DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 111 | Pág. 1

DE SEGURIDAD NACIONAL

PRESIDENCIA DEL EXCMO. SR. D. JUAN JIMÉNEZ TORTOSA
VICEPRESIDENTE PRIMERO

Sesión núm. 19

celebrada el martes 9 de octubre de 2018
en el Palacio del Congreso de los Diputados

Página

ORDEN DEL DÍA:

---

cve: DSCG-12-CM-111

Se abre la sesión a las diez de la mañana.

COMPARECENCIA DEL SEÑOR HERNÁNDEZ GARCÍA (CORONEL DEL ÁREA TÉCNICA DE LA JEFATURA DE INFORMACIÓN DE LA GUARDIA CIVIL), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/001760 y número de expediente del Senado 713/001042).

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Buenos días, señorías. Vamos a dar comienzo a esta sesión de la Comisión Mixta de Seguridad Nacional.

En primer lugar quiero excusar la ausencia del presidente de la Comisión por encontrarse hoy en Valencia.

Ha sido solicitada la comparecencia del señor Hernández García, coronel del área técnica de la Jefatura de Información de la Guardia Civil, a quien damos la bienvenida.

Señor Hernández, tiene la palabra.

El señor **HERNÁNDEZ GARGÍA** (coronel del área técnica de la Jefatura de Información de la Guardia Civil): Muchas gracias, señor presidente.

Señoras y señores diputados y senadores, es un placer y un honor estar aquí hoy representando al Cuerpo de la Guardia Civil. Voy a intentar trasladarles la visión que desde él tenemos sobre la problemática de la ciberseguridad tal y como se encuentra en este momento. Voy a dividir la intervención en dos partes: en primer lugar —seguramente otros ponentes ya lo han hecho—, voy a exponer el estado de la situación —intentaré ser lo más breve posible— y, a renglón seguido, cómo estamos estructurados y organizados en el Cuerpo de la Guardia Civil y cómo atendemos a esta amenaza real. **(Apoya su intervención con una presentación en Power Point)**.

Así pues, en primer lugar, en referencia a Internet, creo que todos saben que a lo largo de los últimos años la generalización del uso de las tecnologías de la información y las comunicaciones ha propiciado un fenómeno sin precedentes y con profunda influencia en lo político, social y económico. Resulta incuestionable que el fenómeno de Internet ha traído consigo la mayor revolución tecnológica que ha vivido la humanidad, puesto que, más allá de los aspectos meramente técnicos o productivos, ha tenido y sigue teniendo una significada repercusión en la forma de moldear nuevos hábitos y comportamientos sociales. La denominada globalización presenta un marco de grandes oportunidades, pero lleva parejo riesgos, la mayoría *a priori* intangibles y, por tanto, de difícil percepción y que en una imparable escalada están llegando a tener transcendentes repercusiones. Los más relevantes riesgos pueden transformarse en verdaderos cisnes negros. De hecho, el propio Internet es un cisne negro, por ejemplo, con el impacto que puede tener la informática de usuario en nuestra sociedad, como en el 11 de septiembre, nuestro 11-M, etcétera. Resulta incuestionable que esta revolución tecnológico-social ha aportado aspectos muy positivos, como es la globalización del conocimiento y el acceso universal a la información a través de la red de redes. Estamos siendo testigos de una total transformación de las relaciones humanas y en la que ya se viene a denominar cuarta revolución industrial. Pero, como sucede con demasiada frecuencia, esta creación humana también ha sido y está siendo utilizada para satisfacer los ilícitos intereses de individuos y grupos faltos de escrúpulos, que han visto en Internet una oportunidad para saciar sus oscuros e ilegítimos intereses. Como tales, podríamos hablar del cibercrimen, el ciberterrorismo, el *hacktivismo*, el ciberespionaje o, incluso, la ciberguerra, que, lamentablemente, se están haciendo un hueco en lo cotidiano. De igual manera, las relaciones entre Estados se están viendo profundamente distorsionadas y en algunos casos gravemente alteradas.

Con respecto al ciberespacio, les puedo comentar que este nuevo marco de relación en lo social, cultural, económico, político y militar depende cada vez más de lo que viene a denominarse el ciberespacio, convirtiéndose este en un recurso vital para el normal desarrollo de las sociedades modernas, por lo que se ha hecho más que conveniente y podríamos decir que necesario articular un sistema de seguridad nacional que gestione los riesgos que amenazan su funcionamiento, lo que ha tenido su máximo exponente en la aprobación por parte del Gobierno de España de la Estrategia de Ciberseguridad Nacional de 2013, en la que se puede leer —y cito, literalmente—: «España está expuesta a los ciberataques, que no solo generan elevados costes económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en sus sistemas, que en la actualidad resultan críticos para el normal funcionamiento de la sociedad».

cve: DSCG-12-CM-111

La vigente Estrategia de Seguridad Nacional de 2017 nos habla en su artículo 4 de esas amenazas y nos define la ciberamenaza como una amenaza transversal facilitadora y potenciadora de toda esta actividad ilícita que ya hemos mencionado: terrorismos y conflictos de múltiples tipos, crimen organizado, espionaje o inestabilidad económica, entre otros. ¿Se esperan acciones de gran impacto? Sí, se esperan acciones de gran impacto. ¿Y de efectos impredecibles? Sí, de efectos impredecibles. ¿Podríamos decir que esperamos cisnes negros? Sí. Hace tiempo que los analistas ya hablan del Pearl Harbor digital. Normalmente, se habla de *blackout* y, asociado a este término aunque quizás en un aspecto menos dramático o tremendista que aquel, últimamente también de ciberhuracanes, pero en cualquier caso siempre de situaciones extremadamente complicadas. Se puede decir que cualquier organización puede ser víctima de una acción de este tipo y que en este momento no existen estructuras que puedan vivir ajenas a esta amenaza. En definitiva, vivimos en un estado de permanente incertidumbre.

