, realizamos análisis y aportamos esta información técnica. El nivel al que estamos acostumbrados dentro de la esfera policial y judicial para demostrar que una persona es responsable de esta actividad criminal que es enjuiciada y lograr una convicción, es un nivel de atribución muy alto y los elementos de evidencia que hacen falta son importantes. Va a resultar difícil encontrar esos elementos de evidencia cuando quien está detrás puede ser un Estado; incluso, aunque a nivel técnico podamos ver que el origen de cierto ataque viene de un Estado en concreto, incluso hasta de un edificio gubernamental de un Estado, ese Estado siempre puede decir: Sí, he sido hackeado, o es un grupo criminal operando desde mi país... Habría que acceder a estos elementos, a estos edificios, habría que interrogar a las personas, y eso difícilmente va a ocurrir cuando haya un ataque procedente de un Estado.

Eso no quiere decir que no los haya, desde luego, y que hasta se pueda realizar la atribución a nivel político. En ese sentido, hay una iniciativa a nivel europeo, que está coordinando el European External Action Service, para realizar un paquete de ciberdiplomacia: cómo realizar una respuesta diplomática ante ciberataques que provienen de países, y están elaborando una serie de potenciales respuestas. Europol juega un papel en este proceso, nos pueden consultar, pero nosotros vamos a dar una información técnica: esto es lo que vemos desde un punto de vista técnico en relación con el origen o las consecuencias del ciberataque. A partir de ahí, hay que rehacer una interpretación política en base a las circunstancias y al entorno político del Estado.

¿Se está haciendo todo lo posible en la lucha contra la ciberdelincuencia? Se están llevando a cabo muchas iniciativas: la creación del Centro Europeo de la Ciberdelincuencia fue una, hace unos años, y en la medida que se puede se están invirtiendo esfuerzos, tanto a nivel operativo como a nivel legislativo, para tratar de actualizar todas las herramientas que hacen falta para luchar contra la ciberdelincuencia.

¿Estos grupos son organizados? Sí, existen grupos organizados, pero existen sobre todo grupos distribuidos. Dentro de la ciberdelincuencia, estamos viendo cada vez más colaboración entre criminales que ni siquiera tienen por qué conocerse físicamente, que operan con seudónimos *online* y colaboran entre ellos con un mismo objetivo, aportando cada uno de ellos una función dentro del grupo criminal. Son grupos, más que jerarquizados, distribuidos. Esto es algo que llevamos viendo y es algo que está ocurriendo.

¿Si nos están ganando en relación con la velocidad? Lo cierto es que la tecnología avanza muy rápidamente y todo avance tecnológico es susceptible de ser utilizado por los criminales para ocultar sus actividades criminales. Nosotros tratamos de que eso no ocurra así, tratamos de estar a la altura y tratamos de estar actualizados con nuevos desarrollos tecnológicos. Es una de las funciones que tenemos dentro del Centro Europeo de Ciberdelincuencia: tratamos de estar actualizados en el funcionamiento de cualquier nueva tecnología, de cualquier nueva aplicación, ver quién es el responsable, el dato de contacto de este nuevo sistema o de esta nueva plataforma por si hay necesidad de requerir datos a esta plataforma o de cómo se interpreta esa tecnología. Si recibimos una petición, facilitamos esta información a los investigadores. Es una de nuestras funciones y en ello estamos invirtiendo esfuerzos.

En relación con la colaboración internacional, iniciativas europeas y la Agencia Europea de Ciberseguridad, ya he contestado. Tenemos una muy buena relación con ellos. Realizamos todos los años varios *workshops*, varios talleres, en los que juntamos a investigadores policiales y a especialistas en ciberseguridad de los CERT y los CSIRT y hablamos sobre cómo mejorar la colaboración y cómo crear equipos conjuntos. Realizamos también ejercicios de simulación. ¿Qué se puede hacer para mejorar la respuesta en caso de ciberataques para estar mejor preparados? Pues realizar ejercicios para comprobar hasta qué punto estamos preparados. Esto es algo que se realiza de manera regular. Recientemente, se ha desarrollado uno a nivel europeo en el que se han involucrado muchos actores, nosotros también hemos participado, para ver cómo funcionan esos mecanismos, que sobre el papel parecen adecuados, a nivel práctico: cómo se va a realizar el intercambio de información, qué herramienta se va a utilizar; cómo traducimos a nivel práctico estos planes y que consigamos una buena coordinación. Para esto se desarrollan muchos ejercicios y nosotros somos parte de ellos.

No sé si me dejo alguna pregunta, la última estaba relacionada con las medidas legislativas y operativas, que creo que he abordado anteriormente, pero si hay alguna contrarréplica, estaré encantado de contestarles.

cve: DSCG-12-CM-124

El señor **PRESIDENTE:** Muchas gracias. Ahora se lo harán saber.
Segundo turno.
¿Señor Yanguas? **(Denegaciones).**
¿Señor Castellana? **(Denegaciones).**
¿Señor Comorera? **(Denegaciones).**
¿Señor Álvarez? Tiene la palabra.

El señor **ÁLVAREZ VILLAZÁN:** Nada más quiero agradecerle las explicaciones que ha dado a las preguntas, porque han sido totalmente exhaustivas.

El señor **PRESIDENTE:** Damos las gracias al compareciente. Parece que ha gozado usted de un éxito de crítica y público, cosa de la que me alegro. Muchas gracias.
Si les parece, reanudamos la sesión en cinco minutos.
Se suspende la sesión.

Eran las diecisiete horas.

Se reanuda la sesión a las diecisiete horas y quince minutos.

El señor **PRESIDENTE:** Señorías, reanudamos la sesión.

— COMPARECENCIA DEL GLOBAL CISO, CHIEF INFORMATION SECURITY OFFICER AND TECHNOLOGY RISK, DEL GRUPO SANTANDER, DON DANIEL BARRIUSO ROJO, ANTE LA COMISIÓN MIXTA DE SEGURIDAD NACIONAL, PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Senado 715/000599 y número de expediente del Congreso de los Diputados 219/001523)
AUTOR: COMISIÓN MIXTA DE SEGURIDAD NACIONAL

El señor **PRESIDENTE:** Doy la bienvenida al señor Barriuso Rojo, que es nuestro siguiente compareciente.
Sin más trámite, le doy la palabra al señor Barriuso para luego abrir el turno de portavoces.
Señor Barriuso, suyo es el turno.

El señor **BARRIUSO ROJO** (global CISO, chief information security officer and technology risk, del Grupo Santander): Buenas tardes.
Lo primero de todo es que me gustaría agradecerles que nos hayan invitado a comparecer hoy. Es un verdadero placer estar aquí y apreciamos mucho la oportunidad. Creo que somos el primer banco que se presenta ante ustedes, y pensamos que para nosotros es una verdadera oportunidad para compartir experiencias e ideas. Es una comparecencia voluntaria y la vemos como una oportunidad para aportar las ideas y soluciones que podamos. Además, pensamos que Santander, igual que el resto de la banca, es parte de un ecosistema donde la inversión que hacemos en ciberseguridad creo que es buena, en general, para el resto de la sociedad. Somos parte de un ecosistema y de una cadena donde las distintas partes pueden contribuir. En ese espíritu, estamos encantados de contribuir hoy y nos gustaría poder añadir nuestro granito de arena para que lo tengan en cuenta en sus consideraciones.
A la hora de preparar la presentación de hoy, la he estructurado en tres partes. Me gustaría comentar la visión del Santander sobre el ciberespacio, sobre los retos y amenazas, pero también las oportunidades que hay; luego me gustaría comentar, con algo de detalle, nuestra filosofía, nuestra aproximación a la ciberseguridad y cómo la abordamos; y, por último, quiero poner sobre la mesa ideas y, quizás, compartir puntos de vista que esperamos que puedan ser de utilidad para ustedes y puedan ayudar al ecosistema más amplio de la ciberseguridad en España.
Empiezo con la parte del mundo digital y el ciberespacio. Creo que es importante tener en cuenta el contexto en el que estamos, en el que las nuevas tecnologías, los sistemas de información, son parte cotidiana del día a día para los ciudadanos y, también, para las empresas. Brindan oportunidades extraordinarias, económicas y sociales, pero esas mismas tecnologías también pueden ser explotadas y utilizadas por criminales. Por tanto, también hay amenazas.
Las amenazas de ciberseguridad, además, son globales, no conocen fronteras. Las amenazas de ciberseguridad no pueden ser eliminadas; pueden ser gestionadas, pero muy difícilmente eliminadas, y el impacto va mucho más allá de lo técnico. El impacto de las ciberamenazas puede ser reputacional,

cve: DSCG-12-CM-124

financiero, económico... Es una amenaza, además, muy dinámica, donde constantemente aparecen nuevas vulnerabilidades, nuevos tipos y técnicas de ataque, y es un riesgo, una amenaza que yo describo como asimétrica. ¿Y qué quiere decir esto para mí? Pues muy sencillo, que los atacantes tienen el terreno a favor. ¿Y en qué sentido? En el de que ellos solo tienen que encontrar una vulnerabilidad una vez para conseguir sus objetivos. El que defiende tiene que defender todo y todo el tiempo. ¿Y esto que quiere decir? Pues que es más fácil atacar que defender. Es más complicado defenderse.

El desafío que tenemos en la sociedad es crear una sociedad ciberresiliente que nos permita protegernos, pero también detectar amenazas, responder a ellas y recuperarnos, y todo ello de manera ágil y dinámica, tanto como el mundo de las amenazas, y a fin de cuentas conseguir que todo el mundo se beneficie de las oportunidades que las nuevas tecnologías traen.

En particular, para nosotros, en el Santander, y yo diría que para la banca en general, la privacidad, el proteger los datos de nuestros clientes es una prioridad y siempre ha estado en el núcleo de lo que hacemos. Pensamos, además, que no solo se trata de hacerlo de puertas para adentro, sino también, como comentaba al principio, de extender nuestra ayuda fuera hasta donde podamos.

