DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 90 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 15

celebrada el jueves 12 de abril de 2018 en el Palacio del Senado

---

Página

ORDEN DEL DÍA:

Comparecencias:

---

cve: DSCG-12-CM-90

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

El señor **PRESIDENTE:** Señorías, buenas tardes, vamos a dar comienzo a esta sesión, no sin antes agradecer al Senado su hospitalidad.

COMPARECENCIAS:

— DE DON FERNANDO PICATOSTE, SOCIO RISK ADVISORY (DELOITTE), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Senado 713/000663 y número de expediente del Congreso de los Diputados 219/001131).

El señor **PRESIDENTE:** Hoy tenemos dos comparecencias y vamos a proceder en el acto a dar la palabra a don Fernando Picatoste, que es el primer compareciente. Tiene usted la palabra.

El señor **PICATOSTE MATEU** (socio Risk Advisory, Deloitte): Buenas tardes a todos. Muchas gracias por invitar a Deloitte. En nombre de todos los socios de Deloitte, agradezco esta oportunidad. Lógicamente es un honor estar aquí con todos ustedes y espero que sea de utilidad a la comisión. **(El señor compareciente apoya su intervención con la proyección de diapositivas).**

Voy a ir muy rápido, y como sé que luego hay dos turnos de preguntas, tendrán ustedes ocasión de preguntar todo lo que consideren oportuno.

Es pertinente que hable un poquitín acerca de Deloitte —ya verán ustedes el motivo—. Luego hablaremos muy brevemente del contexto de ciberseguridad y finalmente de un reto y una oportunidad para España, desarrollado de una forma bastante ágil.

Como ven en esta proyección, somos líderes de servicios de ciberseguridad. Deloitte es la firma de servicios profesionales más grande del mundo; somos más de 250 000 en el mundo, 8000 en España. El capital de Deloitte España es cien por cien español. Los socios españoles somos los propietarios de la firma y hace cinco años iniciamos una andadura hacia una aproximación global de la ciberseguridad. Esta andadura se inició cuando nos dimos cuenta de que para hacer crecer esto de una forma ordenada no podíamos llevar a cabo cada uno acciones individuales, sino que debíamos colaborar en una estrategia clara y unificada. Deloitte España fue la primera en dar un paso al frente y tenemos un centro de operaciones de ciberseguridad que hoy en día da servicio a Europa, Middle East y África, con más de 200 multinacionales internacionales, muchas de ellas sin presencia en España. Por tanto, estamos exportando desde España servicios de ciberseguridad. Este es el *leit motiv* de por qué introducía este punto.

Como ven, estamos conectados con una serie de centros de ciberinteligencia, porque la ciberinteligencia hay que hacerla en idiomas locales, ya que, especialmente en la región de Europa, Middle East y África, el lenguaje es un tema diferenciador. Tenemos centros en Israel, en Turquía, en Alemania y en Holanda, porque la gente que interviene en esos foros habla en esos idiomas.

Les traigo también una proyección sobre cómo enfocamos nuestra ciberseguridad. Lo hemos simplificado mucho para que les sea muy fácil de entender a la alta dirección de las empresas, que es la que se encarga de hacer sostenible la ciberseguridad en esas grandes empresas. Hay que tener una estrategia clara, que es lo que va a ayudarnos a trazar un camino claro por el que abordar las necesidades y hacer un uso eficiente de los recursos. La amenaza es muy grande, pero hay que priorizar cómo la mitigamos.

Sintetizamos la ciberseguridad en tres palabras: protección, vigilancia y resiliencia. Respecto a la primera, toda la vida hemos estado trabajando en poner controles de seguridad. Donde hay que hacer más énfasis actualmente es en la vigilancia, en qué nos dicen esos controles de ciberseguridad y especialmente qué hacemos en caso de que una crisis suceda, y es entrenarnos para la resiliencia. Nosotros damos servicios externos, damos consultoría, también operamos la ciberseguridad de nuestros clientes y, muy importante, formamos a nuestros clientes, porque también hay clientes que necesitan tener sus capacidades propias.

En cuanto al cambio de paradigma de la ciberseguridad, el World Economic Forum lleva hablando de la ciberamenaza desde los últimos siete años; siempre salen en el cuadrante de los riesgos más frecuentes, tienen probabilidad del cien por cien, siempre suceden, siempre están sucediendo cosas. El punto de realidad ha sido el incidente global *wannacry* que, como ustedes saben, en muy poco tiempo demostró que todo el mundo podía estar expuesto ante una vulnerabilidad.

cve: DSCG-12-CM-90

Se habla mucho de la amenaza; pero, basándome en algunas ponencias anteriores que he visto, creo que es interesante hablar de impacto, porque muchas veces se habla de cuál es la amenaza, pero no tanto de cuál es el impacto. Lógicamente, asociado a una ciberamenaza hay un coste económico fuerte —luego desarrollaré cómo evoluciona en el tiempo este coste—. El coste operativo es evidente: no tener disponibles los sistemas. ¿Quiénes de ustedes pueden trabajar hoy en día sin correo electrónico, teléfono móvil o sin acceso a su base de datos? El coste operativo es muy claro. Pero lo que más teme la mayor parte de la gente es el impacto reputacional, es decir, un impacto en un activo intangible, en la marca, en la reputación, que además tarda muy poco en destrozarse y mucho en recuperarse. Esta es una visión de los grandes impactos de la ciberseguridad.

Aquí les doy una visión temporal. Lógicamente, el primer impacto es el coste directo; en el momento de la ciberamenaza hay que restituir los activos, hay que poner en marcha planes de acción, pero justo cuando estamos terminando esto, las organizaciones tienden a hacer planes a cien días; es decir: vamos a contraatacar. Aparecen los planes, que tienen un mayor calado, aparecen los costes indirectos, que no habían aparecido hasta entonces. Ya cuando está terminando esta curva, aparecen los de largo recorrido, porque esto ha venido para quedarse. No podemos pensar que con hacer un plan de acción ya está todo resuelto, sino que el tema va a continuar durante bastante tiempo.

He ido muy rápido intencionadamente. Luego ustedes me preguntan lo que quieran.

Les traigo aquí, como les decía, un reto, solamente uno, porque creo que es lo prioritario, y luego una gran oportunidad. El reto inmediato es qué vamos a hacer con la próxima gran ciberamenaza. Es cierto que *wannacry* ha sido una demostración de que hemos trabajado juntos como una nación, se ha colaborado muy bien. Hay que hacer énfasis en la gobernanza de cómo se gestiona una crisis y en seguir manteniendo el nivel de colaboración y los estándares de confianza mutua. Me gustaría hacer un inciso para decir que el nivel de colaboración de la industria de ciberseguridad española es excelente en todos los ámbitos, tanto en lo público como en lo privado. En el caso de este ciberincidente todos pusimos nuestro granito de arena para tratar de ayudar y solventar la situación.

Como les decía, el *wannacry* sirvió para poner planes de acción inmediatos. Las organizaciones dijeron: yo tengo ya instrumentos, pero voy a reforzar los planes, porque realmente hay cosas que todavía no tengo contempladas, y voy a acometerlos. Es una gran recomendación, cada vez que tengamos un impacto, buscar un plan de mejora para solventar lo que lo ha generado.

Tenemos que seguir trabajando en el liderazgo y la coordinación, pero el gran reto es estar preparados para hacer una gestión adecuada de las crisis. Si entrenamos las capacidades de gestión de crisis, seremos capaces de recuperarnos antes que si no las hemos entrenado. Ese es el principio básico en el que hay que seguir trabajando para coordinar todos los efectos.

Les hablaba de un reto: la amenaza inminente, y de la oportunidad. Les pongo el ejemplo de Israel, y lo ligo con lo que he comentado de Deloitte. Israel tiene el 5 % del mercado mundial de la ciberseguridad, y además, cada vez hay más inversión en *startups* israelíes. Es un movimiento que está muy potenciado por el Estado israelí: hacen publicidad de las empresas, nos llevan a viajes a Israel. El que no haya estado en Israel en una empresa de ciberseguridad parece que no tiene cabida en el mundo actual. Es un movimiento claramente incentivado que tiene un retorno económico relevante para el país, como todos ustedes saben. De hecho, Israel sale en los índices de ciberseguridad justo detrás de Estados Unidos, que, por volumen, es el mayor consumidor.

Si la oportunidad es generar dinero y empleo a través de la ciberseguridad, ¿qué tendríamos que hacer? Hay tres líneas de actuación. La primera es liderar sin miedo tanto en entornos nacionales como internacionales. Como ustedes pueden ver, hay una serie índices, y si en esos índices España tiene que ser la mejor reflejada, enfoquemos el trabajo en salir mejor reflejados en dichos índices. Lógicamente, se ha trabajado mucho en la Estrategia de Seguridad Nacional 2013, de ahí emana la Estrategia de Ciberseguridad, y se ha hecho un refinamiento en la Estrategia de Seguridad Nacional 2017. Hay información valiosísima en esos documentos, puesta en común por la gente que más sabe de ciberseguridad en este país. ¿Qué nos falta? Impulsar todo esto con un plan; no nos podemos quedar en que hemos hecho una estrategia, pero todavía no hemos pasado a la operativa.

Cuando hablamos de liderazgo significa ocupar posiciones relevantes en órganos relevantes de la ciberseguridad. Está Enisa, y tenemos la oportunidad de mandar españoles y tener representación directa en esa empresa. También está la OTAN, tenemos que mandar españoles allí, así como Europol. Pero

cve: DSCG-12-CM-90

tiene que haber un soporte. Lo que nos pasa a los españoles es que muchas veces nos vamos con nuestra mochila y armados con un mondadientes tratamos de conquistar el mundo. De lo que se trata es de impulsar esto de forma clara.

Tenemos la oportunidad de asociar la marca España a la ciberseguridad. Gran parte de los ingresos de España vienen del turismo. Como somos más seguros que nuestros países circundantes, los índices de visitas a nuestro país están aumentando. Les voy a poner un ejemplo que me contaron en Singapur. Singapur, una colonia empobrecida al final de la península de Malasia, con un río contaminado, decide hace veinte años convertir el país en otra cosa y apuestan por convertirlo en el *hub* de acceso de entrada hacia el sudeste asiático, focalizándose en temas como las comunicaciones y la protección de las marcas. Ustedes saben que es muy típico estar en Singapur y decir: multa por. Te multan por cualquier cosa y la propiedad intelectual se protege extremadamente. Las grandes corporaciones tienen allí sedes muy relevantes con el fin de entrar en esos negocios.

Finalmente, en el liderazgo hay tendencias —se ha hablado ya en esta comisión de la digitalización— Está el internet de las cosas, el IoT. En estas tendencias tenemos que demostrar que la industria española es líder. Con esto ganaremos por la mano a otros que están en ello.

Hemos hablado de la dependencia del *phishing* de los móviles por la movilidad. Este es otro aspecto en el que la industria española debería enfocar sus esfuerzos, y, por supuesto, también en defensa —y me parece muy oportuno que comparezca el general Goberna a continuación—.

La segunda línea de actuación es potenciar el ecosistema, como les he mencionado, el caso de Israel no está exento de un gran apoyo institucional. Te invitan a visitar instalaciones militares con cierta tecnología. Cada vez que viene uno de sus representantes comerciales, la embajada vuelca todos sus medios para convencernos de que debemos asistir a todos sus eventos. Deberíamos ayudar a potenciar ese ecosistema.

Por supuesto, se ha comentado bastantes veces en esta comisión que hay que aumentar el presupuesto que se dedica a todos los temas de seguridad, pero hay que hacer una apuesta decidida por aumentar el I+D+i. Tradicionalmente, lo que nos encontramos son consorcios españoles que tiran de los planes H 2020, u otros consorcios, para conseguir algo en lo que no tenemos suficiente presupuesto. Alguno habría que repensarlo, ya que, ¿por qué vamos a contar lo que necesitamos para España en este tipo de foros y hacerlo absolutamente público, si lo que necesitaríamos es impulsarlo directamente nosotros? Hay muchísimo emprendimiento. Existen pymes en el mercado español dedicadas a la ciberseguridad que están haciendo un trabajo muy fuerte, y además algunos organismos les están empezando a apoyar, como, por ejemplo, el Incibe.

En cuanto a dinamizar el mercado, lógicamente ya he hablado de la oportunidad exportadora, pero también hay que dinamizar el mercado nacional, y aquí siempre se ha puesto de ejemplo el DNI electrónico; y la oportunidad es la compra pública innovadora; es decir, ver cómo utilizamos algún proyecto tractor que ayude a desarrollar capacidades dentro del entorno español.

Finalmente, para que realmente podamos capturar la oportunidad, necesitamos aumentar las capacidades del país. Nuestro país ha sido de poner muchos controles; el reto todavía está en la parte de monitorización y respuesta. Pero tenemos que trabajar desde la base para formar cada vez más talento. Hay mucho talento en los universitarios españoles, estamos muy bien considerados fuera de nuestras fronteras, pero debemos hacer formación específica en capacidades de ciberseguridad a todos los niveles. Y, por supuesto, para aumentar la conciencia y la resiliencia, no hay nada más eficaz que la formación y la cultura. Si no sabemos que estamos haciendo un uso inseguro de las redes y de los mecanismos de telecomunicación, lógicamente lo seguiremos haciendo y seguiremos estando igual de expuestos.

Con esto concluyo mi ponencia.

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

A continuación, pasamos al turno de portavoces, empezando por el señor Yanguas, del Grupo Mixto.

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

Al igual que en su día le solicité que alguna comisión se celebrara aquí en el Senado, hoy quiero agradecerle que haya elegido esta casa para las sesiones de hoy. Que quede constancia.

También quiero agradecerle al ponente sus explicaciones. Cuando hablaba de los retos o de las amenazas creo que ha dicho que hay que seguir entrenando. No sé cómo habría que entrenar o a qué se

cve: DSCG-12-CM-90

está usted refiriendo exactamente con esto. Si me lo pudiera ampliar un poco, se lo agradecería. Lo demás me ha quedado bastante claro. Simplemente quiero agradecerle sus explicaciones esta tarde hoy aquí en el Senado.

Muchas gracias.

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

Tiene la palabra el señor Legarda.

El señor **LEGARDA URIARTE:** Muchas gracias, presidente.

Hago uso de la palabra únicamente para agradecer al compareciente las explicaciones y la información que nos ha facilitado.

Muchas gracias.

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

Señor Gutiérrez, tiene la palabra.

El señor **GUTIÉRREZ VIVAS:** Gracias, señor presidente.

Muchísimas gracias, señor Picatoste, por su exposición, que ha sido amena e instructiva. Ha hecho usted una presentación de Deloitte, conocida por todos como una gran empresa y también como una gran consultora y, desde luego, pionera en la consultoría de los servicios de ciberseguridad y de seguridad integral.

Creo que ustedes tienen grandes clientes y, por tanto, me parece que las grandes empresas españolas, a través de consultoras como Deloitte y otras que también se ocupan de esto, tienen bastante bien resuelto, por lo menos, cómo afrontar estos retos, porque las soluciones las tienen. Creo que también tienen la capacidad de inversión, y eso forma parte de la solución.

Creo que en las pymes, Incibe está haciendo una gran labor, aunque nunca será suficiente, desde luego, para llegar a todas las pymes. Quizá dentro del tejido empresarial hará falta —pero ese es otro tema— otro tipo de empresas que, sin llegar a ser Deloitte, puedan dar solución a las pymes a otros precios, que no son los que probablemente puedan pagar a consultoras como la suya.