La ya mencionada Estrategia de Seguridad Nacional también hace una especial mención a las amenazas híbridas, entendiendo como tales aquellas que combinan ataques tradicionales o convencionales con otros no tradicionales, y precisamente en estas amenazas híbridas es donde existe un mayor riesgo de enfrentamiento para los Estados democráticos, puesto que se están produciendo procesos de desinformación e infoxicación, mayoritariamente procedentes de potencias o países extranjeros, en los que los actores son tanto Estados como particulares, aunque, como digo, mayoritaria o preferentemente Estados, que como objetivo último persiguen la polarización y el enfrentamiento de parte de la sociedad. Otro concepto que está tomando mucha fuerza es el de la posverdad, a través del cual que se utilizan los nuevos desarrollos tecnológicos para distribuir informaciones que dan pie a procesos de engaño, decepción o manipulación.

Hablando ya de ciberseguridad, conceptualmente podríamos definirla como el esfuerzo coordinado de todos los actores públicos y privados que coadyuvan al libre ejercicio de los derechos y libertades en el ciberespacio, y entre sus prioridades está la protección de la privacidad, la integridad y el honor de las personas, la defensa de la propiedad privada y la defensa ante la desinformación, la propaganda y la manipulación informativa. El presente 2018 está resultando ser un año especialmente intenso en lo que respecta al marco normativo, toda vez que en el mes de mayo entró en vigor la trasposición de la Directiva de la Unión Europea del Reglamento General de Protección de Datos como norma esencial y marco de referencia para todos los Estados miembros en todo lo relativo a la protección de los datos de carácter personal, y hay que añadir que en septiembre de este mismo año se aprobó la trasposición de la Directiva NIS para homogeneizar la normativa sobre seguridad de redes y sistemas de información y comunicaciones en todos los países de la Unión Europea, otorgando un papel fundamental a los centros y equipos de respuesta antiincidentes de seguridad informática públicos y privados, aunque, evidentemente, siempre con la tutela de los órganos públicos. Hay que destacar el Centro Criptológico Nacional, con su CCN-CERT, y el INCIBE, con su CERT de seguridad industrial, pero también las estructuras de coordinación, que son fundamentales: el Departamento de Seguridad Nacional, el Centro Nacional de Protección de las Infraestructuras Críticas y la Oficina de Coordinación Cibernética, estos últimos dependientes del Ministerio del Interior.

En cuanto a las ciberamenazas, es obligado empezar hablando del ciberdelito, una nueva tipología delictiva que ha venido a trasladar la acción ilícita tradicional al ciberespacio y que está absolutamente incontrolada en el sentido de que la perspectiva del ámbito geográfico ilimitado dificulta mucho la acción penal, toda vez que tenemos que conjugar los derechos penales y procesales de los diferentes países. En el marco de la Unión Europea se supone que esta situación está más o menos controlada, pero fuera del marco de la Unión Europea existe un mecanismo muy potente, que es el Convenio de Budapest sobre cibercriminalidad, que, afortunadamente, ya tienen aprobado todos los países miembros de la Unión Europea y que, de facto, se ha convertido en un estándar internacional, toda vez que ochenta países ya se han adherido a él, si bien todavía quedan más de cien países que no reconocen ese marco normativo.

El ciberterrorismo es una amenaza que está ahí, es una amenaza latente, y la mayor preocupación que tenemos es que las acciones terroristas se trasladen a lo que viene a denominarse infraestructuras críticas y estratégicas. ¿Por qué? Porque pueden tener un grave impacto en la ciudadanía, ya que afectarían a servicios esenciales. De hecho, consideramos el ciberterrorismo como un riesgo emergente se puede decir que a día de hoy de baja probabilidad pero de alto impacto si se llegara a producir; y he enfatizado que a día de hoy porque actualmente sabemos dónde estamos, pero no sabemos dónde estaremos mañana. Por otra parte, cuando hablamos de ciberterrorismo y acciones contra infraestructuras críticas hay que pensar en acciones de falsa bandera, principalmente desarrolladas por Estados, Estados

cve: DSCG-12-CM-111

hostiles que buscan subvertir o desestabilizar a otros Estados y hacen creer que son acciones realizadas por grupos terroristas; y, si son de menor intensidad, son muy frecuentes las acciones de falsa bandera que se atribuyen a grupos *hacktivistas* como anónimos, si bien realmente detrás de ellas están organizaciones estatales. No debemos perder de vista que una de las motivaciones fundamentales de la mayoría de los ciberataques es económica, para atentar contra el potencial económico de los Estados, para debilitar a los Estados y con ello obtener una ventaja competitiva en un mercado globalizado como es el actual, pero, evidentemente, este tipo de ataques a los intereses económicos de un Estado a su vez pueden acarrear pérdida de soberanía nacional.

Esta es la breve introducción que quería hacer con respecto al estado del arte. A continuación voy a referirme a cómo estamos organizados y qué capacidades tenemos en el seno de la Guardia Civil. Me van a permitir que haga un breve informe, desplegado en el formato que se denomina DAFO, y voy a hablarles de debilidades, fortalezas y oportunidades.

En primer lugar, vamos a hablar de fortalezas —permítanme que saque pecho—, y la principal fortaleza del Cuerpo de la Guardia Civil es nuestra vocación de servicio inquebrantable al pueblo español, lo que nos hace ser muy perseverantes en cualquier misión o cometido que el Gobierno de la nación nos encomienda. Creo que todos ustedes son conscientes de que desde 1844 —el año que viene haremos los 175 años de historia— la Guardia Civil ha afrontado siempre retos extremos en lo relativo a seguridad pública, y la situación actual relativa a ciberseguridad se ha convertido en un reto extremo.