Para el grupo Santander la ciberseguridad es una prioridad clave. Proteger la información y los sistemas, los datos de nuestros clientes, es una prioridad clave, y pensamos que, además, lo es desde el punto de vista de nuestra misión, que es ayudar a las personas y a las empresas a prosperar, y también es clave para nuestro objetivo de ofrecer servicios digitales excelentes. De hecho, a medida que generamos más servicios digitales nuestros clientes son más y más digitales y la ciberseguridad es más importante. Nosotros, por ejemplo, ponemos el componente de ciberseguridad al principio, en el diseño de los nuevos servicios para que sea parte de su creación y no una idea posterior. Asimismo, la prioridad que tenemos en el grupo se refleja también en el gobierno, en la gobernanza del Santander. Tenemos un comité dedicado a la ciberseguridad, que preside el consejero delegado, donde estudiamos la situación, los planes y el progreso en ciberseguridad de forma regular. Y es un tema que se aborda también como parte de la agenda del Consejo del Grupo. Por ejemplo, este año, en 2018, hemos tenido una sesión cada trimestre para poner al día y compartir cómo avanzan los planes de seguridad, dónde estamos, y sesiones adicionales donde hemos hecho un poquito de *zoom* en puntos concretos específicos de cíber, que, como bien saben ustedes, es un mundo amplio y complejo. También es una prioridad para las subsidiarias del grupo y es parte del gobierno en todas ellas.

Para nosotros, en Santander, el foco en seguridad es un foco de carácter muy global. Tenemos un marco global de ciberseguridad, tenemos una organización global de ciberseguridad y tenemos un programa también global que nos ayuda a avanzar y a progresar en ciberseguridad. Buscamos una organización ciberresiliente que nos permita proteger, detectar, reaccionar rápidamente de una manera continua, evolucionando y mejorando de forma continua. En un elemento tan dinámico como el ciberespacio, pensamos que hay que mejorar todo el tiempo.

El marco de ciberseguridad para el Santander es una especie de política de muy alto nivel que establece los principios y las responsabilidades clave para distintos temas. En ciberseguridad, el marco fue aprobado en el consejo el año pasado y está alineado con las mejores prácticas internacionales, como el NIST en Estados Unidos o el ISO 27000 internacional, y define las responsabilidades, la aproximación, los principios que utilizamos en cíber. Para nosotros está basado en tres principios, y el primero es defender. Uno de nuestros objetivos clave es defender nuestros sistemas, nuestra información, los datos de nuestros clientes. El segundo principio es anticipar. En otras palabras, ser proactivo. Y el tercer principio es colaborar.

Desde el punto de vista del principio de defender, nosotros utilizamos una analogía para explicar cómo vemos la defensa. Es lo que llamamos las tres murallas de defensa. Literalmente lo dibujamos como tres muros que son los que nos ayudan a poder defendernos.

El primer muro es lo que llamamos proteger. Ahí incorporamos todas las tecnologías, los sistemas y los servicios que nos ayudan a prevenir ciberataques: los *firewall*, los antivirus, etcétera. El segundo muro, que es igualmente importante, es el que describimos como detectar. Es el muro que nos ayuda a estar vigilantes constantemente para encontrar nuevas amenazas. Y el tercer muro, responder, de manera que cuando encontramos una nueva amenaza respondemos lo más rápido posible a ella, lo más efectivamente posible.

En el mundo de ciberseguridad más moderno creo que hay bastante consenso a la hora de decir que la diferencia entre un problema grave y un problema pequeño a veces es detectarlo a tiempo y responder lo más rápido posible. Además, pensamos que es muy importante que cuando se detecta una nueva

cve: DSCG-12-CM-124

amenaza, rápidamente el muro de protección se actualice para estar lo mejor preparados posible, o que cuando se responde a algún evento mejoremos cómo detectamos y cómo nos protegemos para la siguiente vez. Una mejora constante.

En el grupo Santander estamos a punto, además, de inaugurar un nuevo centro de ciberseguridad en España que, justamente, da los servicios de defensa, protección, detección y respuesta para las distintas entidades del grupo, de forma global. Va a contar con más de 3800 metros cuadrados, unos 300 profesionales de ciberseguridad y estará basado en España. Esperamos inaugurarlo en febrero.

El segundo principio del que hablaba es anticipar. La manera en que yo lo describo, quizás un poco simple o gráfica, es que trata de conseguir que esas murallas que he descrito antes, en lugar de muros de ladrillo, que son muy rígidos, sean más bien de lego y se puedan cambiar lo más rápido posible, porque de nuevo son amenazas muy dinámicas. Intentamos anticipar, por una parte, con inteligencia. Intentamos tener buena inteligencia sobre las amenazas existentes, y emergentes también, para poder, en la medida de lo posible, estar preparados en la defensa. Buena inteligencia para nosotros significa colaborar con entidades públicas, con agencias, con otras entidades privadas y con el sector para entender lo mejor posible qué es lo que está ocurriendo y qué es lo que va a ocurrir.

Para nosotros, anticipar también tiene el sentido de vigilar y encontrar cualquier vulnerabilidad para intentar arreglarla lo antes posible. Tenemos, por ejemplo, nuestro propio equipo de *hackers* éticos que buscan testear nuestras defensas para encontrar si hay alguna vulnerabilidad que deberíamos arreglar, sobre todo en un entorno donde las compañías tecnológicas publican nuevas vulnerabilidades constantemente. Hay que ser proactivos en la detección. Pensamos que es importante testear nuestras defensas. Y también anticipar desde el punto de vista de estar preparados con planes de contingencia. Pensamos que es importante que los planes de contingencia, que ayudan a responder ante imprevistos, no solo piensen en los escenarios más tradicionales, más físicos, sino también en los escenarios cíber, que son más nuevos y que también requieren una contingencia y una planificación para estar preparados.

Por último, el tercer principio es colaborar. La manera que tenemos de entender la ciberseguridad es amplia. Pensamos que no se puede abordar la ciberseguridad con un grupo de técnicos como yo, sentados en un garaje con una capucha, todos con el ordenador, sino que pensamos que hay que trabajar un ecosistema mucho más amplio, que va desde los clientes hasta las áreas de negocio, reguladores, fuerzas de seguridad, proveedores, etcétera. Ese ecosistema te puede aportar mucho valor y, además, yo creo que todos tenemos que contribuir. Asimismo, pensamos que los cimientos de esos muros de los que hemos hablado son las personas y sus comportamientos, es decir, los sistemas son tan seguros como las personas que los utilizan. Por tanto, la concienciación, la educación en seguridad es clave.

En el grupo, por ejemplo, ponemos mucho foco en concienciar y formar de manera continua a nuestros empleados. Tenemos vídeos de concienciación, campañas, mensajes, artículos, juegos o talleres que nos ayudan a colaborar con nuestros colegas, con nuestros empleados, para que sean nuestra primera línea de defensa. Además, intentamos tener un mensaje lo más sencillo posible, dando una serie de consejos que ayuden a los empleados del grupo a estar protegidos como empleados, pero también cuando están en su vida cotidiana, como personas. Utilizamos, además, cinco reglas o consejos para ilustrar lo que uno puede hacer para protegerse. El primero: protege tu información y tu equipo. Si no estás utilizando el ordenador, bloquéalo; cuidado con lo que uno conecta al equipo; hay que tener cuidado con la información en cualquier formato en el que esté y dónde se deja.

La segunda regla: piensa antes de hacer clic. Antes de abrir ese archivo, ese *link* que nos llega, pensar dos o tres segundos puede ser la diferencia entre caer en una trampa o estar a salvo. Damos ese consejo.

El tercer consejo utilizado: protege tu clave. Básicamente, elige una clave que sea fácil de recordar, pero difícil de adivinar.

El siguiente es ser discretos *online* y en público. Sobre todo, recordamos a nuestros empleados la importancia que tiene ver ese mundo de los medios sociales como una ventana muy pública ante lo que pongamos ahí. Hay que ser conscientes de lo que uno pone y de lo que uno decide compartir.

Y el último consejo, muy importante para nosotros: si sospechas algo, repórtalo. Si algo no te cuadra, si algo te preocupa, díselo al departamento de ciberseguridad, al departamento de tecnología, porque estamos aquí para echar una mano.

Desde el punto de vista del cliente, también damos información y consejos de manera continua utilizando nuestro canal de internet, nuestras comunicaciones a clientes, incluso por medios más públicos y más amplios, como puede ser Twitter o Facebook, donde damos consejos de manera más regular. Por

cve: DSCG-12-CM-124

ejemplo, en el mes de octubre participamos con Europol en el Mes Europeo de la Ciberseguridad, que en otros países se llama también *October,* y aprovechamos para dar algunos consejos adicionales; de hecho, las cinco reglas de las que he hablado las hemos publicado para quien tenga interés en esto y le pueda ser útil.

Este es el enfoque de los principios que tenemos en cuenta en Santander a la hora de abordar la ciberseguridad.