A mí lo que me preocupa es la Administración. Desde el punto de vista de la Administración, me gustaría saber por qué cree usted que hoy en día no hay ninguna dependencia de la Administración española que esté certificada, por ejemplo, en una ISO 27001. ¿Qué falla en la Administración española para que no esté certificada, no tenga los mecanismos de seguridad adecuados y no tenga planes para la protección de sus infraestructuras y de sus servicios de información? Muchas empresas se están preocupando de esto, pero la Administración no lo hace y no entiendo muy bien por qué. No sé si se han dirigido a ustedes o no. ¿Cree que hay interés pero falta presupuesto? ¿Cree que falta conocimiento dentro de la propia Administración, que también pudiera ser? ¿Falta sentido de la amenaza o del riesgo que supone tener a la Administración española sin certificado de ninguna norma de seguridad? ¿Cuál es su visión al respecto?

La segunda pregunta que me gustaría hacerle es ¿hasta qué punto entiende usted que las operadoras que dan acceso a la red tienen responsabilidad? ¿Cree que podrían hacer más por mejorar la seguridad de sus propios usuarios? Evidentemente, el usuario tiene una responsabilidad, sea un usuario doméstico o cualquier empresa que utiliza los servicios globales de comunicación para desarrollar su negocio o para darle soporte, que hoy en día, como usted bien nos ha contado, es imposible hacerlo sin un correo electrónico y sin una página web, pero quizá los operadores podrían hacer algo más. ¿Cree usted que pueden hacer algo más? Y en ese caso, ¿qué podrían hacer?

Muchísimas gracias, señor Picatoste.

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

Tiene la palabra la señora Angustia.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.

Gracias, señor Picatoste, por sus aportaciones hoy y por haber venido a esta comisión.

Hay un ámbito de trabajo tremendamente importante que realiza el compareciente y que hay que valorar: el trabajo múltiple que hace entre el sector privado y el sector público, que es interesante, sobre todo para el contenido de esta ponencia en ciberseguridad, que precisamente intenta en todo momento encajar las actuaciones público-privadas y enlazarlas con el calado, con la perspectiva o con la pedagogía social que deben tener los nuevos retos y las nuevas herramientas con las que se enfrentan los retos.

cve: DSCG-12-CM-90

Hay dos partes especiales de su trabajo, y aprovecho para preguntarle, porque en su comparecencia no se ha detenido en ellas. La primera es sobre las actuaciones, la cooperación público-privada, los espacios en los que el Gobierno puede colaborar para mejorar en lo que se refiere a riesgos tecnológicos y a la seguridad en las compañías del sector financiero, de telecomunicaciones, de energía, de *utilities,* y también en la función que el sector público, el Gobierno en este caso, tendría en la implantación de servicios esenciales y de seguridad para ciudadanos, así como la percepción que los ciudadanos y ciudadanas tienen de estos nuevos retos.

Otro espacio que me parece interesante es el de la inteligencia económica aplicada al mundo empresarial. ¿Cómo debe garantizarlo el Gobierno? ¿Cómo se puede integrar ese espacio público-privado para garantizar los servicios esenciales y la seguridad? La implantación de la percepción de seguridad por parte de la ciudadanía, ¿qué aporta en concreto a la inteligencia económica, al mundo empresarial? ¿Por qué es necesaria en este momento? ¿Cuál es el grado de desarrollo en el ámbito de las empresas españolas en cuanto a inteligencia económica? ¿Qué herramientas se pueden aportar a este espacio de trabajo para mejorarlo? y ¿qué puede suponer —me refiero, en concreto, a periodos de inestabilidad, de inestabilidad económica y desestabilidad política—, qué campo puede jugar la inteligencia económica en la prevención en ciberseguridad?

Por otra parte —y termino con estas dos preguntas—, si no me equivoco, el ponente, el señor Picatoste, es favorable a que la práctica de la inteligencia económica integre todas las capacidades de obtención, tratamiento y análisis que proporciona el *big data,* y que además es preciso hacerlo con todas las facilidades que ponen a su disposición las tecnologías de la información, pero ¿qué riesgos puede suponer la aplicación del *big data* entre quienes solamente gestionan parte de esos espacios, quienes solamente gestionan datos e información y quienes utilizan este activo para luego convertirlo en conocimiento y en inteligencia? Lo pregunto especialmente porque no solo los retos son nuevos, sino que además están en constante movimiento. Las amenazas de seguridad, sean físicas o cibernéticas, tienen un cierto grado de improvisación en las actuaciones —que no deberían tener— cuando nos enfrentamos a situaciones nuevas. Nos gustaría conocer su opinión sobre estos riesgos. Por otra parte, en los espacios donde se integran todas esas capacidades del *big data,* ¿cuál es la fiabilidad y la calidad de los datos tras el primer filtrado y la primera eliminación de datos brutos?

Y por último, centrándome en la parte de su intervención más educativa dentro del postgrado de inteligencia económica, le diré que hemos tratado temas de formación en esta Comisión de Seguridad Nacional, así como también en la ponencia de ciberseguridad. Hay un espacio en el postgrado, en concreto, respecto a la inteligencia. Pero, ¿cuál es su opinión sobre la formación reglada en espacios anteriores? Me refiero a formación profesional, a grados universitarios. ¿Cuál es su opinión sobre la formación en ciberseguridad en esos espacios?

Muchas gracias.

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

El señor Hernando tiene la palabra.

El señor **HERNANDO VERA:** Gracias, señor presidente.

Gracias, señor Picatoste, por comparecer en esta comisión e ilustrarnos con el trabajo que realiza la compañía a la que representa, y usted personalmente.

Como sabe, el objetivo de esta comisión, de este grupo de trabajo, es hacer un informe que pueda ser útil para mejorar la ciberseguridad en España en su conjunto: en la Administración pública, en todas las administraciones, en el sector privado y en la colaboración entre el sector público y el privado. Por lo tanto, con ese objetivo, yo le formularé una serie de preguntas, básicamente sobre algunos aspectos que usted ha mencionado, pero también sobre otros que no ha mencionado pero que quizá pueda hacerlo en su segunda intervención, lo que nos vendrá bien a efectos del informe que finalmente elaboraremos.

En primer lugar, ¿cree usted que el arsenal legal con el que España se enfrenta en estos momentos a la ciberseguridad es suficiente? ¿Es suficiente la transposición que vamos a hacer de la Directiva NIS? ¿Es suficiente la nueva Ley de protección de datos? ¿Es suficiente la Ley de seguridad privada? ¿Lo son los agentes de seguridad, los agentes de protección de datos? ¿Todo esto es suficiente? ¿Cree usted que el arsenal —permítaseme esta expresión— tiene que reforzarse? ¿Esto tendría que hacerse a nivel no solo nacional, sino también europeo e incluso internacional, por la no territorialidad de la amenaza en el ciberespacio? Esta es la primera cuestión, si tenemos que modificar, mejorar y potenciar nuestra legislación.

cve: DSCG-12-CM-90

En segundo lugar, ¿cree usted que en España hay seguridad en el ciberespacio o lo que hay es más sensación de seguridad en el ciberespacio? Lo voy a trasladar a otro campo, al de la seguridad ciudadana. Yo creo, sinceramente, que España es un país con mucha seguridad ciudadana, y además desde hace muchos años, no en los últimos cuatro u ocho años. Sin embargo, muchas veces —y aquí hay algún experto en la materia— la ciudadanía tiene sensación de inseguridad, aunque, objetivamente, los niveles de criminalidad son bajos y la seguridad es alta. Me da la impresión de que en el ciberespacio es al revés: hay más sensación de seguridad de la que hay en realidad, y me gustaría que nos diera su opinión. Yo he visto en la página de Deloitte que ustedes prestan servicios al sector financiero, al de telecomunicaciones, al de energía y al sector público, y, por consiguiente, supongo que tienen datos y experiencia suficiente para ilustrarnos sobradamente sobre este tema.

En tercer lugar, ¿hay un mejor modelo de integración de las capacidades públicas y privadas que el que estamos poniendo en práctica en España? Es decir, queríamos saber si hay un modelo ideal. Si usted tuviese que hacer una recomendación a esta comisión o al Gobierno de España, díganos qué diría: Ustedes se tienen que parecer a o ustedes tienen que tender al modelo de integración de ciberseguridad público-privado que sigue el Estado que usted considere. Díganos algunas recomendaciones que tienen que ver con la actualidad más internacional, en absoluto nacional.

Objetivos de la ciberseguridad son las compañías, las administraciones, pero también son los ciudadanos, las particulares, cada persona que utiliza un dispositivo. En este sentido, el bien a proteger es el dato, es la privacidad. Hemos tenido un ejemplo muy cercano en el tiempo respecto a una enorme compañía, que tiene 2200 millones de usuarios, donde se ha descubierto un incidente en el que un número importante de sus datos han sido mal utilizados por otra compañía. ¿Usted cree que es posible garantizar la privacidad de los datos, cuando se integran en compañías con enormes plataformas, con los actuales sistemas de coordinación que hay? ¿Es posible que Facebook nos garantice esa privacidad de los datos? Les recuerdo, señorías y señor compareciente, que después de la comparecencia del señor Zuckerberg en el Senado de Estados Unidos, las acciones de Facebook subieron de cotización, entre otras cosas porque garantizó que iba a hacer un poco más de lo que está haciendo, pero tampoco demasiado más. Me gustaría que nos diese su opinión sobre esto, porque el tema de la privacidad y de los datos me parece que es fundamental.

Es evidente que la ciberseguridad afecta a las compañías, al sector privado, a las grandes compañías de telecomunicaciones, incluso a las de energía. Pues bien, ¿usted cree que puede afectar —no quiero polemizar sobre este tema— a los procesos electorales, como se ha puesto de manifiesto en algunas comparecencias y en algunos países en los que están tratándose estos temas? Si el dato es el bien a proteger, ¿considera usted que el *blockchain,* aplicado a todos los sectores económicos, sería una tecnología adecuada para proteger ese dato? ¿Cuál es su experiencia en este terreno?

En relación con el presupuesto, como usted ha dicho —veo que ha leído comparecencias anteriores, y algunos asistimos a ellas—, el problema es la gigantesca brecha que existe con otros países. Un representante de otra consultoría, que estuvo aquí en la sesión anterior, nos habló de que Reino Unido dedica 2300 millones, Francia 1000 millones y aquí, entre el Incibe y el CNI, no llegamos a 200 millones. Por tanto, la brecha es gigantesca. Nos damos cuenta, cuando ustedes comparecen aquí, de que tenemos empresas que son punteras, con muy buenos profesionales y buena formación, pero el *décalage* presupuestario es tan enorme que es muy difícil que podamos llegar donde están otros países. Por lo tanto, me gustaría que nos ilustrase un poco más sobre este tema.

Muchas gracias.

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

Finaliza este primer turno el señor Cosidó.

El señor **COSIDÓ GUTIÉRREZ:** Muchas gracias, señor presidente.

Permítame empezar agradeciéndole al presidente y a la Mesa de esta comisión mixta que nos reunamos por primera vez aquí, en esta Cámara Alta, en el Senado, a lo que damos una muy cordial bienvenida, aunque sea en horarios poco acostumbrados en esta Cámara.

Querría agradecer muy especialmente al ponente la claridad de ideas que nos ha expuesto y la cantidad de sugerencias que nos ha formulado en su intervención. De hecho, es un poco complicado porque, entre lo clara que ha sido la exposición y la cantidad de preguntas que ya le han hecho otros grupos parlamentarios, tampoco quedan muchas más preguntas que hacer, aunque alguna más añadiremos a la lista que se ha hecho.

cve: DSCG-12-CM-90

Quería agradecerle su exposición, pero también querría agradecerle dos cosas. En primer lugar, este es un tema de presupuestos, sin duda —se ha puesto de relieve por parte de algún grupo de la oposición—, pero, en mi opinión, también es una cuestión de ciberpatriotismo. ¿Cómo se explica que un país que dedica menos recursos que otros tenga unos niveles de ciberseguridad muy alta? Pues porque hay un compromiso y una cooperación entre el sector público y el privado que nos permite ser muy eficientes en términos de la inversión que, en realidad, realizamos. Y su presencia aquí, como la de tantos otros representantes de empresas o de sociedad civil, es un buen ejemplo de la disposición para afrontar, como reto de nación, como reto de país, algo tan complejo como es la ciberseguridad.

Y en segundo lugar, yo creo que ustedes, o el equipo que dirige o la parte española de la empresa de la que forma parte, son también un buen ejemplo de liderazgo. Nos ha hablado de 250 000 empleados en todo el mundo —imagino que en España habrá solo una pequeña parte— y, sin embargo, en el ámbito de la ciberseguridad dentro de una gran multinacional, la número 1 del mundo en prestación de servicios, España tiene un liderazgo importante en toda la región de Europa, Oriente Medio y África, según he deducido de su exposición. Por tanto, es un buen ejemplo de ese liderazgo español en materia de ciberseguridad.

La primera pregunta es sobre cómo podemos reforzar ese liderazgo, si me permite la expresión. Nos ha mostrado el caso de Israel, que es muy complejo en Europa, ¿pero cómo podemos ser nosotros un caso de éxito en la Unión Europea?, ¿cómo podemos ser, siendo un país de una dimensión menor que otras economías, un país claramente de referencia en el ámbito de la ciberseguridad? Y ha hecho bastantes propuestas de cosas que hay que hacer. A mí me gustaría hacer especial énfasis en cómo podemos generar ese nivel de *startups* que, en mi opinión, es una de las claves que explican el éxito de Israel en este campo. Si no me equivoco, creo que Israel, que es una economía de la dimensión de la portuguesa, tiene más *startups* tecnológicas que el conjunto de la Unión Europea. Y ponía énfasis en que hay un gran apoyo, una gran implicación pública. Yo creo que esto no es solo una cuestión de grandes empresas. Creo que las pequeñas y medianas empresas tienen mucho que hacer y, por tanto, quisiera saber cómo podemos potenciar todo ese tejido de pequeñas y medianas empresas en innovación y en tecnología para ser realmente un país con liderazgo en el ámbito de la ciberseguridad.

Sobre el marco normativo le ha preguntado el portavoz socialista más en un ámbito nacional. Prácticamente en todas las ponencias se nos dice que no es suficiente, que necesitamos claramente un marco normativo mínimo europeo. Se han dado pasos muy importantes en los últimos años, pero yo diría también que debe ser a nivel global. Es decir, o somos capaces de construir un cierto marco o una realidad que es tan global como es el mundo virtual o de internet, o será muy difícil que podamos dar respuesta incluso a escala europea. Por tanto, yo le pediría que, además de la referencia a nivel nacional que pueda hacer, que haga también, si puede, alguna referencia a nivel de ese ámbito internacional europeo. ¿Qué carencias, qué propuestas podría impulsar España en distintos foros multilaterales para dar una regulación a esta cuestión?

Por otro lado, le pido que se moje un poco más, si puede, en términos de valoración de nuestro nivel de ciberseguridad. Se ha dicho que en el *ranking* de ciberseguridad ocupamos el puesto 19, pero me gustaría que nos dijera en qué sectores cree que tenemos que hacer un mayor esfuerzo para mejorar nuestro nivel de ciberseguridad. Ha mencionado algún sector financiero en el que España tiene muy buen estándar de ciberseguridad. La verdad es que, más o menos, tenemos identificados, a través de los planes de infraestructuras críticas, aquellos más sensibles, más vulnerables, pero también me gustaría saber, si nos puede adelantar algo, en cuáles estamos mejor preparados —siendo el financiero muy sensible—, ya que otros sectores a lo mejor no son tan críticos pero tenemos carencias más importantes.