Una ventaja evidente es nuestro despliegue. Somos el cuerpo de seguridad del Estado con mayor implantación en todo el territorio nacional; luego, nuestra acción directa puede llegar, como digo, a todo el territorio nacional. Desde hace muchos años —les estoy hablando de finales de los años noventa y año 2000— hemos hecho grandes esfuerzos organizativos internos y por dotarnos de recursos para atender este tipo de amenazas, inicialmente el ciberdelito creando las unidades de ciberdelincuencia en el seno de la jefatura de la Policía Judicial y a partir del año 2000 creando estructuras de lucha contra el ciberterrorismo en el seno de la jefatura de Información. Como pueden ver en sus monitores, en esta dilatada experiencia el Grupo de Delitos Telemáticos se creó en el año 1996 y el Grupo de Ciberterrorismo se definió en el año 2000 e inició su actividad operativa en el año 2002, lo que nos convirtió en una unidad pionera no solo en España sino en Europa. De hecho, durante muchos años en el resto de Europa y Latinoamérica no entendían muy bien el modelo español, no entendían que diferenciáramos delincuencia y terrorismo en el ámbito ciber; y digo que no lo entendía porque ahora sí lo entienden, aunque todos —es una expresión que empleo mucho— estamos chapoteando en el mismo charco, que es el ciberespacio, pero estamos combatiendo amenazas muy dispares, e incluso las técnicas y los procedimientos no tienen nada que ver. No obstante, sobre este modelo puedo decirles que, aunque no es exclusivo de la Guardia Civil, porque también lo tiene el Cuerpo Nacional de la Policía Nacional, al final Europa nos ha dado la razón, toda vez que desde hace dos años en el seno de Europol se ha diferenciado la lucha contra el ciberdelito de la lucha contra el ciberterrorismo y ha creado estructuras diferenciadas. Eso no quiere que no seamos estructuras que nos complementemos y cooperemos; al contrario, estamos perfectamente articuladas para reforzar unos las capacidades de otros en un momento determinado.

Otra de las ventajas que tenemos es que nuestros sistemas de información e inteligencia están diseñados *ad hoc.* No utilizamos herramientas comerciales, sino que durante años nos hemos esforzado por dotarnos de herramientas tecnológicas adaptadas a las necesidades reales y a la forma de trabajar de nuestros analistas e investigadores. Durante estos años —les hablo ya de dieciséis, diecisiete años—, poco a poco hemos ido consolidando estructuras de cooperación multilateral y bilateral con terceros tanto a nivel nacional como, especialmente, internacional: intentar plantear la lucha contra las ciberamenazas desde una burbuja nacional es un absurdo, puesto que la amenaza es global, en toda su expresión. Desde hace años tenemos unos ambiciosos programas de formación en excelencia en el ámbito de la informática forense y la ciberseguridad, con el apoyo de centros universitarios. Por último, tenemos activados programas de detección, selección, formación y entrenamiento en todas las disciplinas vinculadas con la ciberseguridad dentro del Cuerpo de la Guardia Civil.

Nuestra obligación es mantener estas fortalezas. Pero, como todos, tenemos debilidades.

Por un lado, como a todos los sectores de la Administración pública y como a toda la sociedad española, la incertidumbre presupuestaria nos ha golpeado muy duro. ¿En que se ha traducido esto? Hemos ralentizado nuestro planes de expansión tecnológica, las previsiones de compra, de integración de herramientas de última tecnología y desarrollos *ad hoc*, como les dije antes. Lamentablemente, todo eso cuesta dinero, y cuesta mucho dinero; la informática y las telecomunicaciones no son precisamente

cve: DSCG-12-CM-111

baratas. Además, muchas veces el retorno de este tipo de inversiones no se ve muy claro cuando hablamos de seguridad, y, por tanto, tenemos problemas, aunque, lógicamente —insisto—, son los problemas que tiene cualquier unidad de la Guardia Civil, cualquier estructura de los cuerpos de seguridad del Estado, cualquier estructura en el Ministerio del Interior y cualquier estructura ministerial. Confiemos en que la situación siga mejorando y que podamos revertir este parón y seguir con nuestros planes de potenciación.

Por otra parte, incertidumbre en el sostenimiento de los recursos humanos. Por la misma razón, en cuanto a las incorporaciones a los cuerpos de seguridad, en este caso a la Guardia Civil, la nueva recluta de funcionarios ha sufrido un parón, un parón importante. Hemos pasado de años de tasa de reposición del 10 % a años de tasa de reposición cero, y eso, lo quieran o no, ha repercutido en que no hemos podido crecer al ritmo que nuestros superiores habían establecido en los planes estratégicos. En concreto, mi unidad lleva seis años de retraso, de acuerdo con los planes estratégicos aprobados por la Dirección General de la Guardia Civil, basado en la carencia de esos recursos humanos.

Un problema que es interno pero que les traslado, porque he venido a contarles todo, bondades y miserias, es el relativo a la incertidumbre en el modelo de carrera profesional, en el sentido de que nos resulta muy complicado articular la legítima ambición de promoción y ascenso con las estructuras de plantillas. Dentro del marco legal que nos permite la Ley de personal, estamos haciendo esfuerzos para encontrar una fórmula que nos haga un poco más flexibles los puestos de trabajo, porque a veces por un ascenso podemos perder un potencial humano muy importante, por una cuestión de disponibilidad o no disponibilidad de una silla.

Tenemos que seguir consolidando las estructuras supranacionales, es fundamental. Hay muchos grupos de trabajo, hay muchos organismos en los que nuestra presencia es ocasional, podríamos decir. Se convocan reuniones, encuentros, jornadas de estudio o intercambio y enviamos funcionarios a esos eventos, pero tenemos que seguir avanzando en este caso en la Guardia Civil, pero extiéndanlo a todas las estructuras nacionales, en que tengan una presencia permanente. Eso implica costes, porque hay que proyectar funcionarios a esas estructuras supranacionales, pero es fundamental la presencia permanente.

Aunque lo estamos llevando a cabo, estamos teniendo una lógica dificultad en la recluta de personal altamente cualificado. ¿Por qué? Porque el personal altamente cualificado decide dedicar su saber en otros ámbitos en los que —vamos a decirlo claro— las compensaciones o recompensas son muchísimo más gratificantes que las que puede obtener en la Administración pública. Este es un problema generalizado. La selección de talento dentro de las estructuras resulta realmente complicada, porque la mayoría del talento se encuentra fuera.

Finalmente, en cuanto a todas estas amenazas, nuestra tendencia es ir corrigiéndolas.

¿Cuáles son las amenazas? La fundamental es que siga creciendo la escalada de las ciberamenazas, los cisnes negros de los que les hablé antes. ¿Hacia dónde puede crecer? Nadie lo sabe. Piensen ustedes que hace pocos años no existían redes sociales, wasap, mensajería instantánea, y, sin embargo, ahora lo vemos como algo cotidiano. Por tanto, este mundo evoluciona a un ritmo frenético y, al mismo ritmo que cambia la sociedad y la tecnología, también evolucionan las amenazas. Debemos estar muy atentos a esta evolución de las amenazas, a esta evolución y a su diversificación, porque antes las amenazas estaban muy focalizadas en ciertos objetivos, como la ciberdelincuencia, pero actualmente, con la generalización de la amenaza, con la extorsión vía *ransomware* cualquier ciudadano puede ser objeto de extorsión en un momento determinado.