En el espíritu de colaboración del que acabo de hablar, me gustaría poner sobre la mesa ideas, perspectivas que esperamos que puedan ser de interés. Me gustaría comentar tres ideas en la sesión de hoy. La primera idea que quiero poner sobre la mesa es la importancia de la concienciación, justo al hilo de lo que estaba hablando. Si pensamos que los cimientos de cíber son los comportamientos de las personas, si pensamos que nuestra sociedad, nuestros negocios, nuestra vida cotidiana dependen de la tecnología, usar esa tecnología de manera segura es cada vez más importante. De hecho, pienso que la medida más importante que podríamos tomar para para ayudar en este ecosistema de ciberseguridad sería la concienciación y la educación de la sociedad, de los ciudadanos, de todos nosotros. Además, se ilustra muy bien con un ejemplo muy relevante, que son los ataques *phishing*. *Phishing* se considera como el método de ataque que se usa en el 90% de los ciberataques. Es muy sencillo. Es ese *e-mail* que a todo el mundo le ha llegado, tarde o temprano, donde el atacante crea un *e-mail* destinado a la víctima, con un *link* o un documento, y el objetivo del atacante es que la víctima lea el *e-mail* de la manera más rápida posible, si puede ser sin que piense, haga clic y lo abra. A menudo, cuando haces clic o abres el documento tu ordenador queda comprometido y ahí puedes tener un virus, puedes tener atacantes conectándose, pueden cifrar tu ordenador y pedir un rescate, etcétera. Además, los mensajes de *phishing* ya no solo llegan por *e-mail*, pueden llegar por SMS, por wasap, por mensajes de las redes sociales. La diferencia entre ser una víctima o estar a salvo a menudo es la decisión que tomamos de hacer clic o no.

Pienso que es fundamental ayudar a todo el mundo a entender cómo protegernos lo más posible. De la misma manera que en el mundo real todos, de manera intuitiva, hemos aprendido a andar seguros por las calles y hay situaciones que te hacen pensar —depende de dónde estés, de la hora que sea, de qué hay alrededor— en ser más cauteloso, pensamos que hay que conseguir ese mismo modo de pensar en el ciberespacio. No solo se trata de información intelectual que uno lee y aprende y ya está, sino que hay una parte que es emocional, es decir, cómo podemos conseguir que todo el mundo tenga un conexión emocional donde ciberseguridad importa, y como te importa piensas en ello y tienes cuidado. Creemos que hay una muy buena oportunidad de crear un mecanismo, quizás una organización, que coordine la concienciación de ciberseguridad, empezando por los más pequeños, los colegios, los niños, las niñas, las madres, los padres, pero siguiendo con el resto de la sociedad, utilizando los medios de comunicación, los canales de comunicación que están al alcance de todos. Además, esa organización podría buscar una colaboración pública, privada, de todo los que estén en este mundo de cíber, donde se puedan aportar ideas, conceptos, incluso materiales, vídeos. Hay una multitud de cosas que se pueden reutilizar al servicio de la sociedad en este campo de la concienciación.

La segunda idea o perspectiva que quería poner sobre la mesa es el ámbito de la colaboración. En el mundo del cibercrimen, los criminales, los atacantes colaboran, comparten, están muy organizados, y creo que es muy importante que los que nos defendemos colaboremos, compartamos y estemos lo mejor organizados posible.

En general, en España vemos un buen ecosistema de colaboración. En el Santander, por ejemplo, tenemos firmados acuerdos de colaboración y de intercambio de información con el GNPIC, el Incibe y el CCN-CERT. Y también tenemos una colaboración estrecha con las fuerzas y cuerpos de seguridad del Estado. A nivel europeo tenemos un esquema de colaboración con Europol. Y participamos en ejercicios y *board games*, algunos europeos, y otros internacionales. Pero pensamos que se puede hacer más, que es clave compartir información sobre amenazas y sobre mejores prácticas de manera voluntaria, flexible. Sería muy bueno encontrar más mecanismos para incentivar que eso ocurra con redes público-privadas, sectoriales y mecanismos a través de los que podamos compartir eso de la manera más ágil posible, incluso en algunos casos de modo automático. Creo que el camino que sigue, por ejemplo, la herramienta que hay en España, denominada Ícaro, que está basada en la tecnología MISP, tiene esa intención, y es muy bueno seguir fomentando herramientas que permitan compartir casi en tiempo real. Además, la cooperación, la colaboración, va más allá de las amenazas. Creo que es importante colaborar desde el punto de vista de la gobernanza, la prevención, la formación, la concienciación o la persecución de delitos. Un punto de vista amplio a la hora de colaborar sería muy positivo.

cve: DSCG-12-CM-124

El tercer punto que quería comentar tiene que ver con algo que creo que es una oportunidad y un reto muy importante: el talento. La demanda de profesionales en ciberseguridad, tanto en España como fuera, cada vez es mayor. A nivel internacional Gartner estima que el número de puestos que quedarán sin cubrir en el mundo cíber en 2021 será de 3,5 millones de ciberprofesionales, es decir, habrá una demanda no satisfecha de 3,5 millones. En 2016 se estimaba en un millón. En organizaciones como la mía, por ejemplo, muchos de mis colegas CISO en otras entidades están muy acostumbrados a tener siempre una vacante abierta y buscar profesionales. Eso es constante. Es muy difícil decir que todos los puestos siempre están cubiertos; y la demanda crece.

La demanda, además, es de un perfil distinto al de la seguridad tradicional. Un rol como el mío, de CISO, o responsable de seguridad en mi caso, sigue teniendo una componente técnica muy importante, y la mayoría del talento para este mundo técnico viene de las ciencias, la tecnología, las ingenierías, las matemáticas. El porcentaje de graduados universitarios de las carreras de ciencias suele estar cerca del 25 %. Además, la ciberseguridad no es solo una profesión, son muchas: se puede ser ciberarquitecto, *hacker* ético —una profesión que atrae a muchos de los chicos y chicas jóvenes—, investigador forense, operador de seguridad, experto en cibervigilancia, analista de amenazas… Hay muchas carreras dentro de lo que es cíber, y todas ellas tienen en común esa parte técnica. Por otra parte, el conocimiento cíber es cada vez más relevante para profesiones que no son necesariamente técnicas. La ciberseguridad se convierte cada vez más en un elemento intrínseco de otras profesiones, como en el mundo del derecho, las comunicaciones, la criminología o la psicología. Creo que hay una componente muy beneficiosa cíber a la hora de entender este mundo al que vamos en otras profesiones.

España cuenta con muy buenos estudiantes y muy buenos profesionales en ciberseguridad —me atrevería a decir que están al nivel de los mejores del mundo—, pero creo que podemos hacer más para potenciar y generar talento. Y permítanme que me detenga un poquito en esto.

En primer lugar, si vemos a los más pequeños en el colegio, podría ser muy positivo incorporar cíber como parte de la educación desde dos puntos de vista. Por un lado, generando ese interés y esas habilidades en la ciberseguridad, que pueden ser muy útiles para el desarrollo de los niños y niñas en este mundo profesional. Pero también puede dar herramientas y conocimientos que a los niños y niñas les ayuden a navegar por este mundo de internet, en el que cada vez se empieza más pronto, para hacerlo de la manera más segura posible.

También la educación secundaria es un punto clave, por lo que sería muy positivo tener mecanismos que nos permitieran identificar el talento o a aquellos niños y niñas que tengan interés en cíber o las ciencias, y crear currículums, asignaturas o grupos que lo fomenten. Israel, por ejemplo, ha avanzado mucho justamente en ese punto: desde muy pronto detectan a los niños y niñas que tienen talento o interés en cíber, y ya en la educación secundaria crean grupos de cíber que tienen asignaturas y un conocimiento especial, hasta el punto de que cuando acaban la educación secundaria muchos de ellos se pueden poner a trabajar como profesionales a los niveles más altos, como profesionales totalmente cualificados. Repito que tenemos una oportunidad muy buena en el mundo de la educación secundaria. Sé que Incibe —creo que ya ha estado en esta comisión— está potenciando esto. Pienso que podemos hacer más y que es muy positivo seguir fomentando este aspecto.

Y, por supuesto, un punto adicional es la universidad, que juega asimismo un papel clave. En el Santander estamos muy comprometidos con la educación universitaria desde hace más de veinte años. A nivel mundial contamos con más de 1200 convenios con universidades de todo el mundo, y en España en particular aportamos más de 60 millones en mecenazgo, 12 000 becas y tenemos más de 100 convenios de colaboración integral con universidades, centros universitarios y de investigación. Pensamos que sería muy bueno desarrollar un currículum cíber en el mundo universitario con una colaboración estrecha público-privada universitaria que nos permitiera crear profesionales preparados para este mundo cíber y, además, contar con un currículum lo más dinámico posible, entendiendo lo que hace falta y sabiendo que es tan dinámico que es bueno adaptar el sistema educativo a ello. Ahí hay una oportunidad.

Por último, todavía en la parte de talento, me gustaría hablar de un reto y una oportunidad que creo que tenemos en cíber, que es el siguiente. Hablaba antes de que el 25 % de los estudiantes vienen de esta rama de la ciencia, pero en algunas ingenierías solo dos de cada diez estudiantes son mujeres. En el mundo de los ciberprofesionales se estima que, globalmente, el 11 % son mujeres, así que tenemos una clara oportunidad para aumentar la diversidad y hacer la ciberseguridad más atractiva y también un mundo más dinámico, de más interés para los niños, las niñas, las mujeres.

cve: DSCG-12-CM-124

Además, creo que la diversidad en el talento cíber nos aporta mucho valor. Si podemos ayudar a que ese 11 % crezca más y más, podremos dar un paso de gigante en este reto de encontrar talento. El Santander tiene becas fomentadas para mujeres del mundo de las tecnologías, lo que se denomina STEM. También somos muy activos en los círculos de Women in Cybersecurity en España y en otros países. De hecho, en junio vamos a albergar la siguiente sesión de Women in Cybersecurity en España, en nuestras oficinas. Pero aplaudiríamos más iniciativas en el aspecto de la diversidad, sobre todo de género, para animar a las niñas y las mujeres a que encuentren una carrera en cíber y fomentarlo.