Algún otro portavoz ha mencionado que la Administración pública debería ser modelo y ejemplo para el sector privado en términos de estándares de seguridad. Tengo una impresión que no sé si compartirá. En lo que es Administración central, y especialmente en aquellas partes más críticas, como el Ministerio de Defensa —posteriormente intervendrá un ponente del Ministerio de Defensa que lo va a explicar mucho mejor—, o el Ministerio del Interior, tenemos estándares de seguridad bastante altos. A mí me preocupa más el ámbito municipal y, en menor medida, el autonómico, donde lo que tenemos es una cierta heterogeneidad; es decir, hay algunas administraciones que están haciendo más esfuerzo y, en cambio, otras se esfuerzan menos. En la medida en que las administraciones cada vez gestionan datos más sensibles desde el punto de vista de la privacidad de los ciudadanos, creo que sería bueno que nos indicara también cómo valora y cómo evalúa —ahí no le pido que se moje, es decir, no hace falta que diga quiénes lo hacen mejor que otros— y, en términos generales, dónde estamos y a dónde tenemos que ir. A ver si es posible que nos adelante algo al respecto.

cve: DSCG-12-CM-90

Hablamos mucho también de las amenazas y, más o menos, las tenemos identificadas para el futuro. Usted ha cambiado un poco el enfoque, y me ha parecido acertado hablar también de los costes y los efectos que tienen estas amenazas, pero me gustaría saber —no utilizaré la palabra enemigo, de lo que hemos hablado en alguna otra comparecencia—, haciendo un poco de prospectiva, de dónde van a venir las amenazas futuras. Es decir, si tenemos que estar más preocupados por la cibercriminalidad, es decir, si la mayoría de las agresiones, de los ataques o de los delitos que se cometen están relacionadas con formas de criminalidad organizada, o si tenemos que estar más preocupados por otros agentes estatales, pues hemos visto recientemente que se han mostrado muy activos también en cuanto a ataques, incluso intentando desestabilizar o interferir en procesos democráticos de algunos países —me temo que me va a decir usted que tenemos que estar preocupados por todo, pero es por si, de alguna manera, lo podemos priorizar—, o por *hackers* que lo que hacen es atacar sistemas por el puro —parece— placer o divertimento en vulnerar o penetrar determinados sistemas. También podemos hablar de organizaciones terroristas. La amenaza es muy poliédrica, pero si miramos hacia el futuro, haciendo un poco de prospectiva, de toda esa panoplia de amenazas que tenemos, ¿cuál le parece que puedan ser las más inquietantes?

Para terminar, le han preguntado también por la colaboración público-privada. Además de unirme a la cuestión, ¿qué podemos hacer para mejorar esa colaboración público-privada que usted ha señalado y yo coincido en que es excelente en España? En el mundo real, en los conceptos tradicionales, teníamos bien delimitadas las esferas de seguridad privada y de seguridad pública. Hay una zona de colaboración entre seguridad privada y seguridad pública, pero estaba bien regulada, bien delimitada. La supremacía de la seguridad pública sobre la seguridad privada era indiscutible. En el ámbito de la ciberseguridad esto es más complicado. ¿Tenemos que reformular conceptos que tradicionalmente hemos manejado con mucha precisión en un ámbito de ciberseguridad pública, ciberseguridad privada? ¿Qué tipo de responsabilidades o de tareas son indelegables por parte de los poderes públicos respecto de las compañías privadas o de la sociedad?

Por último, es casi inevitable, y se han referido a ello, que exista una gran preocupación ciudadana por el uso de los datos y la seguridad de los datos personales que tienen grandes compañías que manejan cantidades ingentes de información. Cualquier ciudadano, todos nosotros, cada vez nos bajamos más aplicaciones en nuestros móviles, en nuestras *tablets,* y aunque supuestamente todos firmamos o aceptamos unas determinadas condiciones, yo creo que muchos no somos conscientes, en eso me incluyo, de la accesibilidad que estamos dando en muchas de estas aplicaciones a datos que son críticos y que afectan a nuestra intimidad más personal, incluyendo el uso de la cámara, la geolocalización. En fin, es increíble.

Se ha señalado educación, concienciación, pero ¿hay algo más? Es decir, ¿los poderes públicos tenemos la obligación de establecer unos límites, unas normas al grado de penetración que le damos a estas empresas en nuestros datos privados? O si eso es una decisión, en su opinión, que corresponde a cada uno y, por lo tanto, si uno firma sin saber lo que está firmando, será problema del que lo firme. Pero, en mi opinión, hay un problema social, porque no hay conciencia del grado de vulnerabilidad que estamos otorgando a través de esas aplicaciones.

Muchas gracias, presidente.

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

El señor Picatoste tiene ahora la oportunidad de contestar a las preguntas y satisfacer las inquietudes de las señoras y señores parlamentarios.

El señor **PICATOSTE MATEU** (socio Risk Advisory, Deloitte): Como cabía esperar, todas las preguntas son interesantísimas y supongo que dispongo de un tiempo limitado. Voy a ser muy rápido y muy conciso en muchas de ellas, porque creo que hay un segundo turno. Voy a tratar de ir de una forma bastante ordenada.

El señor Yanguas me preguntaba que a qué me refería con el entrenamiento. Hacemos simulacros de evacuación de incendios, ¿verdad? Cuando sonaba una sirena la primera vez, cogíamos todas nuestras pertenencias, porque no nos creíamos que eso fuese un simulacro, y salíamos como una chispa por si acaso eso se iba a quemar de verdad. Cuando lo hemos entrenado, ya nos hemos acostumbrado a irnos al punto de reunión, dejar todas nuestras pertenencias, de una forma eficiente, nos recuentan y volvemos. El procedimiento es mucho mejor, mucho más sano, mucho más organizado y, además, mucho más seguro para la protección de las vidas. Va de esto, va de ponernos en situación de que suceda una crisis, ver a quién convocaríamos a un comité para resolver una crisis, que es la primera pregunta. En un comité

cve: DSCG-12-CM-90

para resolver una crisis no tiene que estar todo el mundo, tiene que estar alguien que aporta para resolver la crisis y nadie más. Todo lo demás, en una crisis, serán opiniones posteriores, pero hay que tomar decisiones rápidas en un momento de gran volatilidad de información. Esta disciplina hay que entenderla. Hay muy buenos ejemplos porque se están haciendo múltiples ciberejercicios en el Estado español, desde ejercicios conjuntos en el ámbito de la defensa, como en las administraciones públicas y algunos organismos que lo están haciendo de forma rutinaria, y con esto créanme que se eleva mucho el nivel de concienciación de cómo actuar en una situación de crisis. Ese entrenamiento también nos ayuda a detectar dónde me falta tono. O sea, cuando hago un ejercicio excesivo y me salen agujetas, en la próxima me tiene que coger mejor entrenado por esas agujetas.

El señor Gutiérrez planteaba varias preguntas respecto a la Administración. Les traigo también buenas noticias, porque parece que en esto de la ciberseguridad todo son malas noticias, pero también las hay buenas. Hay algunas administraciones públicas o sociedades estatales con certificaciones porque al prestar servicios han considerado interesante tener certificaciones más típicas del mundo privado, pero las tienen. Pero en el ámbito de actuación de la Administración pública el esquema nacional de seguridad es la normativa básica. El grado de avance es muy significativo, nuevamente, como se ha mencionado aquí, a pesar de las épocas en las que hemos tenido más restricciones presupuestarias. El Centro Criptológico Nacional emitió en su día guías para el cumplimiento del esquema nacional, las guías Stic 800, una serie completa, que hacen un seguimiento de la implantación de la mejora en la Administración General del Estado, en las comunidades autónomas, en la Administración Local y en las universidades.

Hay información de esta que no está clasificada y la pueden consultar ustedes, pero hay avance y, además, proporcional al *gap,* porque lo que han hecho ha sido tipificar cuáles son las aplicaciones más críticas y se han ido poniendo bastantes medidas. Aquí, créanme, es muy espectacular ver un acto del Centro Criptológico Nacional —alguno ha sido en los cines Kinépolis— donde se han juntado más de mil personas de las administraciones y de la empresa privada para hablar de ciberseguridad, compartir buenas prácticas y enseñar cómo mejorar. Además, poniendo al servicio de la ciudadanía herramientas gratuitas para mejorar ese tipo de situaciones. Por lo tanto, hay parte de buenas noticias, aunque con más presupuesto las cosas se podrían hacer seguramente de una forma más ágil y mejor.

La pregunta que me hacía respecto a las operadoras es un dilema que se viene repitiendo toda la vida, es decir, ¿es responsable el que pone la autopista de cuidar los semáforos o proteger que nadie se pase los límites de velocidad? En internet lo malo es que no nos dan un carné de conducir. Para conducir a la gente se le explican unos principios básicos, pasa unos test de actitud y, a partir de ahí, sí que conduce y, además, tiene una edad de entrada. Resulta que nosotros no tenemos ni test de actitud ni edad de entrada y, además, queremos circular a toda velocidad. Claro, la combinatoria hace que eso sea muy complicado. ¿De quién es la responsabilidad de poner esos controles? Pues, lógicamente, desde de los padres respecto a cómo educamos a nuestros hijos sobre lo que tienen que hacer y lo que no en internet, hasta los propios usuarios, y hay más preguntas al respecto que trataré de desarrollar.

También es cierto que en determinados puntos centrales de los nodos de acceso a internet se pueden poner controles y garantías adicionales, pero liga con otras cosas y en cómo se yo que no estoy limitando la libertad del usuario en el acceso a internet. No crean ustedes que es un tema fácil de resolver. Lo que sí me consta es que las operadoras que trabajan en el mercado nacional le dedican mucho tiempo, especialmente enfatizando lo que tiene que hacer el usuario para acceder de una forma segura a sus servicios, que es lo que no hacemos ninguno. Es decir, cualquiera de las operadoras nos instala el *router* en casa y ya tenemos acceso a internet, pero lo de cambiar la *password* que viene por defecto es demasiado complicado y para qué se la voy a cambiar si ya tengo tantas *passwords* que es difícil recordarlas.

En 30 segundos un niño es capaz de romper la seguridad de las wifis domésticas. ¿Por qué? Porque los códigos pseudoaleatorios con que se dan de alta esas contraseñas han sido publicados. Hay una serie de buenas medidas, que además nos indican, que no seguimos, y ahí es donde empieza el problema. Como saben ustedes, se han producido multitud de anécdotas de gente que ha accedido a la casa del vecino y desde esa casa ha realizado actividades delictivas. ¿La culpa de que no se pusieran las medidas de seguridad es de uno mismo o es culpa del operador? Realmente es muy complejo, pero creo que todavía tenemos campo para aprender y, créanme, si estamos en el ciberespacio tenemos que aprender todos de ciberseguridad, y todos es todos, mis hijos, ustedes, yo… Por tanto, cualquier esfuerzo que hagamos por concienciar y por explicar mejor cómo tener una serie de medidas y usos sanos del acceso a las redes será lo mejor que podamos hacer.

cve: DSCG-12-CM-90

En cuanto a la señora Angustia, que empezó con la parte de la colaboración público-privada, que se ha repetido ya más veces, tengo una buena noticia que el señor Cosidó ya ha compartido con ustedes, y es que en España estamos haciendo muchísimas cosas compartidas entre lo público y lo privado. Créanme que el nivel de interacción entre todos es sorprendentemente alto.

Es cierto que nos conocemos casi todos en ese mundo y que hay determinadas situaciones donde no somos competidores, somos colaboradores necesarios para aumentar el nivel de resiliencia de los ciudadanos, de las empresas y del país. No escatimamos en colaborar en ponencias. El general Medina, del mando de ciberdefensa, ha estado en ponencias de Deloitte, igual que el Centro Criptológico Nacional, el Incibe y el Ministerio del Interior. Todos estamos muy alineados. Como ejemplo, se ha mencionado también la protección de las infraestructuras críticas. La normativa estaba y es una buena norma, pero siempre está el dilema entre la intención del regulador y la visión del supervisor. A veces no coinciden, pero este no es el caso. ¿Por qué digo que es una buena norma? Porque ha ayudado a mejorar la resiliencia de las infraestructuras críticas nacionales. ¿Quién paga la fiesta? El 85 % de las infraestructuras críticas está operado por el sector privado, y este sector privado claro que quiere cumplir con todas estas normas, pero lleva su tiempo y su coste asociado. Nuevamente estamos colaborando, y en el caso de la Ley de protección de infraestructuras críticas y en la elaboración de los planes estratégicos, así como para acometer la forma más eficiente de proteger estas infraestructuras, tanto el sector público como el privado han colaborado de forma estrechísima.

En cuanto a la inteligencia económica, sin duda. La inteligencia se hace para tener una posición más avanzada que otro. ¿A qué nos referimos? Si yo quiere vender mejor un producto, tendré que saber qué hace la competencia, cuáles son mis ventajas respecto a ellos, dónde están ellos, dónde no estoy y poner en valor mi producto. Esto es inteligencia económica, es decir, con las capacidades españolas, dónde queremos estar, la gran empresa española dónde quiere estar y dónde no debe estar. Aquí se han cometido errores en el pasado yendo a países sin ninguna seguridad básica. Por mucho que nos queramos internacionalizar, hay que ir a determinados sitios con determinadas precauciones.

Nuevamente hay un nivel altísimo de colaboración público-privada. Tanto el ICEX como la Guardia Civil, con los programas internacionales, ayudan a las empresas españolas en cosas tan básicas como guías de dónde debe estar la gente y dónde no, y el Ministerio de Asuntos Exteriores también ha acompañado en todas estas tareas. No nos vamos solos, hay que tratar de buscar la fuente de información adecuada. En el propio Ministerio de Defensa, el Ceseden publica información accesible de riesgo país accesible preguntando en las fuentes adecuadas si es disponible para una gran empresa que se quiera internacionalizar. Por tanto, la inteligencia económica, sí, hay que potenciarla. Hay otros países que lo potencian más que España. Por ejemplo, Francia y Estados Unidos defienden los intereses de las empresas francesas y estadounidenses fuera de sus fronteras. ¿Cómo? Con múltiples medidas. Hay información disponible en todo el mundo.

En cuanto al uso del *big data*, yo creo más en el *small data*. ¿Para qué voy a replicar con montones de datos una información que está más accesible en una estadística bien procesada y con una fuente fiable? La cuestión es preguntarnos si la fuente es fiable, si la estadística ha sido elaborada con el método adecuado, o si se ha adulterado la fuente o el método de procesamiento. Muchas veces no accedemos a información procesada de altísimo valor y disponible, lo que nos ahorraría hacer montones de búsquedas y recolecciones de información que, al final, nos cuesta ver por dónde vamos. No obstante, el *big data* es la tendencia y las capacidades que ofrece son muy altas. Hay un debate, por ejemplo, en sanidad en cuanto a lo que puede ayudar el *big data* a mejorar enfermedades, especialmente en algunos casos. ¿Qué hay más sensible que la información de sanidad de un paciente? Y les pongo un ejemplo casi de película. Gente que es inquebrantable podría hacer algo insospechado por la salud de su hijo; es decir, si su hijo tiene tal cosa, eso es una vía para poder hacerle extorsión. Todos estos datos que manejamos, al final, tienen una importancia mucho mayor —y voy a decir aquí la palabra— de la que le damos.