No debemos infravalorar los riesgos. Antes dije que, por ejemplo, el ciberterrorismo es una amenaza emergente de baja probabilidad. Pero lo que han de tener muy claro es que, si esa probabilidad se vuelve alta, el riesgo se vuelve crítico, y deberemos estar adaptados. Siguiendo la táctica militar, debemos trabajar sobre la base de la hipótesis más probable, que es nuestro trabajo del día a día, pero es nuestra obligación estar preparados para responder ante la hipótesis más peligrosa. Por tanto, no debemos subestimar los recursos humanos y materiales que necesitamos; y cuando hablo de recursos materiales y, sobre todo, humanos me refiero a que debemos articular mecanismos que nos permitan acceder a esos recursos aunque no formen parte del cuerpo de las administraciones públicas.

Sé que en esta Comisión se ha estado debatiendo sobre el concepto de ciberreserva —si les parece oportuno, luego podríamos profundizar en ello—, y nosotros consideramos que es una iniciativa muy, muy interesante, que precisamente puede venir a paliar muchas de las carencias que les estoy diciendo que tenemos en este momento. Por tanto, las amenazas tenemos que afrontarlas.

cve: DSCG-12-CM-111

Por último, oportunidades. ¿Qué oportunidades tenemos? La coordinación. Afortunadamente, en los últimos años se ha hecho un esfuerzo grandísimo en la coordinación. Los primeros años, cada organización, cada estructura, nosotros mismos íbamos por libre. De hecho, hace dieciséis años los primeros que hablamos de protección de activos de ciberataques fue la Guardia Civil, ya que entonces no existían todavía el Centro Criptológico Nacional ni el Centro Nacional para la Protección de Infraestructuras Críticas. Nos miraban raro y decían: A los guardias civiles se les está yendo la cabeza. ¿Qué están hablando de ciberamenazas? El tiempo nos ha dado la razón. Como les digo, ya hemos sido rebasados, tanto en el Ministerio del Interior como en el de Defensa y en el de Presidencia, por estructuras supranacionales como el F3 de Europol, por la parte de Europol de ciberterrorismo, el comité contra el terrorismo de la Organización de Estados Americanos o la Oficina contra el Crimen y la Droga de la Organización de Naciones Unidas, con los que trabajamos estrechamente.

Es fundamental la especialización. Como he dicho antes, estamos haciendo grandes esfuerzos en formación de excelencia, pero siguen siendo insuficientes. Tenemos que seguir formándonos en cantidad y en calidad. Necesitamos personal cada vez más cualificado, pero también mayor número de personas para atender estas amenazas. Debemos seleccionar y priorizar las amenazas, y para eso están los órganos de coordinación, porque muchas veces los árboles nos impiden ver el bosque: damos cierta importancia a eventos que no la tienen y pasan desapercibidos otros realmente críticos. En este sentido, es muy interesante una iniciativa promovida por el Centro Criptológico Nacional, que es la estructura de la red CSIRT.es, en la que convergemos los cuerpos de seguridad, las estructuras de apoyo tecnológico, los centros de respuesta antiincidentes y —lo que es más importante— los operadores de las infraestructuras y compartimos impresiones, experiencias y pálpitos. Eso nos ayuda a detectar —entendemos que de forma proactiva— posibles amenazas que podrían complicarse si no son debidamente atendidas.

Por último, trabajo en equipo. La Guardia Civil no puede afrontar sola esta realidad. Los cuerpos de seguridad del Estado —haciendo partícipes también a los compañeros de la Policía Nacional— no podemos hacer frente solos a esta situación, ni con las estructuras de los compañeros del Ministerio de Defensa, del Mando Conjunto de Ciberdefensa, sino que necesitamos la confluencia de todos, es decir —lo habrán escuchado muchas veces—, la cooperación público-privada. Esto es fundamental. Más del 80 % de las infraestructuras críticas y estratégicas están operadas por el sector privado. Tenemos que generar unas sinergias positivas precisamente entre las administraciones y el sector privado. Además, hay que trasladar esa sensación de seguridad a la ciudadanía, que no se sienta desangelada y diga: ¿Qué viene por aquí, el Armagedon? Descarguemos ese dramatismo, pero tomémonoslo en serio. A ustedes, que son los legisladores, les pido que tomen nota de lo que humildemente les está contando este coronel, de lo que otros comparecientes les habrán contado y que insten al Ejecutivo a adoptar las acciones, las modificaciones legislativas, etcétera, tendentes a mejorar la seguridad, porque de ello depende el bienestar y el futuro de la sociedad española.

Gracias.

El señor **VICEPRESIDENTE:** Don Luis, gracias por su interesante exposición.

Damos ahora un turno de intervención a los distintos grupos por un tiempo aproximado de cinco minutos, empezando de menor a mayor, y después contestará el compareciente de manera conjunta.

Por el Grupo Mixto, tiene la palabra el señor Yanguas.

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

Buenos días coronel. Quiero disculparme por no haber podido llegar al principio de su comparecencia, pero es que me lo ha impedido un incidente de tráfico. Le diré que como en el Grupo Mixto, Unión del Pueblo Navarro, estoy yo solo y todavía no tengo el don la ubicuidad, tengo que atender en el Senado a otras comisiones, por lo que deberé que ausentarme.

Vuelvo a agradecerle su intervención, que repito que no he podido escuchar en su integridad, aunque luego podré estudiarla más detenidamente en el *Diario de Sesiones*. También quiero agradecer el trabajo diario de los miembros de la Guardia Civil y el suyo propio.

Nada más. Gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Yanguas.