En resumen, la ciberseguridad es una prioridad clave para el Grupo Santander. Sin duda, hay retos, pero a la vez hay una gran oportunidad de avanzar y de ver el ciberespacio como un lugar donde los negocios y las personas prosperen. La colaboración, la concienciación y la gestión del talento nos pueden ayudar enormemente a abordar esos retos y también a generar valor para la sociedad. De hecho, la ciberseguridad puede ser un motor de crecimiento económico que podría ser alimentado por esta colaboración público-privada, la potenciación del talento y la estructura de colaboración. A fin de cuentas, podría ser un vehículo para ayudar a posicionar a España como uno de los lugares más seguros en el ciberespacio y atraer inversión de aquellos que quieran trabajar en este mundo *online*, a negocios *online* que valoren un ecosistema que ayude a estar lo más seguro posible, de la misma manera que cuanto más seguras son las calles mejor podemos funcionar como sociedad y como economía; un lugar en el que la colaboración ayude a esa seguridad *online*, donde los profesionales emprendedores puedan aportar sus ideas para crear negocios.

Por tanto, pensamos que la nueva estrategia de seguridad nacional puede ser una oportunidad para posicionar la ciberseguridad, no solo como una amenaza, sino también como una oportunidad. Asimismo, creo que es importante que la estrategia venga acompañada de los mecanismos y presupuestos necesarios para implementarla y que busquemos un consenso que nos permita avanzar lo más rápidamente posible. Hablamos de un entorno muy dinámico, y creo que tenemos que ser también muy ágiles a la hora de implementar nuestras ideas. No hay que olvidar que una sociedad más resiliente y concienciada y con más conocimiento cíber es también una sociedad mejor preparada para el futuro y para las nuevas tecnologías.

Me gustaría ponerme a su disposición para cualquier pregunta o comentario que quieran hacerme.

El señor **PRESIDENTE:** Muchísimas gracias, señor Barriuso. Eso es exactamente lo que vamos a hacer, empezando por el Grupo Mixto.

Tiene la palabra el señor Yanguas.

El señor **YANGUAS FERNÁNDEZ:** Muchas gracias de nuevo, señor presidente.

Bienvenido a esta comisión, señor Barriuso. Quiero agradecerle, como no puede ser de otra manera, la exposición que nos acaba de hacer, que servirá a la comisión para concluir aspectos importantes que se están tratando en estos meses. Además, ha sido usted didáctico, ha aterrizado en la realidad, porque para el sector al que usted representa la ciberseguridad es importante. Y también me ha gustado oír que tratan la ciberseguridad como algo transversal, en todas sus líneas de negocio, lo que me parece ideal.

Voy a hacerle una pregunta que no tiene nada que ver con lo que usted ha dicho o que no sé si tiene algo que ver, porque se la hago desde el desconocimiento. Con respecto a otros competidores, no solo de España, sino incluso de otros países, ¿hay algún *ranking?* ¿Cómo estamos valorados, o cómo lo están ustedes, entre los competidores, si los podemos llamar así, de su sector? Ya sabemos que Israel es un país de referencia por ser modelo de ciberseguridad en muchas cosas.

Y en cuanto al sector financiero, quisiera saber cómo está su grupo y cómo está España con respecto a otros países.

Lo demás me ha quedado totalmente claro.

Muchas gracias. Buenas tardes.

El señor **PRESIDENTE:** Muchas gracias, señor Yanguas.

Tiene la palabra el señor Castellana.

El señor **CASTELLANA GAMISANS:** Gracias.

Muchas gracias, señor Barriuso, por su presentación. Voy a hacerle dos preguntas relativamente concretas, porque usted es la primera persona del ámbito privado con la que tenemos ocasión de hablar.

cve: DSCG-12-CM-124

En cuanto a la primera pregunta, las capacidades de ataque se basan en desarrollos y, sobre todo, en vulnerabilidades. Entonces, el sistema aceptado de publicación de vulnerabilidades, que hace que el descubridor de la vulnerabilidad se ponga en contacto con el desarrollador del producto para la elaboración de un parche que permita solucionar la vulnerabilidad y que después, una vez se haga público, haya un reconocimiento al descubridor de la vulnerabilidad, es el sistema que permite ir parcheando y asegurando los sistemas. No obstante, precisamente porque la vulnerabilidad es la clave de los ataques, las agencias gubernamentales, para tener capacidad de ciberatacar en nombre de la ciberdefensa, o las empresas que prestan servicios a estas agencias, no solamente conocen vulnerabilidades que no siguen este sistema de publicación, sino que una de sus tareas principales es crear verdaderas bases de datos con muchas vulnerabilidades que no se hacen públicas. Por lo tanto, son vulnerabilidades potenciales que pueden ser aprovechadas por atacantes, pero que estos actores, en principio legítimos, se guardan en su manga. Pues bien, desde un punto de vista privado, me gustaría saber qué consideración tiene usted sobre el riesgo en el que pone a todo el mundo el comportamiento de esos actores para la adquisición de estas capacidades.

En segundo lugar, hablamos mucho de los ataques, se nos habla mucho de la difícil identificación del atacante. Y como en esa frase tan bonita de canciones, poemas, etcétera, que dice que un lápiz no dibuja sin una mano, a nivel de inteligencia no quiero hablar tanto de los ataques como de los atacantes. Por tanto, sin desvelar nada que no tenga que desvelar, quisiera saber qué información tienen sobre los retratos robots de las personas que hay detrás de esos ataques: sus perfiles, orígenes, cómo entran en este mundo, etcétera.

Esas serían las dos preguntas. Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señor Castellana.

Señor Comorera, tiene la palabra.

El señor **COMORERA ESTARELLAS:** Muchas gracias, presidente.

Muchas gracias, señor Barriuso, por su comparecencia y sus interesantes explicaciones. Estamos muy de acuerdo con todo lo que ha comentado sobre la educación y la importancia que tendría introducir en ella toda la temática cíber. También valoramos muy positivamente sus comentarios sobre la educación secundaria. Y, asimismo, la oportunidad que se nos presenta como país en temas de ciberseguridad.

Al igual que mi compañero Castellana, también le voy a hacer un par de preguntas. Los datos que nos van ofreciendo resaltan que cada vez hay más ciberataques, y mi pregunta a usted, como experto que es, es si realmente hay más ciberataques o se están reportando más desde el ámbito privado. En relación con ello, quisiera saber si usted cree que las empresas han perdido el miedo o las reticencias por la llamada pérdida reputacional que supone el reporte de este tipo de ciberataques, entendiendo, como ya nos ha dicho el anterior compareciente, que el sector bancario es de los más preparados para defenderse ante este tipo de ciberamenazas.

Y paso a hacerle otra pregunta, también muy concreta. Cada cierto tiempo vemos campañas fraudulentas, como ha comentado usted, de *phishing* con suplantación de identidad precisamente del Banco de Santander. Incluso en algún correo he recibido algún tipo de mensaje como al que hacía usted referencia. Bien, me gustaría saber qué hacen ustedes cuando detectan eso, que cada cierto tiempo aparece. Aparte de reportar o comunicar, me gustaría que nos explicara, siempre que usted pueda hacerlo, si después ustedes siguen las diligencias, se personan, si la Policía consigue detectar quién está detrás de esos ataques y si ustedes, como entidad, se personan luego en el procedimiento como parte perjudicada.

Esas son las dos preguntas que me gustaría que contestara.

Muchas gracias.

El señor **PRESIDENTE:** Gracias, señoría.

Tiene la palabra el senador Raffo.

El señor **RAFFO CAMARILLO:** Gracias, presidente.

En primer lugar, quiero darle las gracias al señor Barriuso Rojo por su presencia y por compartir estos temas con nosotros. No somos expertos todavía, pero leemos con bastante fruición, y con ansiedad, en algunas ocasiones, tanto lo que es publicado en fuentes fidedignas a través de la red, como en bibliografía.

cve: DSCG-12-CM-124

Y nos está gustando y nos resulta apasionante lo que llevamos debatiendo ya hace unos meses, que tiene muchos campos que lógicamente habrá que ir desarrollando en el futuro.

También quiero agradecerle su sencillez y cómo ha sintetizado los distintos apartados, porque eso ha facilitado que podamos priorizar una batería de preguntas que teníamos que realizar, algunas de las cuales en mi caso ya están respondidas. Así pues, le voy a pedir que profundice un poquitín en algunos temas de un problema tan complejo como el que estamos tratando, con una dimensión yo diría que grandiosa por la amplitud de sus efectos y por cómo afecta a la sociedad en todas sus facetas y en conjunto y también por su recorrido temporal. Y es que no solo estamos hablando del hoy, sino probablemente de un periodo de tiempo bastante largo. La incorporación de una herramienta en las nuevas tecnologías que utiliza el enganche a la red y lo que significa en sí hace que hoy en día la sociedad sea realmente una aldea global no solo por el hecho de tener conocimiento a través de otros medios, y se puede decir que prácticamente todos vivimos en una misma casa, porque es así: desde un terminal de cualquier domicilio se puede estar conectado, con una posibilidad potencial de agresión en otro domicilio de un país distinto en otro extremo del mundo.

Realmente, el riesgo real es el de la conexión en red. Si no fuera así, solo tendríamos que estar pendientes de qué USB conectar, qué disquete o qué otra herramienta de almacenamiento de información en el ordenador, y con pasar un filtro en un momento determinado sería suficiente. Es la red fundamentalmente lo que hace que tengamos un nivel de riesgo muy importante. Eso exige una visión estratégica, tener capacidad de ver a corto, medio y, fundamentalmente, a largo plazo, y también la exigencia de asociarse, cooperar o colaborar, porque solos, de forma aislada, ni los Estados, ni el sector privado, ni el público, ni las personas individualmente, ni las empresas de los distintos sectores van a tener capacidad para defenderse. De hecho, probablemente hoy en día el nivel de organización que tienen los malos —por llamarlos de alguna manera— puede superar permanentemente nuestra propia dinámica, aunque consigamos equipararla conforme vayamos mejorando. En este sentido, se ha referido usted al nivel de cooperación y ha hecho una buena valoración, en líneas generales, de la que existe entre el sector privado y el público y de la Administración con los distintos sectores, y me gustaría que nos informara de cómo es la colaboración y la cooperación en el sector financiero a nivel mundial y en qué cosas sería mejorable, ya que ha mencionado algunos aspectos a mejorar en nuestro país y también a nivel mundial de cara a una defensa común.