Le damos poca importancia a nuestra información. Parece que todo lo que tengo es público. Resulta que si me estuviesen viendo por una cámara en cualquier momento del día, no pasaría nada. ¡Si soy yo el que está diciendo que quiero que todo eso sea público! ¿Cómo? Dándole al clic de la muerte, al de instala, al de dar acceso a la cámara, a mi agenda o al de poder hacer llamadas. Nos lo informan, pero, como queremos tener el servicio que está detrás, no nos paramos. Ligo con algo que luego desarrollaré y es que alguno de esos casos puede llegar a ser abusivo. A lo mejor hay que reflexionar sobre qué se puede hacer, porque es muy difícil que todos los ciudadanos tengan el mismo nivel de concienciación sobre el peligro que asumen y la proporcionalidad entre lo que se pide y lo que se da.

cve: DSCG-12-CM-90

Pasamos al señor Hernando. Le dedicaré un ratito. En cuanto al arsenal legal, las normas han ayudado a impulsar la seguridad. En el caso español, con la Ley de protección de datos hubo un reglamento de medidas de seguridad que ayudó a aumentar las medidas de seguridad de las empresas, especialmente para tener cosas tan básicas como copias de seguridad. A los que se nos ha roto un disco duro o a los que un ordenador no ha vuelto a encenderse sabemos lo que significa ese respaldo que tenemos cuando todo falla. Hay más preguntas al respecto, pero la partida es la internacional, es decir, hay un vacío legal que es el que aprovecha el malo, el cibercriminal, el que quiere hacer un uso ilícito de las cosas. El mecanismo para perseguir todos esos temas es hacer una denuncia y, si quieres traspasar una frontera, una comisión rogatoria. Entonces, ¿cuándo voy a tener yo una respuesta a todo esto? Por tanto, sí creo que hay ámbito de trabajo, especialmente respecto al cibercrimen, en los organismos policiales internacionales, Interpol y Europol, que al menos digan ellos, que son los especialistas, qué más necesitan para poder perseguir adecuadamente esta materia. He puesto este ejemplo porque hay muchos especialistas en todas estas materias. Siempre hay que buscar y beber de la mejor fuente contra la mejor amenaza, y luego lo desarrollaré un poco más.

En cuanto a la seguridad objetiva respecto a la subjetiva, aquí tengo mejores noticias. Hace años salimos como el tercer país más atacado del mundo. No somos el tercer país más atacado, somos el tercer país que sabe que le están atacando gracias al Centro Criptológico Nacional, porque ha puesto medidas para la medición de tráficos agresivos y se están midiendo. Esto es nuevamente una buena noticia, porque muchos a nuestro alrededor, o no lo miden, o no lo saben y, por tanto, no son conscientes del nivel de mejora que les hace falta. En este caso, el nivel de seguridad real es bastante alto respecto a lo que ustedes puedan pensar, y luego lo seguiré perfilando. Para cada tipo de amenaza tenemos un especialista y las funciones que tienen están muy claras y han sido desarrolladas por la Dirección de Seguridad Nacional, el Centro Criptológico dentro del CNI, el Ministerio del Interior —Policía, Guardia Civil y Centro Nacional de Protección de las Infraestructuras Críticas— o el Ministerio de Defensa. Todos estos especialistas ponen el foco en su amenaza y están haciendo muchas cosas con ese poco dinero que han dicho. Es decir, el nivel de inversión de un gran banco en ciberseguridad es superior al de este país. Si me preguntan, solo un banco ya se gasta mucho más dinero en esto.

El nivel de seguridad es mayor de lo que parece. Hay que ir siempre a la fuente más acreditada. Ustedes aquí han entrevistado a mucha de esta gente. Quizá tengan que profundizar en los ámbitos específicos con cada uno de ellos. A mí me gusta ver siempre el vaso medio lleno, no medio vacío; es decir, siempre va a haber camino y, como se ha mencionado, la amenaza es cambiante. Lo que no podemos hacer tampoco es gastar recursos infinitos, porque llegaría un bloqueo por la cantidad de cosas que hay que hacer. Hay que priorizar muy bien las acciones. Realmente, los esquemas que funcionan son los de priorización de riesgos, una estrategia básica que consiste en ver qué es lo más importante que tengo que proteger, cuál es la mayor amenaza, y mitigarla de la forma más eficaz.

En cuanto al modelo de integración de capacidades públicas y privadas, les he contado el caso de Israel, que es real. Los condicionantes de partida son diferentes. Quizás los mejores ejemplos son Estados Unidos e Israel, que son los que mayor industria tienen de todo esto. En cuanto a países más cercanos podrían ser Francia y Alemania. Nadie puede solo en todo esto. Tenemos que buscar los mecanismos para apoyarnos entre todos para hacer un uso eficiente de los recursos. Nuevamente vuelvo a decir que esto no puede ser un tema de recursos infinitos, sino bien priorizados y bien ajustados. Hay que trabajar en un modelo sostenible a futuro. Lo que construyan ustedes tiene que servir para mucho tiempo. Siempre se pone el ejemplo de la privacidad de un *email.* Creo que han tenido ustedes a Elvira Tejada en la sala. La privacidad de un *email* se asimila a una carta, que es una normativa de 1800. Les animo a que lo que hagan lo hagan con vistas a perdurar, porque la amenaza va a cambiar y los mecanismos serán diferentes, pero la esencia probablemente sea la misma.

En cuanto a Facebook, no nos leemos las condiciones. Le transferimos la propiedad de nuestros datos a Facebook. Las fotos ya no son vuestras, son de Facebook. Al principio hubo una polémica muy gorda, porque si yo soy su amigo y usted es amigo de un tercero, teóricamente yo soy amigo del tercero, y esto no se podía limitar. Al principio, en Facebook podías ver en seis saltos la información de cualquier famoso o cualquiera que te planteases; ahora se puede limitar, pero hay usuarios que todavía no saben cómo hacerlo. Hay que entrar en las opciones de privacidad y decir que no quieres compartir con gente que no conozcas, y ya está.

Dicho esto, Facebook avisa de que hace uso de esos datos, porque su modelo de negocio consiste en utilizar esos datos y rentabilizarlos de otro modo, igual que Google. Cuando ustedes aún no han abierto

cve: DSCG-12-CM-90

un correo electrónico y el navegador les anuncia un gimnasio, se empiezan a mirar en el espejo y piensan: ¡Me he descuidado mucho! Pero es que basta con que un amigo te haya mandado un *email* con un contenido parecido para que tengas un contenido relativo a eso. Y lo has aceptado, porque querías tener servicios de localización, servicios contextuales de mayor valor añadido para tu bienestar y uso, pero hay que saber lo que estamos aceptando. Lógicamente, siempre hay un punto donde se llega al abuso, donde ya cedes, vendes sin haber requerido nada.

Estamos avanzando muchísimo con la General Data Protection Regulation, la GDPR, la nueva normativa europea de regulación de datos. Ya teníamos una normativa muy buena, la Ley de Protección de Datos española, muy avanzada respecto a los otros países en la parte de las medidas de protección, en el reglamento de medidas de seguridad, y ahora está más en el flujo de información, en la captación de los consentimientos. Este es el punto importante de esta normativa, que los ciudadanos sean conscientes de que pueden ejercer el uso de sus consentimientos y decir qué sí y qué no. En este caso sí puede haber compañías que no dan la posibilidad de hacer el consentimiento explícito. En ese caso, lógicamente, habrá un marco normativo funcionando desde el 25 de mayo de 2018.

En cuanto al *blockchain*, creo que fue Jesús Romero en su intervención el que les explicó la tecnología de una forma fácil y rápida. Efectivamente, es una base de datos distribuida, donde el mecanismo de confianza no reside en una entidad central, sino en la confianza que otorgan los miembros a ese mecanismo. Es un mecanismo de desintermediación. Hay bastantes expectativas sobre la tecnología, y hay que ver cómo se plasman. Desde luego, tiene mecanismos de cifrado de la información robustos. Se habla, por ejemplo, en la terminología inglesa, del KYC, el *know your customer*. Por qué le voy decir a todo el mundo quién soy, si dejo en un *blockchain* la información para que todo el mundo vea quién soy. Además, soy fiable porque esa información ya ha pasado por *n* personas que han dicho que lo soy. A lo mejor tendría sentido un *blockchain* nacional, en vez de tener un DNI nacional, tener tu información accesible. La tenemos en el DNI, el DNI 3.0 nos da acceso a qué queremos publicar de la información que está guardada en nuestros bolsillos, pero nuevamente hay oportunidades diferentes para hacer cosas de otra forma.

Aquí la normativa, pese a lo que se dice siempre de la ciberseguridad, que parece un *stopper,* que es poner controles al campo, está favoreciendo nuevos modelos de negocio más ágiles y más útiles para los ciudadanos. La tendencia es el eIDAS, la normativa de identificación electrónica, también hay una directiva al respecto, de armonización de los mecanismos de firma electrónica, certificaciones, etcétera. En este caso, la palabra armonización la decimos muy rápido, pero es la clave. El problema es que cuando tenemos una directiva europea, debemos hacer que encaje bien en las normas españolas y es un lío, porque luego empiezas a ver todas las vertientes, todas las interpretaciones y lo que queda puede ser algo totalmente diferente.

También hay que pensar en Europa —y lo ligo con lo que hablábamos sobre el liderazgo—: las oportunidades se juegan en una liga y tenemos que sacar una norma buena para todos los europeos y para los españoles, no doscientas normas que, al final, hacen un conglomerado que para el sujeto paciente es muy difícil saber cómo cumplir e incrementan el coste del cumplimiento, cuando lo que se persigue es, por definición, que las empresas cumplan.

No sé cómo voy de tiempo.

El señor **PRESIDENTE:** Tiene cinco minutos.

El señor **PICATOSTE MATEU** (socio Risk Advisory, Deloitte): Gracias.

En cuanto a la brecha con el presupuesto del Reino Unido, intencionadamente no he repetido las cifras porque ya las tienen ustedes. Es claro y patente que estamos muy lejos. Podríamos avanzar y desarrollar nuestras capacidades, pero sigue habiendo ciertos intereses y dar cuartos al pregonero puede no interesarnos. Si hay que priorizar, empezaría por los temas que sean más sensibles para el Estado español.

Respecto al señor Cosidó, en primer lugar, quiero darle las gracias por su punto de vista. Hay muchos ciberpatriotas. Cuando estamos en los eventos de ciberseguridad, es un orgullo ver el nivel de compartición de todos por el bien común. Es complejo, pero colaboramos entre nosotros de forma absolutamente desinteresada con el fin de mejorar la situación.

Me preguntaba por reforzar el liderazgo, y el caso claro son las *startups*. El Incibe ha llevado a cabo un proceso de aceleración hace poco. Creo que partió con cincuenta y seis s*tartups* de ciberseguridad españolas, las diez últimas de las cuales llevó a un concurso para ayudarles a conseguir rondas de

cve: DSCG-12-CM-90

financiación, que se nutren de *venture capitalist,* del mercado normal de financiación. Es bueno descubrir dos cosas: una, el gran talento que hay ahí, grandes ideas, grandes profesionales y aplicaciones muy útiles que deberían ser potenciadas. Deberíamos buscar la forma de que no llegase un *venture capitalist* extranjero y comprase una *startup* española con una idea que tuviese un gran recorrido. Pero eso tiene su doble vertiente.

El mercado de transacciones en torno a la seguridad es de los más prolíficos en el mundo. Se compran y se venden empresas por altísimos ratios respecto al EBITDA porque estar en ciberseguridad se supone que es avanzado y puntero. Esto es algo a considerar. Si la gente que invierte dinero de forma profesional piensa que esto es un nicho, a lo mejor es un indicador de que es un nicho para todos.

Respecto al marco normativo, ya lo hemos tratado, pero quiero incidir en la perspectiva más internacional, que es la que nos ayudaría a todos a perseguir los temas que ahora mismo no son fáciles de perseguir. Se va a avanzando, pero, como ustedes saben, la autoría de los hechos en internet es muy difícil, salvo que utilices determinadas medidas, y a lo mejor hay que facilitar las medidas para poder perseguir bien las cosas.

Han preguntado sobre la valoración del nivel de ciberseguridad. En lo que se refiere a la Administración, el Centro Criptológico tiene un dato muy bueno en cuanto al volumen de aplicaciones crípticas para cada uno de los estamentos que he mencionado: la AG, las autonomías, la Administración Local y las universidades —cripticidad de las aplicaciones— y el grado de implantación, incluso evolutivo, desde el momento en que se puso en marcha la normativa. Ellos mismos hacen énfasis en un informe que comparten en foros en que todavía queda campo de desarrollo, sobre todo en la continuidad del negocio, en que las copias de seguridad estén disponibles y los mecanismos alternativos, en la monitorización, que es una disciplina relativamente nueva —toda la vida habíamos puesto controles de seguridad, pero ahora como las puertas están abiertas 24 horas, tenemos que estar pendientes 24 horas, y todavía hay carencias significativas—, y la concienciación.

Se ha mencionado varias veces a las pymes. El tejido empresarial español, según las estadísticas, tiene por encima de un 90 % de pymes, considerando gran empresa las superiores a 500 empleados. El Incibe publica muchas guías sobre cómo aumentar los niveles de seguridad; da formación, da talleres gratuitos; se recorre España ofreciendo gratuitamente a la gente esos talleres. Y esto sale con el poco presupuesto del que dispone el organismo, además de la gran cantidad de cosas que hace. Si queremos ayudar al tejido de las pymes, busquemos el mecanismo y démosle capacidad de ayudarles: formación; la estrategia que utilizamos en Deloitte fue la de unificar fuerzas. A lo mejor hay supraorganismos que pueden tener un servicio más unificado y que pueden ayudar a hacer esto de una forma más ágil. Desde luego, con los recursos que tiene hoy en día dedicados a ello no se puede hacer un tratamiento como si tuviésemos un centro de atención al usuario. Aun así, créanme, se hace muchísimo, y la Administración ayuda a resolver ciberincidentes incluso a particulares.

¿De dónde van a venir las amenazas futuras? Depende para quién. Los atacantes son diferentes y las intenciones también. El patrón común que más mueve el cibercrimen es el dinero. Cualquier cosa que lleve por detrás dinero es dinero. ¿Por qué ha crecido tanto el cibercrimen? Porque es mucho más impune, por estas dificultades que tenemos para perseguirlo. Con el narcotráfico, a lo mejor me pegan un tiro, pero en mi sofá en casa, primero, tienen que demostrar que he sido yo el que ha hecho algo, y luego me tienen que pillar y, además, que las evidencias soporten que he sido yo. Esto está proliferando, pero no se crean que con cosas muy avanzadas. Por ejemplo, las suplantaciones, el famoso *phishing.* Hay una página que les recomiendo, el *Anti-Phishing Working Group,* que sigue unas 70 000 campañas de *phishing* anuales, con distintos volúmenes, con lo cual el volumen de *phishing* es espantoso. Al principio era muy poco elaborado: alguien con acento ruso me pedía la *password* directamente, y si se lo daba, era un poquitín ingenuo. Pero ahora el nivel de suplantación es elevadísimo. Es muy difícil diferenciar al atacante de la empresa legítima.

¿De dónde van a venir las amenazas? Por un lado, depende del atacante; hay atacantes que son Estados, hay atacantes que son cibercriminales, etcétera. Van a evolucionar sus métodos y, desde luego, la amenaza avanzada existe. Y, por otro, van a venir de todos los chismes que conectemos a internet inseguros. Esta es una industria que ha nacido insegura, igual que el automóvil. Yo recuerdo que cuando mi padre me llevaba en coche, no existía el reposacabezas delantero, había un solo retrovisor, solo había cinturones de seguridad en la parte delantera, el ABS no existía. Pero esa era la industria, y nos movíamos, nos transportábamos y disfrutábamos del viaje en coche. Tenía sus riesgos, pero no sé si mayores o menores de los que tengo ahora. El problema es que nos empeñemos en conectar cosas a internet de

cve: DSCG-12-CM-90

forma insegura; nuevamente la concepción de los ciudadanos y dispositivos en el IOT, en el mundo del internet de las cosas que no tienen cabida en la securización. Hay que buscar mecanismos alternativos.

De la cooperación pública europea hemos hablado bastantes veces y somos un buen ejemplo, pero nuevamente todo a pulmón. Todo va fenomenal hasta que hablamos del dinero. Hablar de dinero es muy sano, todos necesitamos ganarnos la vida. ¿Cuál es límite de la colaboración público-privada? La propiedad intelectual. Si yo tengo un método diferencial, un *software* propietario, no puedo compartirlo fácilmente porque pierdo competitividad en mi negocio. Eso debería ser subvencionado por mecanismos que lo harían mucho más eficiente, pero hay cosas bastante identificadas.