Por el Grupo Vasco, tiene la palabra el señor Legarda.

cve: DSCG-12-CM-111

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

Quiero dar las gracias al señor Hernández, coronel del área técnica de la Jefatura de Información de la Guardia Civil, por su interesante y didáctica exposición. Me gustaría, porque supongo que el resto de los portavoces profundizarán en otras cuestiones, que nos desarrollase un poco más la cuestión de la coordinación, concretamente qué nivel de coordinación existe en estos momentos entre los diferentes cuerpos de seguridad, tanto del Estado como de las dos policías integrales autonómicas —yo provengo del País Vasco—, de Cataluña y del País Vasco. ¿Qué debilidades y qué fortalezas encuentra? Ha hablado de la coordinación, pero, digamos, tomando como eje a la Guardia Civil, es decir, ha hablado de la colaboración internacional y con otros entes —entre comillas— civiles de la Administración General del Estado, aparte del Ministerio de Defensa. Yo quiero centrarme más en las Fuerzas y Cuerpos de Seguridad del Estado en cuanto a debilidades, fortalezas y amenazas.

Muchas gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Legarda.

Por el Grupo de Esquerra Republicana, tiene la palabra el señor Castellana.

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

Señor Hernández, quería formularle tres preguntas o abordar tres temas. Las ciberamenazas se basan en lo que se llaman las debilidades del *software*, ya sean del propio *software* o del diseño. En ese sentido, los estándares abiertos trabajados por la comunidad, muchas veces con apoyo académico, suelen ser menos vulnerables que otros *softwares* desemblocados por entornos corporativos privados observados por menos ojos, que muchas veces tienen presiones económicas o de tiempo de entrega. Trabajar con estándares abiertos en el gran charco, como ha llamado a Internet, solucionaría muchos problemas de seguridad. Las dos únicas contrapartidas que veríamos a este punto —que para nosotros no son contrapartidas, pero para algunos sí— serían los beneficios de determinadas corporaciones o el hecho de que los Estados —los Estados occidentales no dejan de ser parte de estos Estados— pactan con corporaciones las puertas traseras para hacer cibervigilancia a sus ciudadanos. Me gustaría conocer su opinión sobre si legislativamente se tendrían que impulsar criterios más abiertos de calidad y de transparencia del *software* y del diseño de plataformas.

Usted ha diferenciado entre ciberdelitos y ciberterrorismo. En el mundo ciber hacen falta capacidades. Las capacidades solamente las pueden proveer los Estados con actividades de falsa bandera, como usted muy bien ha dicho, o grupos delictivos con ánimo de lucro. Por tanto, al final, a mi entender, el ciberterrorismo queda vinculado a guerra a escondidas por parte de otros Estados o a ciberdelitos, al crimen organizado también en el cibermundo. Me gustaría que explicase un poco más qué criterios utilizan para separar ciberdelincuencia y ciberterrorismo, entendiendo que en el ciberterrorismo puede incluirse el hecho de la propaganda. Las capacidades no caen del cielo y el mito romántico del *hacker* solitario no existe.

Usted ha hablado de la disponibilidad de recursos humanos y materiales, que entiendo que debe ser un problema en un mundo en expansión y en constante cambio. Desconozco a fondo su trabajo contra el cibercrimen más allá de lo expuesto, las tareas diarias, pero lo que nos llega a los ciudadanos es que dedican parte de su tiempo a investigar delitos de opinión. Quizá no sea su negociado y sea otro de la Guardia Civil, y si es así, le pido disculpas, pero me interesaría saber cuántos recursos se dedican a investigar delitos de opinión que al final en instancias judiciales de otros países son tumbados, porque estos recursos podrían dedicarse a combatir la ciberdelincuencia.

Muchas gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Castellana.

Por el Grupo Parlamentario Ciudadanos, tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Muchas gracias, señor presidente.

Estimado coronel Hernández, en primer lugar, no solo quiero agradecerle su comparecencia ante esta Comisión, sino también la valentía con la que lo ha hecho. Cuando ha comenzado con la introducción me ha extrañado que fuera sobre lo que representa y lo que es Internet, pero cuando ha entrado en materia, concretamente en la Guardia Civil, he visto la valentía que ha tenido a la hora de destacar cosas que tenemos que corregir, porque si no, dentro de no mucho tiempo pueden ser un problema que nos haga arrepentirnos.

cve: DSCG-12-CM-111

En su exposición ha resaltado algo que es correcto, que es el carácter pionero de la Guardia Civil en afrontar este tipo de retos, pero quiero hacer una pequeña reflexión en la que, en cierta medida, también hago la pregunta. La Guardia Civil ha sido pionera porque ha tenido la inquietud de entrar en este ámbito y empezar a investigar y a mejorar sus sistemas de prevención, de protección y de actuación, pero esto ha sucedido de manera dispar en distintos ámbitos. Ha hablado de la Estrategia de Ciberseguridad Nacional y de los planes, y mi pregunta es si considera que podemos entender, por el desarrollo que han ido teniendo las Fuerzas y Cuerpos de Seguridad del Estado, cada uno por su lado, el ejército por un lado, lo público, las administraciones por otro, y por otro la parte privada, que en este momento tenemos un plan de seguridad nacional de Estado o si, como defendemos en mi grupo, debiéramos intentar cerrar un gran pacto de Estado precisamente para hacer ese plan de seguridad nacional de Estado que incluyera dos de los temas que usted ha dicho que le preocupan dentro de la Guardia Civil, pero que a nosotros nos preocupan dentro de la Guardia Civil, en general en las Fuerzas y Cuerpos de Seguridad del Estado, y dentro de la ciberseguridad, que son la falta de recursos humanos y presupuestarios.

Creemos que todavía nos falta mucho por recorrer en el sentido de crear una cultura de la ciberseguridad. Me gustaría que nos diera su opinión sobre si cree que en las escuelas, en las pymes se debería enseñar hacia dónde vamos. A los niños se les habla de seguridad vial para que sepan el mundo que se van a encontrar cuando sean mayores y cómo tienen que actuar, y yo creo que la seguridad vial de los niños en Internet es la ciberseguridad para que sepan cómo se pueden proteger, qué precauciones tienen que tener e incluso cómo pueden contribuir a detectar amenazas o a colaborar después para frenarlas.

También le quiero preguntar por la formación. ¿Cómo entiende usted que habría que encauzar el tema de la formación? Hablamos mucho de que no hay profesionales, de que tiene paro cero, de que se pagan altos salarios, pero ustedes lo hacen internamente, cada uno lo hace por su lado, incluso hacen cursos para el exterior en distintos ámbitos. ¿Cómo cree que deberíamos acometer, de manera integral, como país la formación de profesionales?