Por otro lado, me gustaría que nos ilustrara, si es posible, sobre cómo funciona el protocolo a la hora de identificar una amenaza, cómo se ponen en marcha los procedimientos para establecer los mecanismos de defensa y de respuesta. Ya en una ocasión pregunté en ese sentido a profesionales de otro sector. Con la experiencia que usted tiene en ciberseguridad, en sistemas de información y en los riesgos del sistema tecnológico, quisiera saber si sería posible dar un paso más allá del simple hecho de la defensa para que quien establezca una agresión reciba consecuencias directas en los terminales desde los que ejerce ese ataque. Si existen experiencias en ese sentido, me gustaría saber qué relevancia tienen y la dimensión que se ha podido encontrar en la respuesta: si es eficiente y eficaz o queda mucho por mejorar en este campo.

También nos ha hablado de los retos más importantes para la mejora en líneas generales de la ciberseguridad, poniendo énfasis en el desarrollo e impulso de los sectores profesionales, la cibereducación y la cibersensibilización. Le pediría que añadiera al menos un par de aspectos más, aunque estos son bastante importantes porque estamos hablando del papel de cada persona en esa red mundial y también de los profesionales que nos tienen que defender de las agresiones al sistema. Me gustaría saber si hay algún elemento más de tipo organizativo, de cooperación o de colaboración entre los distintos sectores.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Raffo.

Señora Cabezas, tiene la palabra.

La señora **CABEZAS REGAÑO:** Gracias, presidente.

Bienvenido, señor Barriuso. Como le he dicho al principio de la sesión, como diputada por Córdoba, y por tener el honor de pertenecer a esta comisión, es un placer asistir a esta comparecencia. Hemos visto su amplio currículum, tanto a nivel privado como docente, y creemos que su experiencia es muy importante para esta comisión tras su intervención, con todos los datos que nos ha ido dando.

Su intervención me recuerda mucho a la del director nacional de Ciberseguridad, el señor Ávila, que compareció hace muy poco en el Congreso, tanto porque usted ha hecho un recorrido por lo que está

cve: DSCG-12-CM-124

pasando en un muy corto espacio de tiempo, como por las posibles soluciones a lo que está ocurriendo en nuestro entorno.

En España hay casi 8 millones de personas en el mundo digital, una cifra muy importante. Se habla de que en 2020, aproximadamente, los usuarios de internet llegarán a ser el 53 % de la población. Y en activo hay más de 3 millones de personas. El tema de internet creemos que ha surgido de manera muy rápida y, al revés de lo que ha ocurrido, lo normal es que primero nos formen en las redes sociales, no solo para saber utilizarlas y conocer para qué sirven, sino por el peligro que hay detrás de la pantalla cuando le das a un botón. Eso lo están haciendo en algunos colegios nuestras fuerzas y cuerpos de seguridad del Estado, porque muchos niños no saben que al dar a ese botón se abre una puerta al mundo y que cualquier persona está viendo lo que hacemos, porque además nosotros se lo decimos. Por tanto, como he dicho, sus aportaciones nos parecen fundamentales.

Además, el delincuente o el *hacker* que hay detrás ya no es como el de antes, el delincuente antes era una persona, física, y hoy una persona en un parque con un ordenador puede entrar muy fácilmente en nuestras cuentas, usurpar nuestra identidad, etcétera. Y en cuanto a la pornografía infantil, estamos viendo los datos, escandalosos, que continuamente nos están pasando. Como digo, nos pueden extorsionar, usurpar nuestra identidad... En fin, el delincuente ha cambiado; es un delincuente anónimo físicamente que puede estar en cualquier lugar del mundo y que además se caracteriza, como usted bien ha dicho, por esa evolución tan rápida que está habiendo. Por eso se dice que hoy el *hacker* es el nuevo atracador del siglo XXI, que no lleva pistolas y que desde cualquier punto, por ejemplo, desde un parque, como he dicho, puede hacer todo tipo de actos.

En la comisión sobre el nuevo modelo policial del Congreso, que he mencionado antes, a la cual yo pertenezco, yo hablé sobre algo que el señor Ávila llevó a cabo en Colombia, donde más de 100 000 ciudadanos, a los que se les llama ciudadanos digitales, fueron formados y tienen las competencias necesarias para ejercer sus derechos y responsabilidades de forma digital. Me gustaría que me diera su opinión sobre la posibilidad de que en España existiera eso.

Usted ha hablado también de la formación, de nuestros jóvenes, de nuestros niños, y creo que ahora es vital ese punto en la educación, sobre todo en niños cada vez más pequeños. Estamos hablando de un niño de 3 años, de 5 años, que con un móvil saben más que yo. Es increíble. Yo entiendo que los niños cuanto más pequeños tienen más capacidad de absorber lo que hay a su alrededor. Muchos profesionales opinan como usted, y me ha parecido una buena idea que en la empresa privada también se piense que es una buena opción y que empecemos a trabajar en ese tema.

Los datos del cibercrimen son muy alarmantes, y creo que hay cifras sobre los delitos bancarios bastantes importantes. Por otro lado, el 75% de nuestros escolares sufre acoso escolar virtual.

Creo que es un dato a tener en cuenta desde lo público y lo privado y los poderes públicos tenemos la obligación de recoger todo lo que ustedes puedan aportarnos para empezar a trabajar en ello, porque estamos ante unos delincuentes muy finos que, además, evolucionan rápidamente.

Estamos dando a los niños una *tablet*, un ordenador, un móvil a edades muy tempranas y no les explicamos lo que ocurre, lo que pueden hacer mientras para ellos es un juego. Me refiero a que cada vez vemos a niños más pequeños en las redes sociales. Y hay un dato muy curioso: los padres —en este aspecto debemos hacer una autocrítica— utilizamos la imagen de nuestros niños para decir dónde están, lo que están haciendo, lo que son o dejan de ser; creo que los estamos exponiendo a una ventana bastante peligrosa. Por tanto, formación también para los padres, que tenemos una obligación importante.

Por eso, ante todos esos peligros que le he resumido, le voy a hacer bastantes preguntas; si no puede contestar a todas, me gustaría que nos las enviara porque este tema es importante y debe estar en la agenda política todos los días. No estamos hablando de cualquier cosa y, como he dicho antes, la delincuencia que hay en estos momentos supone no estar seguros en el ciberespacio. Además, España no está entre los diez primeros países más ciberseguros, así que nos queda mucho trabajo por hacer. Me gustaría que usted, que ha trabajado en la empresa privada, nos dijera qué deberíamos mejorar en España, que nos dijera cuáles son sus aportaciones a corto plazo, porque no hablamos de aquí a cinco o seis años. Como usted ha dicho, en el ciberespacio todo avanza en cuestión de minutos y no podemos quedarnos atrás.

También me gustaría saber cómo fortalecer la capacidad de prevención, detección y respuesta, algo que ha mencionado en los últimos meses en algunas de sus comparecencias, congresos o conferencias; usted se refiere siempre a esos asuntos. Es verdad que una sociedad conocedora de las amenazas y desafíos para la seguridad es una sociedad mejor preparada, estamos de acuerdo en eso. Por eso, con

cve: DSCG-12-CM-124

esos conocimientos y experiencias, me gustaría que nos indicara qué debemos mejorar, siempre a corto plazo porque estos proyectos no son a cinco o diez años, entendemos que hay que actuar rápidamente.

Y una pregunta muy importante para el Grupo Popular, que además usted ha mencionado en su comparecencia, es cómo valora el nivel de inversión en materia de ciberseguridad dentro del sector financiero. Usted ha hablado mucho del talento, disponemos de talento, pero no sabemos si es suficiente para cubrir el mercado nacional. Prácticamente me ha dicho que no estamos cubiertos, que necesitamos más personas formadas y desde edades muy tempranas, y por eso es muy importante la Secundaria. El señor Ávila decía en su comparecencia que si se nos escapan esos alumnos y alumnas en la Secundaria, ya los hemos perdido, porque es la edad más fácil para captar ese talento. Por tanto, si nosotros perdemos a los delincuentes del ciberespacio, les van a contratar porque están muy pendientes de esos alumnos que, además de su preparación, tienen capacidad para manejarse en las nuevas tecnologías. Me gustaría que me dijera si esto es cierto o si usted lo cree así.

Queremos saber qué canales de cooperación con las administraciones públicas, en especial con nuestras fuerzas y cuerpos de seguridad del Estado, está llevando a cabo, como usted ha mencionado, el Grupo Santander, y si considera que se puede mejorar y en qué sentido.

También me gustaría saber cómo podemos mejorar las sinergias entre los operadores críticos, en su caso, con el sector financiero y las administraciones públicas en materia de ciberseguridad.

Yo tengo muchas más preguntas pero entiendo que el presidente está siendo muy cariñoso conmigo, porque ya me he pasado. Si usted puede las contesta y si no puede responder nos las manda, pero yo le reitero mi agradecimiento porque creo que es un tema ahora mismo importantísimo, no solamente para el sector financiero sino para el público también, y tenemos que aunar esfuerzos para hacer una sociedad más segura en el ciberespacio.

Muchísimas gracias. Gracias, presidente.

El señor **PRESIDENTE:** Muchas gracias, señora Cabezas. Es muy natural ser cariñoso con las diputadas y diputados de esta comisión.

Insiste la interpelante en que sean soluciones a corto plazo, sabe quién va a estar aquí en la próxima legislatura y, por tanto, nos interesa más lo que nos pueda decir ahora. Tiene la palabra.

El señor **BARRIUSO ROJO** (global CISO, chief information security officer and technology risk, del Grupo Santander): Muchas gracias por las preguntas, la verdad es que son preguntas muy buenas, algunas muy amplias, e intentaré responderlas una a una respetando el orden en que se han hecho, creo que no hay mucho solape, para dar mi punto de vista.