En cuanto a las tareas no delegables del poder público, la protección de los españoles en los distintos ámbitos empieza en la defensa —en ciberseguridad ya estamos poniendo medios, seguramente insuficientes; tendríamos campo para avanzar—, lo mismo en Interior y en Asuntos Exteriores; la ciberseguridad es muy transversal a todos ellos.

El último tema se refiere al uso y seguridad de los datos personales. Lógicamente somos nosotros los que queremos tener esta aplicación instalada y no nos leemos lo que nos pide. Esto es como lo que me dice mi hijo: ¡Si lo tienen todos los de clase! Bueno, pues tú no. ¿Y por qué no? Ya te lo explicaré, pero lo que vamos a hacer es instalarnos esta aplicación tú y yo juntos. Y esa es una práctica muy sana, que ustedes se sienten con sus hijos a ver qué hacen con el ordenador, qué instalan en el ordenador. Porque vienen con problemas, y tenemos que aprender juntos muchas veces. No sabemos hasta qué punto nuestros hijos nos van a dar lecciones por las acciones de concienciación que pueden estar haciendo Policía y Guardia Civil de forma fantástica en los colegios. Mi hija lleva la cámara tapada con una tirita. Y le pregunto, ¿sabes por qué la tienes que poner? No, pero tengo que tener la tirita. Bueno, hija, muy bien, por lo menos tenemos la tirita, ya iremos avanzando.

Creo que más o menos he contestado a la mayor parte de las preguntas. Supongo que para lo que no quede suficientemente claro tienen ustedes un segundo turno.

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

Abrimos un segundo turno muy breve de tres minutos.

¿Señor Legarda? **(Denegaciones).**

¿Señor Gutiérrez? **(Denegaciones).**

¿Señora Angustia? **(Denegaciones).**

¿Señor Hernando? **(Denegaciones).**

¿Señor Cosidó? Tiene la palabra.

El señor **COSIDÓ GUTIÉRREZ:** Un turno rapidísimo, presidente.

Primero, para darle las gracias al señor Picatoste por las respuestas porque han sido muy completas y muy útiles, y segundo, dos cuestiones.

Una, certificación, entiendo que sí, pero ¿obligatoria o voluntaria? ¿Hasta dónde obligamos a certificar?

Y dos, identidad digital. Hemos hablado de la principal vulnerabilidad, que es el anonimato que en ocasiones hay en internet, ¿avanzamos hacia una mayor identidad digital en la red o lo mantenemos como está?

El señor **PRESIDENTE:** Pues solo tiene dos preguntas, que responderá con la continencia verbal que ha acreditado en la primera intervención.

El señor **PICATOSTE MATEU** (socio Risk Advisory, Deloitte): En cuanto al tema de la certificación, los mecanismos de certificación surgen siempre por la necesidad de un marco de referencia, y es una buena práctica. No hay nada que se pueda certificar si no hay un marco de referencia, porque, si no existe el marco, qué estamos certificando. El hecho de tener un marco de referencia contrastado, estandarizado es desde luego un gran avance. La certificación en la parte privada suele ser una garantía de calidad, siempre y cuando lo que estás certificando sea pertinente al uso de la certificación. Puede haber ciertos desajustes. Certificamos algo con una norma muy rimbombante pero estamos certificando un proceso que no tiene ninguna relevancia para el fin último. Como buena práctica, siempre debería terminar siendo voluntaria. ¿Obligatoria? La Administración *de facto* en la mayor parte de las licitaciones pide este tipo de acreditaciones. Cuando se quiere trabajar con la Administración pública, una ISO 27001, una 9000 están a la orden del día, y es una demostración de la calidad de los procesos de las empresas que entregan

cve: DSCG-12-CM-90

esos servicios. Y cuando hablo de la calidad de los procesos que entregan esos servicios, puede tratarse de un servicio público o privado. Nuevamente, el esquema nacional de seguridad está abogando por algún sello y creo que hay que estudiarlo.

En cuanto a la obligatoriedad, no creo que consiga el fin, porque el fin es el convencimiento de que esto mejora la calidad, y perseguir la calidad en sí es un objetivo.

Respecto a la identidad digital y al anonimato, cuando yo quiero acceder a un servicio absolutamente lícito, no tengo ningún problema en acreditarme y en dar todos mis datos, siempre y cuando no abusen de ellos. Ya hemos hablado de este tema. El anonimato en internet no es una materia para tratar en dos minutos. Se habla mucho de lo que hay en las redes Tor. Es un tema altamente complicado, porque cuando uno no quiere que se sepa que ha estado, algo puede haber detrás. Pero, dicho esto, creo que siempre tendrá que haber servicios que, para garantizar al resto de los usuarios un buen servicio, no van a tener que ser anónimos, porque, si no, se van a deteriorar las conversaciones y las interacciones que se tengan con ese servicio. Desde el momento en que tienes a alguien que no es quien dice ser —como en el caso de los foros, cuando se mete alguien que dice ser un niño, como tu hijo, y no lo es— tendremos que avanzar para proteger. Hay redes sociales que utilizan esto de una forma muy adecuada, pero en otros casos no se pueden poner puertas al campo. Es más, yo siempre me planteo por qué hay una red que hace no sé cuántos niveles de capas de encriptación, o cambio de direcciones IP dinámicas, y quién puede estar detrás para que todo el mundo entre por allí y esté vigilando. En todo caso, el que quiera hacer un uso anónimo de internet, que lo haga como considere.

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

Damos por terminada esta comparecencia, reiterándole el agradecimiento de toda la comisión.

El señor **PICATOSTE MATEU** (socio Risk Advisory, Deloitte): Muchas gracias a vosotros. **(Pausa).**

— DEL GENERAL DE DIVISIÓN DON JOSÉ LUIS GOBERNA CARIDE, SUBDIRECTOR GENERAL DEL CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (CESTIC), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Senado 715/000416 y número de expediente del Congreso de los Diputados 212/001203).

El señor **PRESIDENTE:** Continuamos con la sesión. Me doy por enterado de que hay una discriminación por cámaras en lo que se refiere a la intendencia; en concreto, en cuanto al café, que supongo que será corregida en el acto.

Y le doy la palabra al general Goberna para que lleve a cabo su primera exposición.

El señor **GOBERNA CARIDE** (general de división y subdirector general del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones, CESTIC): Buenas tardes a todos. Muy amables. Muchísimas gracias por la invitación para comparecer en esta sede parlamentaria, sede de la soberanía nacional. **(El señor compareciente apoya su intervención con la proyección de diapositivas).**

Es un honor comparecer hoy en esta Comisión Mixta de Seguridad Nacional. Como saben, las tecnologías juegan un papel de gran relevancia en el mundo globalizado en el que vivimos, caracterizado por la rápida y constante evolución. Estamos en los albores de la cuarta revolución industrial, caracterizada por la plena automatización de la industria, sustentada en diversas bases tecnológicas, como el internet de las cosas, los sistemas ciberfísicos, la inteligencia de datos a gran escala —conocida como *big data*—, o el procesamiento y almacenamiento en la nube, que, indudablemente, van a cambiar la sociedad, tal y como la conocemos en este momento.

En el ámbito de la defensa y la seguridad, las tecnologías de la información y las comunicaciones son mucho más importantes si cabe, puesto que se han convertido en un elemento imprescindible para la operatividad y la supervivencia de las Fuerzas Armadas. Hoy no es posible realizar operaciones militares con garantías sin el apoyo de las tecnologías más modernas y avanzadas. En la tecnología radica, en muchas ocasiones, la seguridad y la superioridad de nuestras Fuerzas Armadas en los teatros y zonas de operaciones donde nos encontramos en este momento. Al mismo tiempo, las ciberamenazas están creciendo y evolucionan rápidamente, con una amplia gama de fuentes y actores de potenciales amenazas que tienen acceso a técnicas cada vez más sofisticadas para la explotación de las vulnerabilidades de las propias tecnologías, de los sistemas y de los servicios y aplicaciones a disposición de los usuarios. El peligro que representan estas amenazas para nuestra información se agrava por las deficiencias que

cve: DSCG-12-CM-90

siguen existiendo en los sistemas y en la gestión de la información, entre otras muchas causas. Por ello, no solo debemos aspirar a protegernos pasivamente de estas amenazas, sino que debemos ser capaces de anticiparnos a ellas y evitarlas de forma proactiva.

En esta exposición haré un repaso de la normativa que nos sirve de arranque para todos los pasos que el Ministerio de Defensa ha ido dando durante estos dos-tres últimos años. El primer contexto estaría enmarcado por la Estrategia de Seguridad Nacional de 2017, que establece como objetivo de ciberseguridad garantizar un uso seguro de las redes y los sistemas de información y comunicaciones, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques —entendiendo esa respuesta, como ha dicho el señor Picatoste, como esa resiliencia—, potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. Para ello se fijan seis líneas de acción, que ustedes conocen perfectamente: capacidades y coordinación, normativa, organización, estructuras de cooperación, industria e innovación, conocimientos y cooperación internacional.

La Estrategia de Ciberseguridad Nacional de 2013, cuya revisión estaba prevista en el texto de la anterior Estrategia de Seguridad Nacional, abundaba en esta materia y fijaba como objetivo global lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, y que fortalezca las mismas capacidades que se citaban antes: prevención, defensa, detección y respuesta a los ciberataques. Establecía seis objetivos: la Administración General del Estado, en general, el sector público; el sector empresarial; las capacidades; sensibilizar sobre los riesgos; conocimientos; y el ámbito internacional, una vez más. En su primer objetivo es donde se encuentra el Ministerio de Defensa y se indica que, además de mejorar las capacidades de los sistemas militares de defensa y de inteligencia, es necesario reforzar la seguridad de los sistemas de información y comunicaciones estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio. Concretamente, en la línea de acción número uno, que supongo que será revisada cuando corresponda, se pide incrementar las capacidades de prevención, detección, análisis, respuesta, recuperación y coordinación ante ciberamenazas, haciendo énfasis, una vez más, en las Administraciones públicas, en las infraestructuras críticas, en las capacidades militares y de defensa y en otros sistemas de interés nacional. Incluye potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna en el ciberespacio, legítima y proporcionada, ante amenazas o agresiones que puedan afectar a la defensa nacional.

Finalmente, en ese marco general, quiero hacer una alusión al esquema nacional de Seguridad, que realmente es el verdadero instrumento para medir y para elevar nuestro nivel de ciberseguridad nacional, que establece seis principios básicos: una seguridad integral, gestión de riesgos —prevención, reacción—, recuperación, líneas de defensa en profundidad, reevaluación periódica y función diferenciada. ¿Y diferenciada de qué? Pues dentro de los sistemas, la seguridad de lo que es la información y de lo que son los servicios en sí mismos. Asimismo, fija 15 requisitos mínimos de seguridad, que no voy a citar porque son realmente prolijos, y abundan en todo tipo de variables sobre los que descansa precisamente ese nivel de seguridad; y recoge 75 medidas concretas o agrupadas en tres áreas: las del marco organizativo, las del tipo operacional y las de protección, que no solamente se fijan en los sistemas sino que también van a las personas, a las instalaciones, a la documentación —que ya deja de ser en papel para ser electrónica— y a todos aquellos mecanismos que recogen la protección en el más amplio sentido de la palabra. Al final, también el esquema nacional de seguridad contempla la elaboración de un informe anual, del que luego les daré los datos que han expuesto hoy mismo el Centro Criptológico Nacional y su equipo de respuesta antes incidentes, el Computer Emergency Reaction Team. Además establece los criterios para la categorización de los sistemas, herramienta clave en todo este proceso en materia de seguridad y, para ello, se debe modular el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad. Considerar esa trilogía siempre es muy importante, en lugar de dar tanta importancia al continente, a los sistemas como el verdadero problema, porque el problema muchas veces es el contenido, la información, que es lo que realmente da valor a lo que transita por el sistema. En ese juego es donde está la seguridad bajo un criterio de clara proporcionalidad.

Hecha esta introducción, les querría mostrar qué es el centro que dirijo en el Ministerio de Defensa. Se trata de un centro creado hace poco más de dos años, en una revisión del real decreto de estructura orgánica básica del Ministerio de Defensa, con el objetivo principal de racionalizar el contexto de los sistemas y tecnologías de la información y las comunicaciones. En 2014 se inició un proceso de revisión de la política de los sistemas y tecnologías que estaba claramente desfasado desde el Plan director del año 2002. Se partía de un entorno caracterizado por una situación realmente insostenible que exigía

cve: DSCG-12-CM-90

lograr nuevas capacidades y salvar las existentes en un escenario de recursos económicos muy limitados. Como consecuencia, desde la Secretaría de Estado de Defensa se impulsó el desarrollo de una nueva política para adaptarla a las necesidades de la defensa nacional y sentar las bases para disponer de una única infraestructura integral de información para la defensa, gestionada de forma centralizada desde la secretaría de estado. Para ello, en septiembre de 2015 se creó el Cestic, y en diciembre de ese mismo año, en estrecha coordinación con la Jefatura del Estado Mayor de la Defensa, se aprobó la nueva política; y, en 2016, se aprobó la integración orgánica en el citado centro de otros organismos del departamento con responsabilidades en toda esta materia, iniciando un proceso de centralización y racionalización en el ámbito.

El Cestic depende directamente del secretario de Estado de Defensa, órgano superior del departamento al que le corresponde, entre otras competencias, la dirección, impulso y gestión de las políticas de sistemas, tecnologías y la seguridad de la información en el ámbito de la defensa. Al Cestic, como órgano subordinado, le corresponde la planificación y desarrollo de las políticas de los sistemas y también de la seguridad de la información del departamento, así como la supervisión y dirección de su ejecución. El Cestic es el operador de sistemas y proveedor de servicios de la citada infraestructura única y, por tanto, el responsable directo de su seguridad. A estos efectos, dependen funcionalmente de este centro todos los órganos competentes en la materia en las Fuerzas Armadas y de los organismos autónomos del departamento.

Dentro de las políticas para llevar a cabo su desarrollo se están realizando los planes correspondientes, cuyas principales medidas les describiré a continuación. Hay tres grandes planes: el primero, es el Plan de actuación para la seguridad de la información del Ministerio de Defensa, orientado a la seguridad integral de la información del departamento. Este plan recoge todas las medidas para facilitar el desarrollo de la política y está alineado con las regulaciones e iniciativas en esta materia en la Administración General del Estado. Tiene un horizonte de ejecución de seis años, desde 2018 a 2023. En él se establecen ocho objetivos estratégicos que, como ustedes pueden observar en la pantalla, contemplan el desarrollo de la normativa de seguridad de segundo y tercer nivel, estableciendo un proceso de revisión continúa; incrementar el grado de cumplimiento de la legislación vigente sobre protección de datos de carácter personal; incrementar el grado de cumplimiento del esquema nacional de seguridad; incrementar el grado de cumplimiento de la normativa de protección de información clasificada, que afecta a las cinco áreas en las que se organiza la seguridad de la información en el Ministerio de Defensa —personas, instalaciones, documentos, sistemas y empresas—; identificar medidas de protección para aumentar la seguridad en los sistemas, tanto en el entorno de la infraestructura permanente como en los desplegables en zonas de operaciones; incrementar el grado de conocimiento de la situación en materia de seguridad del departamento mediante indicadores y plan de auditorías; impulsar la capacitación, concienciación y sensibilidad del personal en seguridad e información; y, finalmente, constituir y optimizar el funcionamiento de la estructura de gobierno en el ministerio de la seguridad de la información, con sus niveles que, si quieren, les detallaré más tarde.

Este plan de actuación, recientemente publicado en el *Boletín Oficial del Ministerio de Defensa,* se desarrolla a través de seis planes, uno general, y uno adaptado a cada una de las áreas de las que hemos hablado anteriormente. Hay un plan de actuación sobre la seguridad de la información en las personas, aspecto crítico; la seguridad de la información en las instalaciones; el plan de acción sobre la seguridad en los documentos, ya no en los de papel sino en los electrónicos, en la transformación digital que estamos viviendo; el plan de acción sobre los propios sistemas; y, finalmente, en las relaciones con aquellas empresas que tienen que ver con el Ministerio de Defensa.