En relación con su aportación, me voy a ir a la parte final. Ha hablado de algo que estamos poniendo de manifiesto permanentemente, que es el tema de la guerra híbrida y del hecho de que todavía no haya habido ninguna convención en Naciones Unidas que haya afrontado esto para marcar unos criterios éticos de comportamiento y para que los Estados que realizan actuaciones que no son adecuadas sean sancionados, porque de otra manera sería como si se estuviera en un videojuego: Jugamos entre Estados y si consigo hacer lo que quiero puedo conseguir una gran operación de espionaje industrial, armamentístico o de cualquier materia, incluso puedo bloquear o incidir en la economía de otro país, pero no pasa nada porque estamos divirtiéndonos.

Ha hablado de la desinformación. Mientras más mejora y más progreso en la capacidad de comunicación del conjunto de la sociedad mayor riesgo de desinformación. Cuanta mayor facilidad para que cada uno coloque su valla publicitaria en las redes sociales, que tenga material para construir información medianamente veraz y pueda hacer que esa información se pueda compartir y extender a mucha gente, más fácil será manipular la opinión pública. Es cierto que cuando ustedes y nosotros hablamos de esto no nos referimos a los comentarios de cotilleo, sino a informaciones tendentes a conseguir un resultado que pueda hacer que hoy el *brexit* sea de una u otra manera o que una democracia tenga un resultado electoral u otro. Nosotros jamás vamos a criminalizar su trabajo en esta materia. Entendemos que cuando ustedes actúan es porque creen que deben hacerlo y no lo hacen con ninguna tendencia, sino con ánimo de prevención y de protección del conjunto de la sociedad, lo que implica a todos los que vivimos en este país, incluidos todos los grupos parlamentarios que hoy estamos aquí.

Para terminar, quiero hacerle una pregunta sobre algo de lo que no hablamos nunca, porque *a priori* no tiene que ver con la ciberseguridad, pero que en el futuro puede terminar teniendo mucho que ver, que es el control de los macrodatos. En este momento, todos tenemos nuestros datos y nuestra vida puestos en Internet, por lo que somos vulnerables, podemos ser objeto de ataques, incluso de presiones y de extorsiones. Estamos poniendo todos nuestros datos no en las Fuerzas y Cuerpos de Seguridad del Estado que son las que tienen que protegernos, sino en manos de empresas privadas, de multinacionales que controlan esa información y que con los algoritmos determinados pueden conocernos. A partir de ahí, si estamos hablando de que se puede manipular, desinformar y conseguir estados de ánimo y de opinión pública, imaginemos lo que se puede conseguir con ese control de los macrodatos. Quisiera preguntarle, con la inquietud que les mueve, con las líneas de trabajo que van aventurando para el futuro, en los congresos y en los ámbitos en los que comparten información, si cree que los Estados tienen que empezar

cve: DSCG-12-CM-111

a tener algún tipo de control de esos macrodatos y a realizar actuaciones, independientemente de las leyes de protección de datos, etcétera, para garantizar que en el futuro no seamos manipulados por una gran multinacional de control de macrodatos.

Muchas gracias.

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

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

El señor **ALONSO CANTORNÉ:** Muchas gracias, señor presidente.

Señor Hernández, bienvenido. Quiero agradecerle su exposición. Antes de nada, quiero presentarme, porque nosotros conocemos algunas cosas de usted, pero posiblemente usted no nos conoce a nosotros. Soy del Grupo Confederal, de En Comú Podem; por tanto, soy catalán y soy ateo, pero en el tema del *procés* siempre he sido agnóstico.

Supongo que es consciente de que de aquí a pocos días se celebrará el aniversario de la república de los ocho segundos. Hay una serie de cosas que me gustaría conocer, pero antes, si me lo permite, haré una pequeña introducción. Más de dos millones de personas en Cataluña creyeron a unos dirigentes que les prometían una independencia exprés y mágica, como bien denunció el diputado de las 155 monedas. La oferta era muy golosa. ¿Quién no estaría dispuesto a tener un país nuevo, a construir un país nuevo, sin corrupción, sin paro, con mejores pensiones, etcétera? Solamente los agnósticos como yo. El 1 de octubre fue uno de los días históricos del *procés*. La nula visión política del presidente Rajoy y de la vicepresidenta Sáenz de Santamaría, entre otros, convirtieron una extraordinaria manifestación en una fotografía que ha desprestigiado a la democracia española en el mundo y que dio combustible al independentismo. Antes, los días 6 y 7 de septiembre, en el Parlament se vulneró l'Estatut y la Constitución. Después, el 1 de octubre se desarrollaron los acontecimientos de los que todos somos conocedores. Resultado: 155, elecciones, continúa la división del país y un nuevo Gobierno dispuesto a negociar con la Generalitat, que, por cierto, vive su particular Dragon Khan, puesto que un día amenaza y al día siguiente pide diálogo.

Un año después —y ahora entro en materia— existen diferentes visiones de lo que pasó durante aquellas jornadas. Personalmente opino que aquello que pasó, y que pasa, fue una crisis constitucional que debería resolverse con tiempo y acuerdos, lógicamente si existe voluntad por parte de la Generalitat de Catalunya. Otros, como la consellera Ponsatí, consideraron que aquello era una partida de póker y que iban de farol. Por último, están los que ahora no gobiernan, que una y otra vez repitieron y repiten que aquello fue un golpe de Estado, que nuestro grupo siempre ha pensado que es una exageración y que lo único que busca son réditos electorales y alimenta la mística del independentismo mágico.