La primera pregunta del señor Yanguas tenía que ver con la identificación de vulnerabilidades, de ataques con habilidades que son desarrolladas en el mundo del ciberespacio; algunas se publican inmediatamente, otras parece que se quedan en una base de datos. Mi punto de vista en esto es que yo soy muy partidario de la detección y publicación responsable de vulnerabilidades. Es importante incentivar eso, incentivar que las personas que tengan interés en esto lo hagan de manera responsable. ¿Qué quiere decir? Uno encuentra una vulnerabilidad, se informa a la organización que la pueda arreglar y, como se arregla, se hace más público. Hay muchas personas que se dedican a eso y es muy bueno, muy positivo. Pero hay otros, distintos grupos con distintos intereses, que lo hacen de otra manera. A mí me gustaría ver a más gente que lo haga de manera responsable; es muy importante.

También había una pregunta, que era en realidad la primera —me la he saltado, discúlpeme, señor Yanguas—, sobre cómo comparamos el Santander con los competidores. Nosotros vemos a nuestros competidores, del sector privado y del público, en ciberseguridad como aliados no como competidores, no buscamos compararnos, lo que buscamos es trabajar juntos. Puedo comentar, por supuesto, qué hacemos en Santander y cómo intentamos avanzar, pero no podría comentar quién va más deprisa o menos deprisa. La clave es no mirar a ver cómo se posiciona uno, sino cómo puede uno colaborar, aprender de otros y contribuir a otros. Esa es la filosofía que tenemos. La verdadera competencia son los criminales, hay que intentar estar lo mejor posible en un mundo que es muy retador.

También hay una pregunta acerca del perfil de los atacantes, sobre cómo los caracterizaría. Yo lo que diría es que la motivación de los atacantes, de los cibercriminales no es muy distinta de la motivación que había en el mundo del crimen antes del ciberespacio, cambian las herramientas. Por ejemplo, vemos que el crimen organizado cada vez utiliza más herramientas cíber como una manera de hacer lo que el crimen organizado puede hacer; las protestas antes eran más físicas y ahora son más *online*. Los actores tienen la misma motivación y distintas herramientas. En algunos casos, como en el mundo del

cve: DSCG-12-CM-124

cibercrimen, el talento a veces se compra, se contrata a alguien que trabaje para organizaciones que se dedican a ese crimen. Es muy importante entender que el crimen es crimen, se haga en el ciberespacio o en la vida real. Pero a veces parece que se idealiza un poco esto del *online* y que no tiene consecuencias, y las tiene, tiene consecuencias, las personas pueden sufrir y es muy duro cuando ves a alguien que ha tenido un problema de ciberseguridad; en el entorno familiar o de amigos seguro que todos conocemos a alguien, y es muy duro y se sufre como ser humano. Es muy importante explicar que el crimen es crimen allá donde se haga. Como ha recordado su señoría antes, creo que sería muy importante intentar captar a las personas que tienen este interés y este talento en el cíber para que sean parte de los que defienden y protegen a la sociedad y a las personas, en lugar de hacer cosas que, sabiéndolo o sin saber, pueden ser delitos.

Respecto al hecho de que parece que hay más reportes de ataques, estoy de acuerdo con eso y, además, todos los informes que están a nuestra disposición nos dicen que cada vez se reporta más porque hay más incidentes y más ataques de cíber. Creo que es una mezcla, por una parte, vemos que a medida que las nuevas tecnologías están más en nuestras vidas hay más ataques; si vemos el ciberespacio como un mundo en sí mismo, está creciendo, con lo cual hay ataques. Y, por otro lado, cada vez se reporta más porque la regulación existente fomenta que se reporte. Por ejemplo, nosotros reportamos los eventos relevantes tanto al regulador como a las agencias relevantes, etcétera. Creo que eso también hace que se reporte más de lo que se reportaba antes, lo cual es positivo y ayuda a ver esa perspectiva de incremento. Con lo cual, no todo el incremento es malo, sino que parte de ese incremento significa que hay más transparencia.

Estoy repasando las notas.

El señor **PRESIDENTE:** No se preocupe, si falta alguna pregunta, hay un segundo turno y los intervinientes podrán subrayar lo que falte.

El señor **BARRIUSO ROJO** (global CISO, chief information security officer and technology risk, del Grupo Santander): De acuerdo. Espero poder cubrir todas.

Había una pregunta relativa a las campañas que se pueden ver en la banca, incluso desde el punto de vista del Banco Santander, donde hay ataques de *phishing,* y es cómo respondemos o cómo lo gestionamos. Intentamos hacerlo de la manera más proactiva posible. Cuando detectamos que hay una campaña que intenta engañar a un potencial cliente o dirigirlo a un sitio que no es el Santander, sino un sitio malicioso, lo reportamos a las autoridades, tomamos las medidas oportunas para intentar que ese sitio no esté disponible porque es fraudulento y, en efecto, nos personamos como parte de la denuncia cuando se consigue encontrar al culpable. Creo que es importante y responsable perseguir los delitos allá donde ocurran. También es importante, cuando se detectan campañas de este tipo, avisar y notificarlo, y de la manera más proactiva posible intentamos informar a nuestros clientes. A veces utilizamos canales amplios como Twitter, pero también en nuestra web o en nuestras comunicaciones a clientes, constantemente, hacemos referencia a lo último que vemos en el mundo del ciberespacio.

Había una pregunta, que creo que es muy amplia, sobre cómo vemos la colaboración a nivel más amplio, a nivel internacional y cómo se puede seguir mejorando. Una cosa que me gustaría poner sobre la mesa es que yo nací en España, en Madrid, pero la mayor parte de mi carrera profesional la he desarrollado en el extranjero, concretamente, en Reino Unido, donde resido. He trabajado en multitud de países y quizás eso me haya permitido tener una visión un poco amplia sobre qué funciona más o qué funciona menos en distintos lugares. Diría que hay una colaboración amplia en España, y es muy positivo, como decía antes. En muchos países, en el sector de la banca, pero también en otros sectores se colabora ampliamente, hay organismos como el FS-ISAC que buscan hacer más colaboración internacional, y eso es muy importante. Si hablamos de amenazas cada vez más globales y de que la mayoría de las entidades tenemos en el corazón defender a nuestros clientes y los sistemas, es decir, no es un tema competitivo, creo que sería bueno fomentar esta colaboración, no solo en países como España, por supuesto, sino también de manera internacional. Nosotros estamos muy a favor de cualquier iniciativa que genere incentivos y sistemas para colaborar y compartir, de hecho, somos muy activos en varias redes internacionales de colaboración.

Otra pregunta que se formula es cómo hacemos cuando identificamos una amenaza y cómo respondemos a ella, cuáles son los mecanismos. De manera muy general describiría dos formas. Hay amenazas que uno identifica porque son conocidas; un tipo de actividad concreta que intenta entrar o que uno ve intentando conectarse es conocido como amenaza, con lo cual, la respuesta suele ser muy rápida

cve: DSCG-12-CM-124

porque la conoces y respondes a ella. Pero hay amenazas que son más nuevas, que nadie ha visto antes y esas son más retadoras, y la manera de abordarlas es buscando la anomalía, lo inusual; un tipo de conexión, un tipo de tráfico, un tipo de actividad que es inusual, y hay que investigar. Nosotros utilizamos sistemas, como el *big data*, que ayuda a correlacionar datos, y también intentamos aprovechar la inteligencia artificial para ser lo más rápidos posible. Siempre hay una parte humana donde el profesional, el experto, juega un rol clave a la hora de entender qué está ocurriendo, y nuestra aproximación es responder lo más rápido posible. Tenemos planes de respuesta que están preparados para, una vez se detecta la amenaza, responder a ella. A veces es una respuesta técnica muy rápida y a veces puede ser una respuesta que lleve más tiempo, más organizativa. Además, pensamos que es muy importante que esos procedimientos, no solo existan en un documento, en un libro, sino que se ejerciten. Así de manera regular hacemos lo que llamamos *board games*: es decir, ponemos un escenario de algo que podría ser real y probamos cómo funcionaría la respuesta para aprender de esa experiencia. A veces lo más práctico para aprender es verse en la situación. Por tanto, hacemos nuestros propios *board games* simulados que nos ayuden a mejorar en nuestros planes de respuesta.

Continuando con la lista de preguntas, la señora Cabezas me ha planteado una serie de cuestiones muy interesantes que intentaré abordar en su totalidad en la medida en que tengamos tiempo.

El primer punto al que se refería es esa iniciativa en Colombia. No la conozco personalmente pero sí he visto de cerca iniciativas similares. Por ejemplo, en Reino Unido hay una iniciativa en la que expertos, profesionales de cíber pueden contribuir a las fuerzas de seguridad en la lucha contra el cibercrimen. De hecho nosotros tenemos en Reino Unido una persona del equipo que colabora con ellos. Allí han creado un mecanismo con el que pueden beneficiarse de la experiencia, de la capacidad de esas personas para combatir ese crimen en el mundo cíber. Y yo creo que puede ser práctico si se hace de la manera adecuada, aunque creo que no ha de reemplazar la capacidad que tiene el mundo de las fuerzas de seguridad del Estado. Pero pensamos que, donde se pueda ayudar, por qué no ver un esquema que fomenta el voluntariado y donde todos aquellos que tengan interés, capacidad y conocimiento puedan aportar un granito de arena, bien sea desde el punto de vista de la formación, ayudando con herramientas o de otras maneras. Creo que esa puede ser una oportunidad en general, pero debería ser un apoyo, nunca una alternativa a que las fuerzas y cuerpos de seguridad del Estado cuenten con los recursos necesarios.