El segundo plan es de carácter complementario, pero realmente es el que debe disponer de una mayor dotación presupuestaria porque es el que está enfocado hacia las tecnologías. Tendrá un horizonte temporal de seis años también, y se denomina Plan estratégico de sistemas de información y comunicaciones. Este plan desarrolla los seis ejes estratégicos de la política tecnológica del ministerio: avanzar hacia esa única infraestructura; dar prioridad a las actuaciones orientadas a satisfacer las necesidades de las Fuerzas Armadas; potenciar la utilización de sistemas homogéneos normalizados e interoperables; consolidar la seguridad en los sistemas a través del fortalecimiento de las capacidades que he repetido tantas veces —prevención, detención y respuesta a los ciberataques—, en línea con la política de seguridad de la información del ministerio, con la estrategia de ciberseguridad nacional y con las políticas que vengan de las organizaciones internacionales en las que estamos presentes; avanzar

cve: DSCG-12-CM-90

hacia un nuevo modelo de gobierno integral de los sistemas de información, que ya es un hecho; y optimizar la gestión de los recursos humanos, financieros y materiales.

En materia de ciberseguridad, incluye, concretamente en el primer eje, diseñar y desplegar las capacidades de esa infraestructura única organizada en seis bloques, uno de los cuales es precisamente la seguridad de la información en los sistemas. Estas capacidades se integran en la citada infraestructura única, que será una infraestructura privada del Gobierno de España, destinada a los servicios específicos de la defensa y seguridad nacional, para lo que estará dotada de los más altos estándares de calidad y seguridad. Dicha I3D dispondrá de un núcleo protegido que asegure la supervivencia de determinados servicios críticos con el alcance necesario que posibilite el funcionamiento de los sistemas de defensa, incluso en situaciones adversas, o ante cualquier tipo de incidente que pueda afectarle. Para ello, la I3D contará con capacidades de ciberseguridad en cada una de sus áreas de capacidad. Asimismo, la I3D contará con un centro de operaciones de ciberseguridad que opere con todas sus capacidades: telecomunicaciones, infraestructura de núcleo, información, aplicaciones de usuario, gestión, etcétera. Para ello, el citado COS utilizará la información obtenida de los diferentes componentes de la infraestructura y llevará a cabo su normalización, agregación, procesamiento y evaluación, con el fin de proporcionar información relevante de todas las capacidades en tiempo real.

En el cuarto eje encontrarán el modelo de gestión de la seguridad de la información y la implantación de una estructura de coordinación asociada, así como el establecimiento de los procedimientos de coordinación y relación asociados a la gestión de dicha seguridad. Se contempla en este eje realizar el mayor esfuerzo posible para el cumplimiento y la adecuación al esquema nacional de seguridad de todos esos sistemas del núcleo protegido de categoría alta, dado que la información que va a rodar por ahí es reservada y secreta.

Por último, lo más cercano al común de los mortales es el Plan de acción del Ministerio de Defensa para la transformación digital, orientado a la revisión integral de los procesos y a la racionalización de los actuales sistemas de información y servicios de dicho ministerio relacionados con la Administración General del Estado, priorizando en este momento, en su primera parte, los que prevén las Leyes 39/2015 y 40/2015, de inmediata aplicación en el mes de octubre de este año. Tiene como finalidad principal lograr un mejor aprovechamiento de estos servicios, basados en la integración de capacidades en dichas actividades y procesos, e incluye todas las actuaciones en el corto plazo, dos o tres años, para llevar a cabo esta enorme normalización del Ministerio de Defensa en su servicio al ciudadano, en su relación con las empresas y en su relación con el resto de las administraciones.

En este momento hay dos ministerios que hemos aprobado este plan de transformación digital y, próximamente, en la comisión ejecutiva de estrategia, se van a debatir otros cuatro planes de transformación digital de la propia administración general en todo aquello que se refiere a medios y servicios que no afecten a la defensa, la consulta política, situaciones de crisis y seguridad del Estado que no manejen información clasificada. Esta es la primera parte de este plan que hemos aprobado.

La segunda parte ya está siendo diseñada y aborda los sistemas de carácter sectorial y operativo que prestan servicios directamente a las Fuerzas Armadas. Estos servicios formarán parte normalmente de lo que antes hemos denominado dominios de seguridad de carácter oficial y, preferentemente, del núcleo protegido de la infraestructura. Además de las medidas previstas por la Secretaría General de Administración Digital en la estrategia TIC de la AGE, las actuaciones de este plan tienen tres objetivos y las siete directrices de la estrategia de la información del Ministerio de Defensa. Por lo que se refiere a los tres objetivos: alinearse con los otros dos planes —la estrategia de digitalización y la estrategia de seguridad—; mejorar la explotación de la información —es decir, acercar el manejo de todos los dispositivos y aplicaciones al usuario—; y facilitar la accesibilidad sin perjuicio de la debida protección de la información. Para ello, se asegurará la información a lo largo del ciclo de vida, con la flexibilidad necesaria para que sea accesible a los usuarios autorizados, en el momento y lugar oportunos, de forma segura y fiable, estableciendo el entorno que proteja los activos de información del departamento de una manera en la que la protección de la información no afecte a su transmisión o a su tratamiento.

Las siete directrices, que al final son siete grupos de 27 medidas concretas, son: identificar y desarrollar procesos funcionales y operativos y los productos de información; identificar el valor de los datos y de la información; estandarizar datos, información, registros y archivos; implementar planes de formación y mejorar el empleo de aplicaciones de usuario y herramientas colaborativas; establecer una estructura de gestión de la información orientada a facilitar el desarrollo de los cometidos del departamento; facilitar el acceso directo; y, finalmente, proteger y gestionar el riesgo de los datos, de la información y del

cve: DSCG-12-CM-90

conocimiento, de manera que la debida protección de la información no afecte a su tratamiento o transmisión. En resumen, con estos tres planes se recogen las actuaciones coordinadas del Ministerio de Defensa en materia de ciberseguridad, con un enfoque integral de seguridad, tecnologías, procesos e información.

Para finalizar, quiero compartir con ustedes algunas reflexiones generales. Los retos a los que nos enfrentamos en materia de ciberseguridad nos exigen que sigamos reforzando y desarrollando nuestras capacidades y las medidas de protección de forma permanente en un nuevo marco de referencia, donde las telecomunicaciones, las grandes bases de datos, su procesamiento, almacenamiento, sistemas de identificación y acceso, aplicaciones de usuario y servicios de gestión forman ya un todo integral, que precisa también seguridad en profundidad, por capas, en todos los niveles. El mayor activo a proteger en los sistemas es la información, considerando su carácter estratégico para la defensa nacional y la necesidad de conocer su valor en cada caso, para lograr esa superioridad en la toma de decisiones o en la conducción de las operaciones militares que nos ofrezca la ventaja en la defensa y, llegado el caso, en el enfrentamiento. Cuanto más relevante y de calidad sea esa información, mayores deberían ser los recursos dedicados a su protección. Y cuanto mejor administrada, gestionada, explotada y protegida, más útil, fiable y provechosa nos resultará en todos los casos.

Técnicamente debemos centrarnos en los datos, como ha dicho anteriormente, en repetidas ocasiones, el señor Picatoste, para poder enfrentarnos a las nuevas y crecientes amenazas, y poder sacar mayor partido de la información.

Finalmente, insisto, en que es imprescindible aplicar el esquema nacional de seguridad a todos los sistemas de información, y la normativa de protección de materias clasificadas en el caso de la información de este carácter. Para mejorar el nivel de ciberseguridad de los sistemas debemos trabajar no solo en el ámbito tecnológico sino también en el normativo, organizativo, de competencias profesionales y de cooperación, factores que influyen directamente en el estado de la ciberseguridad en el que nos encontramos.

Muchas gracias.

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

Voy a dar paso ahora a los portavoces. Les rogaría que se circunscribiesen a los cinco minutos que les corresponden.

Tiene la palabra el señor Yanguas.

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

Me circunscribo a esos cinco minutos porque únicamente quiero intervenir para agradecer al general las explicaciones que nos ha dado.

Muchas gracias. Buenas tardes.

El señor **PRESIDENTE:** Muchas gracias.

Señor Legarda, tiene la palabra.

El señor **LEGARDA URIARTE:** Muchas gracias, presidente.

Simplemente quería plantear una cuestión. Nos decía al final de su intervención que la cuestión estratégica más importante es proteger la información, los datos. En este sentido, me gustaría que me dijera a qué información se está refiriendo. ¿Una información propia de los sistemas de defensa o transferida por organizaciones internacionales de las que formamos parte? Si esto es así, también me gustaría preguntar si tiene esto algo que ver en los sistemas de defensa y en la protección de la información con alguna actividad del ministerio, desde el punto de vista de defensa y de lo que se llaman las campañas de desinformación o los ataques disruptivos.

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

Señor Salvador, tiene la palabra.

El señor **SALVADOR GARCÍA:** Gracias, señor presidente. También seré breve.

Antes de nada quiero felicitarle y decirle que nos deja muy tranquilos en el sentido de que nuestro ejército está en buenas manos porque vemos que, como era de esperar, están perfectamente organizados, tienen un plan y saben perfectamente cómo desarrollarlo y llevarlo adelante.

cve: DSCG-12-CM-90

Quiero aprovechar su presencia aquí, ya que está en un ámbito distinto al de otros comparecientes que tienen que ver con la Administración o con el sector privado. Por ejemplo, cuando se ha mencionado el tema de las *fake news* se utiliza la palabra ciberguerra o ciberdefensa y parece ya que entonces entramos en palabra mayores, cuando al final estamos hablando también del uso fraudulento de la tecnología para conseguir unos fines que no son deseados.

Es verdad que desde hace ya bastante tiempo existe el mantra de que determinados ejércitos, de determinados países, podrían utilizar precisamente unidades bien pertrechadas y formadas en estos ámbitos para obtener información relevante de otros gobiernos, de otros ejércitos, y para llevar a cabo operaciones incluso agresivas en determinados momentos, con el fin de bloquear un país, etcétera. Sobre eso se ha hablado muy poco, incluso en esta comisión, porque siempre nos centramos en ciberdelitos y en ciberdelincuentes, pero no en ciberdefensa. Se presupone quién es el enemigo, quiénes son los malos, pero claro, hablar de que el Gobierno de otro país, que no nos ha declarado públicamente ninguna hostilidad, está haciendo travesuras que nos pueden generar graves perjuicios es muy complicado de explicar. ¿Por qué? Porque, primero, hay que demostrar quién lo está haciendo, y si son buenos y organizados costará mucho trabajo; y, segundo, porque tenemos que estar absolutamente preparados para no ser vulnerables, de manera que eso no nos pueda afectar y que, en un momento determinado, no digo poder contraatacar, pero sí tener actividades en este sentido de defensa.

He visto también en el organigrama que estaba presentando que, evidentemente, por una parte llevan a cabo todo un proceso de convergencia con la Administración General del Estado, para llevar el plan de la mano en cuanto a su desarrollo —y en mi grupo eso nos parece absolutamente adecuado porque todos los relojes tienen que estar sincronizados, en cuanto a la transformación digital— pero, por otra, también tienen en cuenta las estrategias políticas e iniciativas de OTAN y Unión Europea. Entonces, en ese marco que he circunscrito a otros países, que en un momento determinado pueden iniciar agresiones, lo que se denominaría en el mundo civil como ciberdelitos o ciberataques, ¿qué tipo de riesgos afronta nuestro país cotidianamente? No le voy a pedir que indique qué países lo han hecho, no le pondré en ese compromiso, pero ¿qué tipo de ataques se pueden producir en ocasiones a los que hemos tenido que dar respuesta, aunque no hayan tenido ninguna publicidad?

También quisiera preguntarle por el personal, el perfil, la formación y los recursos que destinan dentro del ejército, porque me ha parecido entender que son absolutamente conscientes de la grandísima importancia de este campo, aunque a veces no sucede lo mismo en la sociedad civil e incluso en la propia Administración. Ustedes no se pueden permitir fallar y, por tanto, me parece que eso sí está hecho. Sin embargo, me gustaría saber si, dentro del conjunto del ejército, están satisfechos con las inversiones que se están haciendo en este campo, si se están destinando todos los medios necesarios e, incluso, y con esto termino, si se está poniendo un mayor nivel de celo para poder hacerlo bien del que usted puede apreciar en el conjunto de la Administración General del Estado o, incluso, en la sociedad civil. En este sentido, quizá, por estar ajenos, probablemente, a los riesgos.

Muchas gracias.

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

Senadora Angustia, tiene la palabra.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente. Buenas tardes, general. Gracias por su presencia en esta Cámara y por la claridad de la exposición.

Dentro del esfuerzo que está completando el Ministerio de Defensa en torno al proceso de transformación digital, con esta puesta en marcha de una estrategia de información que permita afrontar absolutamente la eficiencia y el tratamiento eficaz y seguro de la información, que es un recurso estratégico que, además, tiene que estar sustentando por las tecnologías de la información y la comunicación, y que debe aportar esa visión de liderazgo, de la que muy bien se hablaba en la comparecencia anterior, quiero preguntar específicamente por las especificidades y la prioridad que, por supuesto, deben tener las propias Fuerzas Armadas dentro de ese plan global del Ministerio de Defensa. ¿Cuál es el grado de desarrollo de ese proceso de transformación digital dentro del espacio de las Fuerzas Armadas? ¿Cómo valora el espacio concreto de formación que se ha realizado? Y ¿cuáles son, dentro del espacio global de la transformación digital y del campo de la formación, los retos que quedan por delante o cuál es la parte del plan que queda por desarrollar, sobre todo, teniendo en cuenta que es importante no solo por la gestión del espacio interno sino por la relación, obligada y necesaria, dentro de la Unión Europea y de la OTAN como alianzas para la interoperabilidad y la seguridad en los sistemas de información y de las telecomunicaciones?

cve: DSCG-12-CM-90

Por otra parte, quiero hacer alguna pregunta de actualidad, contextualizada dentro del espacio del último año, en el que se han producido las supuestamente llamadas campañas de desinformación, ejercidas —dicen— por los espacios anticapitalistas contra Gobiernos occidentales y contra los intereses globales, intentando desestabilizarlos. Sin embargo, lo que sí ha quedado patente a lo largo de esto año es que las campañas de información que se enfrentan a estas mal llamadas —porque no hay pruebas de ellas— campañas de desinformación sí resultan ser eficaces, ya que lanzan mensajes que, sin ningún tipo de comprobación, sin ningún tipo de pruebas, sí calan y condicionan la imagen de muchos espacios, de muchos organismos y de muchos Gobiernos; repito, sin haber aportado ninguna información al respecto. En los últimos días se ha avanzado en ese espacio que lleva operando durante un año, y la sorpresa es que la conexión con la realidad no aparece por parte del bloque ruso sino que las conexiones se realizan en Estados Unidos y en la OTAN, hablando de manipulaciones de discursos políticos del presidente Trump, de que se han realizado a través de empresas de capital británico, como la Cambridge Analytica y recibiendo las informaciones de la desactivación de la posibilidad de operar en redes sociales de empresas como AggregatelQ, de capital canadiense —y, por lo tanto, creo que no está sujeta a ese eje del mal— o de Atlantic Council. Estos espacios terminan relacionados con la OTAN, porque parece que en esos sectores de poder político y esos medios de comunicación que manifiestan los estudios apoyados por *think-tanks,* la fuente de información es la inteligencia estadounidense o la propia OTAN, en el caso del Atlantic Council.