No le preguntaré por su opinión, que me imagino que no me la puede dar y para el caso tampoco es relevante, pero sí me parece fundamental saber si desde los cuerpos de seguridad del Estado, en concreto desde su área de gestión, se consideró, como usted ha dicho antes, como hipótesis probable o más peligrosa el golpe de Estado. En el caso de que se llegara a considerar, ¿tomaron medidas para evitarlo? ¿Cuáles fueron? El 1 de octubre en algunos de los locales de la Generalitat que se dejaron para la votación se cortó Internet. ¿Fueron ustedes los responsables? Leyendo algunos de sus artículos, nos recuerda que fue Estonia, país digital por excelencia, la primera víctima de un ciberataque a gran escala vía Internet dirigido contra sus estructuras TIC. Durante dos semanas, de abril a mayo —como usted sabe perfectamente— de 2007, *hackers* supuestamente rusos llegaron a provocar la autodesconexión del país báltico a Internet. El Gobierno estonio salió airoso y hoy en Estonia ha vuelto la armonía. Estonia es una referencia en materia de ciberseguridad; es cierto, ¿no? Gracias a aquel misterioso ciberataque solo un año después, en 2008, se inauguró en Tallin el Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN.

Vuelvo a las preguntas anteriores. Usted conocía la colaboración de un aliado de la OTAN con el Gobierno de la Generalitat y la inspiración que de Estonia llegaba a Cataluña para trabajar por una Administración digital más eficiente; también que en el Govern de Catalunya se implantó la tecnología blockchain. ¿Qué es blockchain? Básicamente la separación de la información en cadenas de bloques. Gracias a esa tecnología un Gobierno podría llegar a protegerse incluso de injerencias externas escondiéndose del flujo de información visible en el ciberespacio. Su seguridad, usted lo sabe, es máxima. ¿Cree que esa tecnología fue usada por el Gobierno de la Generalitat para ocultar sus intenciones?

cve: DSCG-12-CM-111

Sobre el resultado no le pregunto, porque todos lo conocemos. Si España es un socio fiable en la defensa de los derechos humanos, la legalidad internacional y el multilateralismo y las amenazas globales requieren respuestas integrales coordinadas y cooperativas, si el Gobierno del Partido Popular y sus socios de Ciudadanos hablaban de un golpe de Estado a la democracia, ¿cómo es posible que Estonia, aliado y sede del Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN, no alertara a España de lo que ocurría?

Usted habla de la cooperación necesaria entre los cuerpos de seguridad. Naturalmente, es imprescindible. ¿Existía colaboración entre el área técnica de la jefatura de información de la Guardia Civil y la UCRO, la Unidad Central de Recursos Operativos de la Generalitat de Catalunya? ¿Existe colaboración en estos momentos? ¿Considera necesario revisar los protocolos entre países aliados, las comunidades autónomas y el Estado para mejorar la coordinación y evitar situaciones como la acontecida?

Cambio radicalmente de tema. Entiendo que usted no puede informar de las cosas que están en manos de los jueces, pero le pondré un ejemplo al que seguro que nos puede dar respuesta. Si usted y yo formamos un tándem, nos unimos y creamos un fondo de armario de veinticinco años de grabaciones a personajes públicos en conversaciones privadas y luego lo vamos filtrando a la prensa, filtraciones que pueden llegar a afectar a la seguridad del Estado, ¿cree que estamos hablando de delincuencia común? Si esa misma información traspasa el puro chantaje a las personas implicadas y se vuelve viral en las redes, ¿en esa acción deliberada de desestabilizar un país estaríamos hablando de desinformación, de transparencia, de ciberdelincuencia o de ciberterrorismo? ¿Existe la posibilidad de que los Estados puedan ser chantajeados por mafias organizadas que supuestamente trabajan para defender al Estado? Vulgarmente a eso se le denomina cloacas que, como todos sabemos, son el ecosistema de las ratas. ¿Cómo evitar que las cloacas rezumen suciedad y que las ratas se apoderen de ellas? ¿Existe algún gato capaz de evitar que se vuelva a dar una situación de filtración de conversaciones como la descrita?

Estas son las preguntas. Muchas gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Alonso.

Por el Grupo Parlamentario Socialista, tiene la palabra el señor Hernando.

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

Coronel, gracias por su presencia y por la exposición que ha hecho. Como usted verá, esta es una Comisión diversa, plural en la que cada miembro puede decir y exponer lo que considere oportuno. Usted es un servidor público y no le voy a recordar, porque no es mi función, cuáles son sus derechos y obligaciones a la hora de contestar a las preguntas y a las intervenciones —he visto que el letrado estaba tirando de Reglamento—, pero usted sabe perfectamente cuáles son. Me da la impresión, lo digo sinceramente, respetando la absoluta libertad de cada grupo de decir lo que estime conveniente y donde lo estima conveniente, de que hay intervenciones que no van dirigidas a usted. También me da la impresión de que cuando algunos ven un uniforme de la Guardia Civil reaccionan de determinada manera. La reacción que a mí me suelen producir los uniformes de la Guardia Civil es de respeto, consideración y agradecimiento hacia el cuerpo que usted representa. Lo digo con absoluto respeto a todas las intervenciones y a lo que aquí se pueda exponer.

Entro en el tema del que nos habíamos ido. En primer lugar, quiero agradecerle su sinceridad. Lo que nosotros demandamos básicamente a los comparecientes es sinceridad, porque eso nos resulta muy útil para acometer el informe con el que tenemos que concluir esta Comisión, que está basado en consideraciones y recomendaciones al Ejecutivo, como usted ha dicho. Por tanto, sinceridad, que es muy loable en este caso, porque usted ha puesto los puntos sobre las íes en cuanto a las debilidades. Las fortalezas nos las podíamos imaginar, y está bien resaltarlas, pero fundamentalmente nos interesan las debilidades en materia presupuestaria, en materia de personal, en materia de especialización, incluso respecto al futuro de su carrera profesional. Prácticamente todos los representantes de la Administración y de los distintos institutos y organismos que se dedican a la ciberseguridad coinciden —si las ha leído, que imagino que sí— en la necesidad de que haya mayor presupuesto, mayor dotación de personal y mayor especialización. Repito que le agradezco su intervención y su sinceridad.