¿Medidas para mejorar a corto plazo? Creo que esta es una pregunta muy buena. Es un tema que me apasiona mucho y podría estar horas y horas compartiendo y escuchando ideas, porque creo que es un reto que todos vemos y que todos tenemos que contribuir a él. Yo creo que a corto plazo en los tres elementos de los que hablaba, que eran concienciación, colaboración y generación de talento, se puede aportar mucho. Creo que son cosas que se pueden hacer más o menos rápido porque, además, los seres humanos aprendemos rápido y podemos beneficiarnos muy rápido de información y de conocimiento, y los niños, que usted mencionaba, más todavía. También hay medidas técnicas que desde los organismos públicos se pueden fomentar. Algunas están en marcha, otras todavía no, y creo que deberían estar apoyadas con el presupuesto adecuado. Es decir, hay que invertir en capacidades que nos ayuden a detectar ataques en el territorio nacional, invertir en sistemas de alerta temprana, invertir en herramientas de reporte, en herramientas de gestión de riesgos. Creo que esto es muy importante y sería muy bueno fomentar que se siga desarrollando. Mi punto clave aquí sería lo que le he explicado antes, y es que la estrategia de seguridad nacional será mucho más efectiva si viene dotada en un presupuesto asignado y dedicado a cíber. En el debate sobre si algo en cíber se puede hacer o no, se puede agilizar, creo que la clave es que haya consenso y que las medidas se tomen de manera rápida.

¿Cómo se valora la inversión dentro del sector financiero? Yo creo que en el Santander, sin ninguna duda, y en el sector financiero en general la ciberseguridad se entiende como una prioridad y un área de inversión. Se invierte como uno de los sectores que más recursos dedican a la ciberseguridad. No es el único, hay otros sectores, y yo creo que es importante que, en realidad, todo el tejido del sector privado, y también el público, entienda que quizá esto de la seguridad, que a lo mejor hace quince o veinte años para algunos sectores era menos importante, va a ser importante para todos. Con lo cual, el mensaje para mí es que todos los sectores han de invertir en ciberseguridad y que nadie es ajeno a esto. De hecho, en sectores que tradicionalmente eran muy físicos ahora vemos que cada vez están más en el espacio cibernético, internet de la cosas. Lo que antes era un motor y ya está, ahora es un motor que se comunica con internet. Pienso que hay una oportunidad para que todos los sectores piensen que la seguridad es una inversión.

cve: DSCG-12-CM-124

Respecto al talento, en España lo vemos como un reto. Creo que hay mucha demanda de ciberprofesionales y sería muy positivo abordarlo. Para mí una oportunidad clave de la que hablábamos antes está en los niños y niñas desde el momento en que están en la escuela, aunque estoy totalmente de acuerdo en que en las madres y padres también es importante. La educación secundaria creo que puede jugar un papel clave. De hecho, ese talento no solo es bueno para defendernos, sino para crear crecimiento económico. Para empezar, empleo, por supuesto, pero también empresas que se dediquen a esto de cíber, que es un sector en auge. Si tenemos buen talento y tenemos un buen ecosistema creo que podemos aprovecharlo no solo para satisfacer la demanda de defensa, sino también para que innoven, creen ideas, creen *startups*, creen empresas. Yo creo que la educación secundaria puede ser el pilar clave porque, en efecto, ahí es donde los niños y las niñas empiezan a tomar la decisión sobre su carrera y si la ciencia no te atrae en ese momento, será difícil que te atraiga más adelante. Para aquellos que les atrae y que siguen ese camino, la universidad juega un papel clave y, de nuevo, para mí un currículum de ciberseguridad que se pueda elaborar de manera ágil, quizás de una manera distinta a otras áreas, entre los sectores públicos y privados sería muy positivo. Además, es una carrera muy bonita, muy interesante y que puede aportar mucho a las personas que se dedican a ello, con lo cual, si lo fomentamos poniendo sobre la mesa un currículum que te diga que si acabas eso puedes ser un ciberarquitecto o un *hacker* ético; si damos eso como formación, creo que podría ser muy positivo.

En cuanto a los canales de cooperación, vemos muchos. En España, como comentaba, nosotros tenemos acuerdo de colaboración con múltiples entidades. También hay canales de cooperación voluntarios donde se comparte información para mejorar el ecosistema. En el sector de la banca se colabora y se comparte información sobre mejores prácticas y cómo estar todos mejor protegidos y me consta que en otros sectores también. Es importante que veamos los canales de cooperación como un mecanismo voluntario y flexible. En aquellos lugares donde se ha hecho muy rígido, al final, ha sido menos efectivo porque lo que buscamos es que se genere valor añadido, no que se haga *tic* en una caja. Para mí, cuanto más flexible, cuanto voluntario y más suponga animar e incentivar en lugar de poner un esquema rígido, más positivo será.

Desde el punto de vista internacional, en Estados Unidos hemos visto en los últimos años muchos avances en este mundo. De hecho, tienen una serie de ecosistemas que llaman los FS-ISAC. ISAC es el término que utilizan para la célula de colaborar y está FS Financial Services, Oil & Gas, etcétera; tienen una serie de componentes que les permite compartir información en tiempo real, con sistemas donde uno pone la amenaza, y eso se publica al resto de miembros y, además, con esquemas muy bien pensados sobre el nivel de confianza: verde, ámbar y rojo. Cuanto más sensible es el dato, más cuidado se tiene al compartir. Y hay alguna información que al ser verde y de carácter menos sensible se comparte de forma mucho más amplia. Hay mecanismos que se pueden reutilizar y podemos beneficiarnos viendo la experiencia de otros.

Desde el punto de vista del ecosistema privado y público, creo que es muy importante y además muy útil que compartamos y colaboremos y para mí, más allá de compartir amenazas o mejores prácticas, hay que compartir lo más ampliamente posible: ideas sobre formación, educación, concienciación, cómo abordar este reto juntos y también cómo hacer una oportunidad. Yo creo que hay una oportunidad y espero que la Estrategia de seguridad nacional nos ayude a abordarla y, quizás, a mirarla como una oportunidad.

Creo que he respondido a todas las preguntas. Si me he dejado alguna, por favor, no duden en replantearla.

El señor **PRESIDENTE:** Lo vamos a comprobar en el acto.

Señor Castellana, ¿alguna pregunta se ha quedado en el tintero?

El señor **CASTELLANA GAMISANS:** Gracias.

En cuanto a las dos preguntas que le he hecho, evidentemente, estamos de acuerdo con el sistema que hemos comentado de publicación responsable de vulnerabilidades, que es lo que nos permite que los sistemas sean parcheables. Lo que pasa es que ahora se ve mucho más explícito. Agencias gubernamentales, muchas de carácter occidental, europeas o americanas, son las que tienen estas vulnerabilidades y son las que la utilizan en el ámbito de la ciberdefensa para ciberatacar. Hay empresas privadas que se dedican a recopilar estas bases de datos para ponerlas a disposición de esas agencias gubernamentales para sus actividades. Esto va en contra de las buenas prácticas. Seguramente no sea usted el interlocutor para hacerle esta pregunta, pero estas prácticas que permiten generar capacidades

cve: DSCG-12-CM-124

cibermilitares van en contra de las buenas prácticas de seguridad que nos interesan a todos. En ese sentido le interpelaba a usted, para hablar claramente de los agentes a los cuales me refería.

Por lo que refiere al conocimiento del atacante, tan solo compartir la percepción desde otro lado. Es decir, mientras que en mundo tradicional, que aún existe, había y hay una identificación mucho más clara de los grupos criminales, de las mafias, de los cárteles, de las organizaciones que hay detrás de esta actividad criminal, en el cibercrimen hablamos constantemente de los ataques. Nos han comentado que acaban cayendo criminales de este tipo pero, en cambio, no tenemos una radiografía para entender, básicamente, quién está detrás y así poder tener terapias contra este tipo de actitudes.

Si sobre estas cuestiones puede añadir alguna cosa más estaría bien, si no, lo dejamos aquí. Le agradezco la información y la luz que nos ha dado sobre este tema.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Castellana.

Señor Comorera, ¿hay alguna cuestión que se haya quedado pendiente? **(Denegaciones).**

Muchas gracias.

Señor Raffo, tiene la palabra.

El señor **RAFFO CAMARILLO:** Gracias.

Sí, fundamentalmente, quiero que me aclare dos cuestiones. Ha comentado que en líneas generales funcionaba relativamente bien todo el asunto relacionado con la cooperación y la colaboración con los organismos públicos y con los sectores privado y público en nuestro país, pero que había algún margen de mejora. Me gustaría, si puede, que comentara algo al respecto, sobre cuál sería el margen de mejora y si se refiere a los asuntos organizativos. Por ejemplo, la primera vez que yo analicé el sistema con todos los elementos me pareció un rompecabezas brutal, o sea, no está nada simplificado. Los norteamericanos aprendieron bastante del famoso atentado de septiembre. Hoy llaman comunidades de inteligencia a lo que antes eran un montón de agencias —le estoy poniendo un ejemplo, no tiene que ver con esto, aunque algo sí en algún los apartados— y lo resolvieron, lógicamente, generando una organización mucho más dúctil, más fácil de entender, de comprender y de interrelacionarse. En cualquier organización el principio de autoridad, estructura y jerarquía tiene que estar claro, pero si aparecen muchos elementos, como champiñones, es complicado de gestionar. Lo que estoy haciendo es una introducción a modo de marco, pero lo que le pregunto es si ve algún aspecto relacionado con la organización.

La otra cuestión tiene que ver con los procedimientos. Me interesa saber la comunicación que existe cuando en un momento determinado se identifica un riesgo, con qué agilidad y con qué rapidez se responde. Estas son las dos cuestiones que quiero que me aclare, si puede y si tiene conocimiento sobre esos aspectos.