Entonces, al hilo de todas estas informaciones, nosotros sí pensamos que lo que queda en evidencia es la órbita de ese espacio de alianza que es la OTAN y, muy en concreto, el tratamiento de la información y la utilización que se le da en estos espacios de alianza. Esta teoría no solo es financiada por empresas de armamento, petroleras y fondos buitre, sino que hila de forma muy clara un espacio privado empresarial con los espacios políticos. Nuestra opinión ya queda manifiesta, pero la reitero: sí nos parece que se pone en evidencia ese espacio de alianza, pero ¿serán tenidas en cuenta estas informaciones? ¿Hay alguna previsión en la consideración de las estrategias? No estamos hablando de rupturas, que nadie malinterprete lo que decimos, pero sí de una revisión de este espacio de nuevas informaciones, de esas estrategias y de la política de gestión de datos, de información y de conocimiento conjunto que establecemos en ese marco de la OTAN y la Unión Europea.

Por otra parte, hemos de hablar en concreto de las actuaciones del *think tank* que es el Atlantic Council, porque ha hecho unas manifestaciones y ha pedido directamente al Parlamento español, a su Gobierno y a las agencias españolas de seguridad que se colabore para escrutar las actividades de plataformas y medios que tengan vínculos con Rusia y su impacto informativo en las democracias deliberativas. Repito que esto es importante porque en realidad no se ha aportado ninguna prueba de que haya una campaña guiada de manipulación y desinformación en el espacio ruso. Además, este *think tank* recomienda a los Estados Unidos —esto nos afecta, porque habla de comunicación estratégica con Europa— que reconstruya su diplomacia pública y su capacidad de comunicación estratégica con Europa prestando atención a las actividades del poder blando prooccidentales y proamericanas. ¿Se van a valorar en nuestros espacios de gestión, protección y seguridad de la información estas recomendaciones que hace el Atlantic Council? ¿Se está valorando atenderlas? ¿Se han valorado y se han descartado? Además, nos surge otra duda, ¿cómo de frecuentes son las revisiones de esa visión integradora y global en la estrategia de la información del Ministerio de Defensa en referencia, concretamente, a esas regulaciones en el ámbito de la defensa nacional?

Con esto concluyo y creo que además he sido escrupulosamente rigurosa con el tiempo.

El señor **PRESIDENTE:** No exactamente, pero, en fin, no ha estado mal. **(Risas.—La señora Angustia Gómez: Pero casi; lo he dejado ahí porque me parecía que tenía que dejarlo).**

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

Gracias, general Goberna, por su exposición. Como ha ocurrido hasta ahora con los comparecientes, hemos tenido la suerte de que usted también nos haya dado información interesante que nos ayudará después, en los debates, a construir el escenario sobre el que tenemos que trabajar, que no deja de ser ese novedoso escenario de lucha, de batalla o de guerra —como cada uno lo quiera llamar— que es el ciberespacio. Una vez superada la confrontación en el espacio de la tierra, el aire, el mar, el espacio sideral, etcétera, que ha sido la anterior a esta, con los famosos misiles del paraguas de protección, ahora nos encontramos con lo que viene a denominarse la guerra híbrida, la zona gris, y con lo que significa todo lo relacionado con el ciberespacio y con la utilización que de él hacen los poderes públicos para la defensa, la inteligencia o los sistemas de ataque que cada Estado considere oportuno impulsar para sus propios intereses.

cve: DSCG-12-CM-90

A mí lo que me parece un poco sorprendente cuando hablamos de desinformación es que se dé el visto bueno a una parte de la información que sale y no se le dé a otra. Creo que todas han de ser tenidas en consideración. A mí me resulta muy interesante lo de Cambridge Analytica, que, curiosamente, coincide en el tiempo con lo que se ha hablado de la famosa granja de San Petersburgo; coincide en el tiempo y la finalidad y el objetivo son el mismo. Lo difícil de demostrar, porque, si esa información se tiene, la tienen los servicios de inteligencia, pero elaborada según sus propios esquemas de funcionamiento y no la van a dar, es que haya un Estado detrás de esa intervención. Pero que la campaña de desinformación tenía unos nodos, unos puntos de encuentro, yo creo que está perfectamente demostrado. Recientemente se presentó un informe en el Instituto Tecnológico de Massachusetts que aclaraba algunas de estas circunstancias, que, además, tienen correspondencia en el tiempo, en los ritmos y en la planificación con dos instrumentos de información muy importantes, que son rusos, lo que no quiere decir que estén apoyados por el estado ni por los poderes públicos rusos, que son RT y Sputnik. Hay una correspondencia también, y una sincronización en el tiempo y en la información, al darle el primer impulso a esa información y después en la resonancia que los medios le dan.

Hay quien dice que lo que no está en la red no existe, pero yo soy de los que piensan que por mucho que esté en la red, si una información no aparece en los grandes medios de comunicación de masas no existe, por ejemplo, RT emite en 100 idiomas o dialectos. Esto hay que tenerlo en cuenta, porque en la red se habla el inglés, el castellano, el chino y alguno más, el francés o el alemán, y es complicado encontrar medios de comunicación que hablen 100 idiomas y dialectos. Yo no querría profundizar mucho más en esto, porque solo quiero que nos diga cómo visualiza cualitativamente el avance que puede haber en España en capacidad técnica, que englobaría tanto los recursos relacionados con las personas que tenemos destinadas en estas tareas, en estas funciones, como los medios tecnológicos y su relación con que sean propiamente españoles; o dicho de otro modo, cómo visualiza cualitativamente que formemos cuadros humanos y también diseñemos y fabriquemos esos medios tecnológicos propiamente nuestros; se lo pregunto con idea de que conozcamos un poquitín más la menor o mayor dependencia que tenemos de los medios humanos o tecnológicos de otros países. También quisiera saber cuáles serían los puntos prioritarios a mejorar para responder a esta realidad nueva, que cada vez se hace más evidente. Me refiero a la capacidad para responder a una mayor y mejor coordinación en ámbitos supra, como en los ámbitos interdepartamentales de la propia Administración pública. Por supuesto, también me interesa saber cuáles serían las prioridades para mejorar los medios humanos y tecnológicos que están a nuestra disposición hoy en día.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Tiene la palabra el señor Aznar.

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

Intervendré de forma muy breve, pero permítame que antes, igual que han hecho mis compañeros, le agradezcamos los senadores haber traído la celebración de la comisión a esta casa. Y a la vista de que ha funcionado el servicio de intendencia hábilmente manejado por el letrado de la comisión, ya que todo el mundo sabe que hay café aquí también, que se repita la experiencia.

General, muchísimas gracias por su intervención, concisa, concreta y, sobre todo, muy clara. Querría hacerle, como le digo, de forma muy rápida, dos o tres preguntas a lo máximo, para que pueda usted completar un poco lo que nos ha dicho. Como mis compañeros han hablado de ciberdefensa, de ciberseguridad, que son dos términos que venimos utilizando en algunas ocasiones incluso indistintamente, aunque yo creo que son conceptos que se pueden diferenciar claramente, me gustaría que usted nos los diferenciase, porque en la comisión, donde intentamos ser lo más precisos posible, y también en los medios de comunicación y en la calle, estos dos términos se están confundiendo habitualmente. Tenemos además algunos senadores que aquí nos sentamos —enlazando con esto— una curiosidad que quisiéramos despejar; en el caso de que se produjese un ciberataque a sus sistemas, ¿cómo se coordinaría con el cibermando de Defensa? Creo que es una pregunta muy concreta que nos podrá responder.

A lo largo de las comparecencias que se han venido sucediendo aquí hemos hablado, sobre todo en el Grupo Popular, en varias ocasiones de los ciberreservistas, que existen en países de nuestro entorno y que están dando un resultado importante, según confiesan algunas fuentes; sin embargo, aquí han hecho sonreír a muchos, como si estuviéramos hablando de alguna cuestión poco menos que ridícula. Por eso,

cve: DSCG-12-CM-90

me gustaría saber su opinión, porque nosotros entendemos que, salvo opinión más fundada, este puede ser un tema muy interesante en el futuro.

También me gustaría, para finalizar, que nos diera usted una pincelada sobre la trasposición de la directiva. Sabe usted que en este momento hay un anteproyecto de ley para trasponer la Directiva europea de seguridad de los sistemas de información y las redes. Me gustaría saber su opinión sobre cómo va esto.

Una vez más, muchas gracias por su exposición y, sin duda, por las respuestas que nos va a dar.

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

Tiene la palabra el general.

El señor **GOBERNA CARIDE** (general de división, subdirector general del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones): Muchas gracias, señor presidente.

Voy a intentar dar las respuestas más concretas posibles a las cuestiones que han planteado, que les agradezco de antemano porque abundan en lo que ha sido el centro de mi exposición.

El señor Legarda me preguntaba de qué tipo de información estamos hablando, si de la propia, la heredada o la transferida por las organizaciones internacionales. Luego me ha hecho otra pregunta sobre las campañas de desinformación.

Respecto a la primera pregunta, de qué tipo de información estamos hablando, le diré que de la información del Ministerio de Defensa, de información de carácter estratégico, de información que procede de consulta política, no estrictamente operativa, y de aquella que tiene el nivel más inmediato, de la información táctica en las zonas de operaciones en las que estamos involucrados. Por tanto, la información, como tal, es un segundo escalón de la jerarquía cognitiva. Debajo, como ustedes saben, están los datos y encima la información que tiene más o menos actualidad. Como hemos dicho, con el desarrollo de las tecnologías, lo importante son los datos porque con los mismos datos se pueden construir diferentes informaciones. Con el paso del tiempo, uno puede coger esa información y convertirla en conocimiento o archivarla. Por tanto, es un factor muy importante para poder concretar de qué estamos hablando en el ámbito de la información.

La información tiene un valor en función de su capacidad de responder a una necesidad inmediata. En el Ministerio de Defensa, el concepto que tenemos de esa información, que pueden ser noticias, eventos o cualquier cosa que cambie nuestra actualidad, tiene su valor en función de su capacidad de resolver el problema, y nuestro problema es la defensa nacional. En consecuencia, la organización de la información debe responder a lo que llamamos administrar la información, que es mantener su ciclo de vida, tener claro quién genera esa información; tener claro cuál es su nivel de credibilidad, de relevancia, que es el factor para despejar la duda sobre las campañas de desinformación; y tener claro cómo vamos a hacer que esa información sea útil, rápida y, además, adaptada. Por eso, hablábamos en la estrategia de la información de que hay que primar la accesibilidad, de que el usuario final, esté desplegado en Mali, en el Líbano, en Afganistán o Letonia, debe disponer de la información precisa para resolver su problema. Eso es lo que denominamos mejorar la explotación, acercar la información a quien la necesita. De esa manera, ¿qué conseguiremos? La superioridad en la información. Por eso decimos en el Ministerio de Defensa que la información es un recurso estratégico, porque hay que manejarla en cada momento en diferentes circunstancias, porque hay que ser capaz de gestionarla, y también de explotarla, de sacarle el mayor partido en cada momento. En cuanto a los tipos de información, reitero lo que he dicho al principio, que la información es de todo tipo, en función de los intereses de España y de su defensa nacional.

En relación a las campañas de desinformación, entiendo que usted quiere saber qué hay de creíble, de increíble o de certero. Pues bien, en ese ciclo de la información hay que realizar un análisis que también le sirve a la inteligencia, porque hay que ver de dónde procede la información. Es muy difícil ahora mismo, en el mundo en el que vivimos, identificar la fuente en muchos casos. Se puede estar transmitiendo una información desde el este, pero a lo mejor el origen está en el oeste. No se sabe. ¿Por qué? Porque, técnicamente hablando, es muy fácil transmitir una información desde América o Asia, pero, dada la dificultad de detectar los diferentes pasos de la difusión masiva que se hace de esa información o de los ataques que recibimos, es difícil poder identificar al agente agresor en cada momento. ¿Cómo se resuelve esto? Compilando, buscando patrones de comportamiento a lo largo del tiempo. El que realmente es un atacante no ataca un día, ese es un aficionado, el que ataca tiene un plan y un objetivo. Entonces la única forma de poder abordar y ganar credibilidad es compilando; es decir, acumulando información, procesándola, contrastándola y, a partir de ahí, generar un modelo y ver si ese modelo nos responde; es

cve: DSCG-12-CM-90

decir, aplicar el método científico, en una palabra. Si nos responde quiere decir que estamos en lo cierto; siempre pensando que el nivel de certeza que hay en estas cosas puede ser relativo. Es lo único que les puedo decir.

No me corresponde hablar de inteligencia —y luego responderé con más detalle a la pregunta del señor Aznar— ni de ciberdefensa. Yo dirijo el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa desde un punto de vista estrictamente técnico, de provisión de servicios. Evidentemente, los ataques los recibimos nosotros, no los reciben otros; pero las respuestas, buscar la resiliencia, está en manos operativas, no está en las manos del gestor de la infraestructura. Esta cuestión la podré ir resolviendo según vaya contestando a las preguntas.

El señor Salvador hablaba de la ciberguerra, de la ciberdefensa, usaba toda esta terminología que hay ahora. Hoy ya no se declara la guerra, pero ni en los otros ámbitos. Esta la vivimos, pero ni nos la han declarado ni nos ponen condiciones para que capitulemos o para que lleguemos a un acuerdo; sin embargo, existe. Es una guerra que va a más. ¿Por qué? Porque la sociedad se está transformando, porque vamos hacia la cuarta revolución, como decía al principio. Es decir, estamos abandonando el ámbito electrónico y estamos metiéndonos en el mundo digital pero realmente inteligente, del internet de las cosas. El coche nos va a decir que no va a andar porque no hemos pasado las revisiones correspondientes y los sistemas van a dejar de funcionar cuando no se haya cubierto toda su logística integrada; por tanto, tratamos de ser eficientes. Las máquinas cada vez alcanzarán un mayor protagonismo, y en la guerra más; en la guerra cada vez más porque resulta más barato, entre otras cosas. Este es un ámbito que no requiere grandes inversiones si lo contrastamos con otros sistemas, ¿verdad? Es un sistema que en sus costes va a la baja porque los teléfonos móviles cada vez son más baratos y en cuanto a la fibra óptica en España no les quiero a ustedes ni contar el despliegue que tenemos. Las capacidades nacionales y las infraestructuras que tenemos son realmente muy amplias y muy buenas y, por tanto, tenemos que aprovecharlas.

Me preguntaba usted por las estructuras operativas que hay en todo este mundo. Se habla mucho de ciberdefensa, que es una faceta de la defensa nacional que se complementa con otros ámbitos ya bastante más tradicionales en nuestro mundo, en el mundo militar, como puede ser la guerra electrónica, las operaciones de información, que en muchos casos enfocarían mejor, desde mi punto de vista, muchas de las cuestiones que ustedes plantean de las *fake news* o de la desinformación. Es menos un problema de la ciberseguridad que un problema de operaciones de información, de operaciones psicológicas. España tiene muchísima experiencia en esto porque hemos participado en operaciones de paz y ha logrado grandes éxitos; por ejemplo, estabilizar en los Balcanes o llevar una política de comunicación estratégica en Afganistán. Ahí ha habido un gran protagonismo español. Es un sector en el que les aseguro que somos líderes. Sí, somos líderes en comunicación, en estabilizar zonas, en hablar con agresores, en que hablen entre sí, es decir, en generar un clima de mayor estabilidad y reconducción de una sociedad. Eso se lo puedo confirmar porque lo he vivido en primera persona.

En otros países, efectivamente, este es un tema que se está abordando con esa perspectiva integral. A veces escuchamos que países como China, o como Israel, y recientemente Alemania, tienen unos contingentes tremendos metidos en este ámbito. Están haciendo un esfuerzo enorme en este reenfoque de capacidades, pero están aprovechando las capacidades que ya tienen, es decir, están integrando la guerra electrónica, las operaciones de información, la inteligencia táctica, etcétera; estamos en el camino, porque las capacidades operativas dependen de la disposición de conjuntar que tengamos. Ya no se conciben operaciones solo del Ejército de Tierra, o solo de la Armada o del Ejército del Aire. Abrimos un nuevo dominio, el del ciberespacio; dominio en que no se puede interaccionar solo con alguien que nos quiera hacer un poco la guerra en la red; hay otros aspectos de la red que hemos de abordar, porque no solamente se trata de negar un servicio, de intentar robarnos los datos o de suplantar nuestra identidad. Es un concepto integral que todos nuestros aliados están enfocando de esa manera.

Me preguntaba usted qué tipo de ataques recibimos. Le contesto: de ese tipo; son ataques bastante cotidianos, de denegación de servicio, de hacer caer, con determinados correos, al usuario, lo que ocurre normalmente; pero también hay *phishings* y otros ataques más rocambolescos de ingeniería social. Lo que pasa es que internamente en el Ministerio de Defensa no van buscando normalmente a la persona, sino que se van realizando determinados ataques para sacar la firma, que se dice. Se quiere ver cómo nos comportamos. Esa es la evaluación que le puedo hacer en este momento.

Los perfiles de formación, sobre los que han preguntado varios de ustedes, son muy importantes y se están abordando en todos los niveles, en la enseñanza de formación, en la de perfeccionamiento y en la

cve: DSCG-12-CM-90

de especialización. En este momento tenemos en marcha varias iniciativas de estudios de postgrado con universidades en Madrid y fuera de Madrid para introducir estas materias en los diferentes niveles de enseñanza. Creemos que revisar el catálogo nacional de capacitaciones profesionales es una oportunidad, un elemento clave para toda la población, porque ahí está muy estructurado en los cuatro niveles de Europa cómo es la enseñanza en España al margen de las titulaciones. Estamos echando mano de esas referencias porque creemos que en el sistema educativo general normalmente está la solución para cuestiones tan técnicas como estas. Con esas familias que hay en el catálogo nacional, de telecomunicaciones y de informática, se forma a nuestra población en los centros de enseñanza del sistema educativo general. Introduciendo esas variaciones, se mejora todo, y nos beneficiamos en las Fuerzas Armadas porque, al fin y al cabo, nuestra enseñanza está homologada, está integrada en el sistema educativo general, y si se da formación de ciberseguridad en un instituto politécnico o de enseñanza secundaria nos vamos a beneficiar todos los españoles. No sé si he contestado a todas sus preguntas, espero que sí, más o menos.

La señora Angustia me ha hablado prolijamente de la transformación digital en nuestras Fuerzas Armadas. Me preguntaba, en concreto, qué prioridad le daban la parte de la Administración General del Estado y la parte operativa. Como he dicho antes, el Ministerio de Defensa, igual que el Ministerio del Interior, tiene dos planes distintos, dos planes diferentes por la materia, porque hay materias que afectan a la consulta política o a la defensa nacional, y hay también materias clasificadas; cada información necesita un tratamiento diferente. La digitalización no solamente consiste en el empleo de mejores bases de datos, de mejores iPad, de mejores procesadores o de mejores ordenadores; la digitalización consiste principalmente en revisar la organización, en ver cómo las tecnologías nos pueden ayudar y lo que está en el medio entre esas tecnologías y la organización es la información una vez más; o sea, depurar datos, homologar datos y estandarizar el tipo de datos. No podemos estar hablando de *big data* cuando las fuentes de los datos son tan diversas, cuando tenemos a lo mejor una inflación enorme de sistemas de información. Lo primero que hay que hacer es homologar el dato e integrar los que tenemos porque no podemos hacer borrón y cuenta nueva. A partir de esos datos hay que estandarizar productos de información, como se hace en la Administración General del Estado, y en los ministerios. Ahora que estamos en plena campaña de la declaración de la renta pueden ver que el esfuerzo que año a año se hace para digitalizar el pago del impuesto es tremendo. Esas son las referencias; los sistemas tácticos tampoco son tan distintos y el tratamiento debe seguir unos cauces parecidos.

La formación —contesto a las preguntas al respecto aunque creo que ya las he contestado— es una preocupación constante en nuestro sistema de enseñanza y el salto que estamos dando es importante. El mando de ciberdefensa, con verdadero liderazgo, nos está concienciando de los riesgos que entraña esta amenaza en el día a día para todos nosotros, y también se realizan cursos de concienciación, informativos y formativos, con los que se obtiene una titulación que capacita para ocupar puestos de trabajo. Estamos empezando; no es un tema que se pueda resolver en pocos meses.

En relación con lo que usted me dice de las campañas de desinformación y de la credibilidad de todas esas aseveraciones que se hacen, le digo lo que he dicho antes, que hay que analizar esas informaciones con rigor, y que hay que buscar la relevancia que tiene esa información para nosotros. Hemos de analizar si es objetiva, si es oportuna, si es útil, si es eficaz, si es precisa y, sobre todo, si es fiable, porque puede proceder de una fuente muy seria, pero, a lo mejor, dicha fuente no tiene las mismas intenciones que nosotros. Todo eso es un proceso que se llama ciclo de inteligencia. Pero, insisto, no soy yo la persona que tenga la competencia para hablar de este asunto.

Las campañas de desinformación, como he dicho, si cubren esos parámetros de los que hemos hablado, a lo mejor podríamos asociarlos. Pero ya le digo que todo eso tiene que ser analizado con rigor y con metodología. En España se está avanzando a pasos agigantados. Lo dice el Centro Criptológico Nacional al hacer su informe anual. No sé si lo conocen, se llama INES —un nombre muy español—, es el Informe Nacional del Estado de la Seguridad, que año a año, realiza ese análisis en todos los ámbitos que el señor Picatoste enunció antes. Cada año se incrementa el número de empresas que llevan a cabo esa auditoría general. Por tanto, nos dice que estamos en una situación media. No es para echar cohetes. Pero eso nos tiene que dar también un mensaje alentador, el de cada vez hay mayor conciencia de que, efectivamente, hay que cubrir esos parámetros y aplicar esas 75 medidas. Verdaderamente, es un lujo tener un esquema nacional de seguridad sobre el que reflejar cómo nuestros sistemas pueden ser de mayor o menor fiabilidad, o cómo la información está siendo mejor o peor procesada. Yo lo enfocaría de esa manera.

cve: DSCG-12-CM-90

Por lo que se refiere al avance en la formación de las personas, es evidente. Le puedo contar, por ejemplo, que la presencia industrial de España en este ámbito, en la OTAN, cada vez es mayor. Las empresas españolas tienen un protagonismo importante en las licitaciones, más del que yo he conocido hace diez años, para la renovación tecnológica de la alianza. Están presentes en determinados sistemas, lo que, lógicamente, nos revierte a nosotros. Porque en todo aquello que se pueda desarrollar dentro de la alianza, tecnológicamente hablando, ahorramos dos pasos y no tenemos por qué volver a darlos aquí. Puedo asegurarle que, en efecto, estamos dando pasos muy importantes.

Finalmente, el señor Aznar me pedía que diferenciase entre ciberdefensa y ciberseguridad. Esta última es una capacidad similar a las telecomunicaciones, similar a la informática, más estructural, más de infraestructura, es decir, hablamos de grandes bases de datos, de capacidad de almacenamiento, de capacidad de procesamiento, de capacidad de acceso y de identificación. Hay otras capacidades en un nivel superior, que se plasman en cada uno de los sistemas que, al final, se vienen reflejando en nuestros terminales de usuario. La ciberseguridad es transversal, es decir, que requiere de la seguridad de las telecomunicaciones, de la seguridad de la informática, de la seguridad de su iPad, de todos los niveles. No consiste en la capacidad de asegurar una línea de comunicación, ya sea de satélite, de fibra óptica o de radio; o en la capacidad de asegurar una base de datos; o en que usted tenga el sistema operativo actualizado en su teléfono, sino que su abordaje es integral. Y, por tanto, necesita un tratamiento integral. Va unida a la infraestructura, al día a día.

¿Y qué es la ciberdefensa? Hemos de partir de la idea de que ya no es una capacidad estrictamente técnica, sino operativa. Porque se parte del hecho de que ya no tengo un fallo cuando tengo configurado mi sistema, sino que tengo la presunción o la seguridad de que alguien me está atacando. Entonces, tengo que saber quién me ataca y qué características tiene ese hipotético atacante, qué nivel de riesgo conlleva y, a la vez, si se pone muy pesado y me pone en riesgo determinadas estructuras que hacen que la defensa nacional se ponga en riesgo, incluso tendré que pensarme si le tengo que atacar, aunque en este aspecto no va a haber efectos letales, pero, a lo mejor, no nos queda más remedio que tomar esta medida. Quiero decir que la ciberseguridad es una capacidad de infraestructura, así la define la NATO, la OTAN, y la ciberdefensa es una capacidad operativa, igual que la guerra electrónica, la inteligencia táctica, la defensa aérea o la vigilancia marítima o cualquier otro tipo de operación militar. En ese contexto se utilizan muchas veces las palabras CERT, Csirt o COS, y esa es la distinción que tenemos que hacer. Los centros de operaciones de ciberseguridad son centros de operaciones de infraestructura y los CERT son centros de respuesta, no solo de resiliencia, como decía el señor Picatoste, sino de respuesta en el sentido de que te voy a responder. Es decir, tengo que disuadirte o crear un sistema de inteligencia para generar una decepción, como decíamos antes cuando hablábamos de las desinformaciones.

En ese sentido, el Ministerio de Defensa ha atendido a las dos necesidades. Por un lado, ha creado el mando de ciberdefensa porque es una capacidad operativa necesaria. Tenemos que hablar el mismo idioma con nuestros aliados porque ellos también están desarrollando esas capacidades. En ese ámbito es más difícil hablar, también se lo puedo decir, porque cuando se habla de armas la cosa se pone un poquito más complicada, entre otras cosas, porque son capacidades que uno tiene para poder guardar su casa y no suele ser tan fácil compartirlo. En cambio, en la ciberseguridad sí. ¿Por qué? Porque vivimos mucho más a caballo de las tecnologías, es mucho más fácil compartir riesgos porque, entre otras cosas, al final, si no actualizamos determinados *software*, no lo actualizamos todos. Lo que está ocurriendo con el *wannacry* o con otros incidentes que ha habido últimamente con microprocesadores muchas veces no se deben a que haya habido un ataque; el ataque se produce porque antes ha existido una vulnerabilidad y es más fácil compartirlo. En este aspecto, es muy importante tener una visión integral. El Ministerio de Defensa decidió crear el Cestic porque no se podía estar llevando diferentes comunicaciones, tratamiento de la comunicación o diferentes capacidades satelitales en varios centros. Por eso se realizó esa integración.

¿Qué ocurre cuando hay un ataque? Mire usted, yo me pongo a las órdenes del general Medina. Existe un acuerdo entre el Sedef y el Jemad de que en el momento en que se produzca un ataque, una situación de beligerancia, donde no habrá declaración de guerra, repito, evidentemente, se activa un plan derivado en el cual el Ministerio de Defensa tiene que defenderse de aquella manera, es decir, no se defiende solo cerrando la puerta, sino aplicando un mayor número de medidas de defensa adicionales, aplicando toda la inteligencia que uno haya podido acumular previamente, colaborando con el centro principal de referencia, que es el Centro Criptológico Nacional, que actúa de esta manera, y, llegado el

cve: DSCG-12-CM-90

caso, si el Jemad lo decide, en coordinación con el mando de operaciones, realizar una operación de respuesta de otra manera, un ataque en toda regla en el ciberespacio.

Me hablaba usted de los ciberreservistas. Para mí es un tema serio porque, en el modelo de ejército profesional que tenemos, la alternativa para responder a una mayor necesidad de personal en el Ministerio de Defensa son los reservistas, en este ámbito y en todos los demás. ¿Cuál es la clave de lograr el éxito, al igual que se ha logrado en otros ámbitos como, por ejemplo, en la sanidad militar? La selección y la formación. Este es un ámbito, como hemos hablado antes, muy novedoso.

Por tanto, para poder ser ciberreservista voluntario, que supongo es de lo que habla usted, porque también los hay de alta disponibilidad u obligatorios en caso de que el Gobierno lo decida, la clave está en delimitar perfectamente cuáles son las características de selección: técnicos superiores, técnicos medios, técnicos ingenieros, graduados... Hay que establecerlo y luego identificar los puestos de trabajo. En la parte de ciberseguridad que me toca yo estaría encantado de tener ese tipo de personal y estoy convencido de que el general Medina también, y en otros ámbitos de la ciberdefensa y de la ciberseguridad de los ejércitos, supongo que también. Y luego hay que realizar un planeamiento serio en lo que se refiere a la formación continuada. Es decir, el ciberreservista puede ascender como cualquier otro reservista. Si es oficial puede llegar a capitán, si es suboficial también puede escalar en los diferentes niveles, y lo mismo sucede con la tropa. Por tanto, es un tema que hay que planear y hay que crear incentivos.

Por último, me preguntaba usted por la Directiva NIS. La Directiva NIS es una directiva que trasciende un poco al ámbito de la defensa porque, tanto en esta directiva, como en la parte correspondiente a los sectores estratégicos a que afecta la defensa, no es un sector estratégico crítico, no le afecta la Ley de protección de infraestructuras críticas, y por tanto, es un ámbito en el que estamos un poco de lado. Es decir, sí se identifica el centro de respuesta a incidentes informáticos del Ministerio de Defensa, pero no por el hecho de jugar dentro de las infraestructuras críticas, sino poniéndose a disposición del Consejo de Seguridad Nacional. Por tanto, es un ámbito más donde el Consejo de Seguridad Nacional ejerce su coordinación, pero no porque exista un sector estratégico de la Defensa Nacional. No se contempla ni en la ley de infraestructuras críticas ni en la transposición de la directiva. Así pues, es un tema en el que estamos; se ha participado comentando esa directiva, pero no de una forma directa, aunque no por ello dejo de reconocer que es algo muy importante para España.

Y con esto creo haber contestado ya a todo.

El señor **PRESIDENTE:** Muchísimas gracias, general.
Se abre ahora un segundo turno con la brevedad de la que ustedes han hecho gala.
Tiene la palabra el señor Legarda.

El señor **LEGARDA URIARTE:** Muchas gracias, señor presidente.
Intervengo solo para agradecer al general la respuesta que me ha dado.
Muchas gracias.

El señor **PRESIDENTE:** Gracias.
Tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Gracias, señor presidente.
Simplemente quiero agradecer la intervención del general.

El señor **PRESIDENTE:** Gracias.
Tiene la palabra la señora Angustia.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente.
No vamos a hacer uso del turno; solo queremos agradecer al compareciente, tanto su exposición, como su respuesta a las preguntas que le hemos formulado.

El señor **PRESIDENTE:** Gracias.
Tiene la palabra el señor Raffo.

El señor **RAFFO CAMARILLO:** Gracias, señor presidente.
Yo también quiero agradecer al general su presencia y la información que nos ha facilitado.

cve: DSCG-12-CM-90

El señor **PRESIDENTE:** Gracias.
Tiene la palabra el señor Aznar.

El señor **AZNAR FERNÁNDEZ:** Gracias, presidente.
Yo exactamente igual que todos.

El señor **PRESIDENTE:** Pues muchas gracias, general. Ha hecho usted gala de la celeridad y precisión que se le presume a un general de división del Cuerpo de Ingenieros. Y le ha devuelto la tranquilidad al señor Salvador, que sabe que estamos en buenas manos; de modo que el fin de semana será extraordinariamente plácido. **(El señor Salvador García: No lo dudaba, ¿eh?—Risas).**
Gracias por su comparecencia, general.
Se levanta la sesión.

Eran las diecisiete horas y cuarenta minutos.

cve: DSCG-12-CM-90