Lo otro tiene que ver con lo siguiente. Yo soy de los que piensan que a esas personas que pueden poner en riesgo la estabilidad entera del sector financiero de un país a nivel mundial, que son responsables de las tensiones internacionales entre distintos países, responsables de las infraestructuras críticas en un país —que pueden producir, entre comillas, «catástrofes importantes», desde catástrofes económicas hasta físicas— les sale bastante barato. No hablo del Código Penal —que ahora lo comentaré—, digo que si todo consiste en obtener como resultado el fracaso y volver a intentarlo, lo voy a volver a intentar. Lo tengo clarísimo; yo por lo menos lo tengo clarísimo: volvería a intentarlo. En concreto, estaríamos sometiendo la situación en la que estamos a la dinámica de prueba error, en la que siempre sale ganando el que hace la prueba: el atacante. La pregunta que yo hacía era: ¿hoy día se están estudiando sistemas, herramientas, instrumentos, métodos, procedimientos en los que no le salga gratis tantear una agresión a un agresor?

Ahora voy a lo siguiente. Con su experiencia y la responsabilidad que tiene —porque a fin de cuentas estamos hablando de un banco que está instalado a nivel mundial—, ¿es suficiente lo que plantea el Código Penal en cuanto a las penas de los que hoy consideramos que pueden ser potenciales delitos o los que antes no lo eran y ya lo son? ¿Tienen suficiente castigo?

No sé si me he explicado con claridad.

Gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Raffo.

Señora Cabezas, tiene la palabra.

cve: DSCG-12-CM-124

La señora **CABEZAS REGAÑO:** Gracias, presidente. Muy brevemente.

Vuelvo a la docencia, donde yo creo que es importante que insistamos mucho y trabajemos tanto a nivel privado como público: ¿qué perfiles de talento podría describirme con el fin de modificar —si hubiera que hacerlo— los planes de estudio, tanto en el nivel universitario como en formación profesional, para dar respuesta precisamente a ese mercado que hace un momento nos comentaba para seguir trabajando en la ciberseguridad? Esa es la única pregunta que le formulo.

Le agradezco su comparecencia porque son aportaciones importantes y creo firmemente que tanto a nivel público como a nivel privado tenemos que trabajar y colaborar mutuamente ante este gran reto del ciberespacio. La ciberseguridad nos afecta a todos y va a seguir afectando a las nuevas generaciones. Tenemos que estar preparados para el gran reto de ese nuevo delincuente que no tiene cara, ni brazos, ni piernas, al que no vamos a ver pero que está en cualquier parte del mundo y nos puede usurpar tanto la identidad como desvalijar las cuentas del banco, tengamos mucho o tengamos poco. Estamos en un enorme peligro. Por lo tanto, creo que es importante esa colaboración público-privada, y le agradezco enormemente su comparecencia y la oportunidad que me ha dado de poder participar en esta comparecencia.

Gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señora Cabezas.

Vuelve a estar usted en el uso de la palabra, señor Barriuso.

El señor **BARRIUSO ROJO** (global CISO, chief information security officer and technology risk, del Grupo Santander): Muchas gracias.

No puedo opinar sobre lo que cada uno hace con las vulnerabilidades que encuentra, es difícil para mí poder tener un punto de vista sobre lo que distintos organismos hacen. Lo que sí puedo decir es que creo que es muy importante que todos seamos proactivos para encontrar esas vulnerabilidades y cerrarlas. Nosotros, en el Santander, estamos siempre buscando qué vulnerabilidades hay nuevas, cuáles se conocen o se van a conocer e intentar crear un sistema lo más rápido posible. Pensamos que eso ayuda a un ecosistema positivo.

Un punto muy positivo que usted elaboraba es la atribución, cómo conocer el perfil de los atacantes para poder protegernos lo mejor posible. Está muy en boga en seguridad todo este mundo de la atribución, que, además, tiene que ver también con la persecución. Lo que yo comentaría sobre esto es que cada vez es más importante entender las técnicas, los procedimientos, los métodos de ataque para poder estar preparado lo antes posible no solo para el que ha venido, sino para el que va a venir.

Por ejemplo, hablaba de nuestra filosofía de ciberseguridad y sobre anticipar, es lo que nosotros llamamos ciberinteligencia; intentamos conocer lo mejor posible a aquellos que pueden llevar a cabo un ataque para estar prevenidos lo mejor posible. No es fácil porque es muy dinámico, cambia mucho, pero si consigues entender la herramienta que se utiliza en este tipo de ataques, te ayuda mucho si viene otro con la misma herramienta. Entonces sí ponemos el esfuerzo en intentar entender ese perfil, muchas veces técnico, de los distintos atacantes. Y es curioso además que cada atacante tiene su propio perfil. Generalmente puedes ver distintos atacantes basándote en cómo operan.

La pregunta sobre el margen de mejora. Yo quizás hablaría de dos puntos que nos pueden ayudar a mejorar: uno es la agilidad a la hora de compartir sistemas en tiempo real; a fin de cuentas, cuanto más podamos automatizar, desde que encontramos amenazas hasta que conseguimos protegernos, mejor. Creo que hay que seguir fomentando sistemas para compartir información de amenazas, indicadores de compromiso. Toda la información técnica en tiempo real, mejor. Y creo que la herramienta Ícaro que tenemos es un buen camino a seguir. Se trata de que esté lo más implantada posible y de que todos podamos beneficiarnos lo más posible de lo que todos compartimos.

Y algo que yo haría es encontrar la manera de tener un mecanismo único, lo más centralizado posible, para reportar eventos e incidentes. Cuanto más fragmentados estemos, más tiempo lleva y más parcial es la información que recibimos. Somos partidarios de un mecanismo único al que uno pueda acudir para aportar y recibir información. Y creo que es muy importante que sea bidireccional. La información ha de fluir en los dos sentidos. Es bueno aportar y también es bueno entender qué se ha conseguido con eso, qué sabemos a través de otros y crear el ecosistema más seguro posible.

En cuanto a la pregunta de la atribución desde el punto de vista de cómo podemos hacer que haya más consecuencias en los ciberataques, le diré que es cierto que hay mucha conversación en el mundo cíber sobre esta idea de atacas de vuelta, pues atacas tú si te atacan. Es un tema complejo, porque, a

cve: DSCG-12-CM-124

menudo, el atacante no ataca desde su sistema, sino que ha entrado en el de otra persona o en el de otra entidad, para atacar desde ahí, o hay varios en la cadena. Con lo cual, es arriesgado si uno se precipita e intenta responder donde cree que viene el ataque, porque puede causar un doble daño. Este es un tema delicado y creo que el sector privado tiene que ser muy cauteloso. Creo que las fuerzas y cuerpos de seguridad del Estado son los mecanismos adecuados para perseguir estos delitos. Quizás ahí está la clave, en cómo podemos trabajar internacionalmente para perseguir los delitos de la mejor manera posible, de la manera más rápida posible: Europol, Interpol... Cuanto más ágil sea esa persecución, mejor, porque, obviamente, a menudo la investigación no es solo en un país. Si hablamos de que hay varios saltos para llegar a una víctima, generalmente, la investigación puede requerir colaboración a través de muchos países. Quizá el ciberespacio enfatiza esa necesidad de poder operar de manera muy ágil a la hora de perseguir delitos.

Le diré en cuanto a la pregunta sobre si las penas son adecuadas que no soy abogado ni experto jurídico. Sí creo que en España contamos con un cuerpo jurídico que es positivo y que persigue estos delitos. Quizás el reto es seguir avanzando a la hora de poder abordar a los delincuentes, porque la atribución no es fácil, no lo es desde que hay un evento hasta que se consigue determinar al culpable y encontrarlo. Es importante que todos los que nos vemos en este mundo de la ciberseguridad, que somos parte de ello o víctimas de ello en algún momento, contribuyamos y persigamos el delito de forma que no quede impune. Creo que eso es muy positivo.

Y, finalmente, la pregunta sobre docencia. Yo soy muy apasionado de ese mundo y he contribuido con la universidad bastantes años. Además, creo que es muy bonito, porque uno se da cuenta de cómo ayudar a educar a la gente más joven o a aquellos que tienen interés generalmente es un proceso de aprendizaje también para aquellos que educan y para los profesores, con lo cual, yo solía aprender más de lo que enseñaba, máxime en este mundo, donde muchas personas son autodidactas.

Para mí, el mundo del cíber necesita formación en ciencias: matemáticas, informática —yo soy informático—, telecomunicaciones o ingenierías. Las matemáticas son muy útiles para el cíber. Creo que hay un montón de perfiles que me llevaría unos minutos enumerarlos: desarrolladores de código seguro, arquitectos, hackers éticos... Hay una serie de perfiles que en un futuro podrían regularizarse como carreras profesionales, con sus *skills*, con su formación adecuada, con partes comunes y con partes muy especializadas. Y creo que cada vez van a tener más demanda. Con lo cual, la oportunidad de conseguir que tengamos más profesionales y que salgan lo mejor formados posible de la universidad está ahí.

El señor **PRESIDENTE:** Muchísimas gracias.

Antes de despedir al compareciente, quiero comunicar a los portavoces que tendremos que convocar, con una cierta premura, Mesa y Portavoces para decidir sobre las comparecencias que están pendientes, para decidir si las mantenemos o no las mantenemos, con el propósito de tener ya un borrador sobre la ponencia, que empiece a circular, si el letrado no me engaña y no tiene ninguna razón para hacerlo, a partir de mediados de enero, cuando ya podríamos ir pasando de las musas al teatro y empezar a tener conclusiones.

Esta comparecencia nos ha sido muy útil, como todas las demás, para orientar a la comisión en las recomendaciones que tienen que ver en este terreno.

Le doy las gracias más efusivas por su comparecencia, por su presencia, por su claridad y por el carácter exhaustivo de sus respuestas.

Se levanta la sesión.

Eran las dieciocho horas y cuarenta minutos.

cve: DSCG-12-CM-124