Me gustaría que en su segunda intervención se centrase en tres de los aspectos que ha mencionado a lo largo de la intervención, que son el ciberterrorismo, el ciberhacktivismo y la intervención de terceros Estados, ya sea a través de acciones de bandera falsa o de otro tipo. Ciberterrorismo. Usted pertenece a la jefatura de información que, como ha dicho, entre los años 2000 y 2002 creó la primera unidad de ciberterrorismo. Haré preguntas muy concretas, más allá de que no pueda profundizar en el escaso

cve: DSCG-12-CM-111

tiempo que va a tener para responder. Usted dice que en estos momentos es una amenaza con pocas probabilidades de triunfar. Es una evidencia que los terroristas han utilizado la red para determinadas acciones de información, propaganda y captación, no hace falta demostrarlo. La cuestión es si considera que determinados grupos terroristas —estamos hablando fundamentalmente del yihadismo radical— han podido tener ya acceso, no a la tecnología, sino a los conocimientos especializados, muy especializados, que pueden dar lugar a que la red sea utilizada no como medio, sino como fin en sí mismo, es decir, atentar contra esas infraestructuras críticas a través de la red; si eso es una posibilidad o no teniendo en cuenta además la asimetría de estas acciones, ya que son acciones muy baratas en relación con el terrorismo tradicional o que conocemos habitualmente, me refiero a la compra de bombas o de otro tipo de tecnología. Por lo tanto, ustedes tienen una unidad desde el año 2000 o 2002 especializada en esto, tienen mucha experiencia en combatir el terrorismo, ya sea el más conocido por España, el terrorismo de ETA, o el de otras organizaciones terroristas, pero también el terrorismo yihadista. Entonces, ¿qué información tiene o qué probabilidades hay respecto a este tema? Por otro lado, dentro del *ciberhacktivismo,* cuáles considera usted que son las mayores amenazas, si son las amenazas de negación de servicio —en mi modesta y humilde opinión, lo más típico—, la destrucción de datos, el robo de datos, y cuál es nuestra preparación como país y, en concreto, la que desarrolla la Guardia Civil.

Por último, la actuación de terceros países. En este tema no sé por qué voy a decir nada, yo tenía que estar escaldado porque recibí muchas críticas cuando me referí a este tema hace ocho o nueve meses. Sin embargo, estaríamos en una auténtica burbuja en esta Comisión si no nos hiciésemos eco de lo que hemos conocido y de las denuncias que se han producido hace escasamente una semana por parte del Gobierno del Reino Unido, del Gobierno holandés, del Gobierno australiano y del Gobierno de Canadá. No me voy a referir al británico porque algunos pueden considerar que es demasiado próximo al eje atlántico, pero sí me referiré al holandés o al canadiense que han denunciado la actuación de servicios de inteligencia de determinado país, Rusia, con activismo y acciones hostiles en la red; en concreto, respecto a la Organización para la Prohibición de las Armas Químicas con sede en La Haya o la Agencia Mundial Antidopaje con sede en Montreal. Estos Gobiernos han manifestado que la coordinación entre ellos y sus distintas agencias de inteligencia ha dado lugar a poder detectar estas agresiones hostiles por parte de la GRU rusa. ¿Ha tenido España alguna participación? ¿Han conocido estos hechos? ¿Hemos tenido alguna vulnerabilidad respecto a esto que le acabo de contar que sí ha ocurrido en otros países? Me refiero simplemente a estos temas, no a *fake news* ni a nada por el estilo, no a campañas electorales. Lo que está claro es que el Gobierno de Canadá ha detectado una intromisión en la Agencia Mundial Antidopaje y el Gobierno de Holanda la ha detectado en la Organización para la Prohibición de las Armas Químicas. Me parece importante que en una Comisión del Congreso de los Diputados donde estamos tratando los temas de ciberseguridad sepamos si en España hemos tenido algún conocimiento, si hemos colaborado o participado, o si ha habido alguna amenaza en relación con esto que sí ha sido una amenaza y una acción concreta para países como los que he mencionado.

Muchas gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Hernando.

Para finalizar, por el Grupo Parlamentario Popular, tiene la palabra el señor Ramírez.

El señor **RAMÍREZ RODRÍGUEZ:** Con la venia, señor presidente.

Muchas gracias, coronel Hernández García, por su intervención, por el altísimo nivel de conocimiento que nos ha mostrado y, por supuesto, también le felicito por la talla que da la Guardia Civil en un asunto como este. Nos ha dicho usted que ya en el año 1996 la Guardia Civil empezó a trabajar en lo que era el ciberdelito, y desde luego nos parecen años muy pretéritos para lo que es la ciberseguridad y para el desconocimiento profundo que todavía existe en la sociedad española sobre esta materia. También ha comentado que se esperan acciones de gran impacto y efectos impredecibles. Nos ha hablado de ciberhuracanes y básicamente de incertidumbre. Todo esto, a pesar de que ya hay mucho trabajo hecho y mucho especialista, aún es un mundo nuevo y desconocido y no deja de sorprendernos todo lo que nos cuenta. La muestra es que en esta Comisión Mixta de Seguridad Nacional, como usted ha visto, a algunos les va poco todo lo relacionado con ciberseguridad y siguen yéndose a temas muy localizados, concretos, que bien podrían ser tratados en otra Comisión y que, por mucho que se salpiquen con la palabra ciberseguridad, nada tienen que ver con el objeto de su presencia aquí. Yo creo que en las Cortes Generales —parafraseando sus palabras— llevamos a cabo acciones para las hipótesis más probables, pero la creación de esta Comisión de Seguridad Nacional o la propia promulgación de la Ley de Seguridad

cve: DSCG-12-CM-111

Nacional nos dan a entender que también estamos preparados para las hipótesis más peligrosas. Creo que la ciberseguridad debe ser objeto de nuestra atención de una manera prioritaria y, en la medida de lo posible, tenemos que intentar saber más cada día del impacto que tiene sobre nuestra vida, sobre nuestra economía, sobre la protección de datos, en fin, sobre todas esas incertidumbres a las que usted se ha referido.

Coronel Hernández García, en el Grupo Parlamentario Popular hemos preparado unas preguntas que paso a formularle. En primer lugar, ¿podría darme la razón de las acciones tomadas por la Guardia Civil en materia de formación de talento orientado a la investigación forense y lucha contra el cibercrimen? ¿Considera que la actual estructura orgánica de la Guardia Civil permite afrontar adecuadamente las acciones tanto de inteligencia como de investigación judicializada en esta materia? ¿Cree que la Guardia Civil dispone de suficientes recursos tanto económicos como de talento para abordar las tareas que se le han encomendado en materia de lucha contra el cibercrimen? ¿Considera adecuados los sistemas de reclutamiento, captación, formación y de carrera profesional actuales para poder asegurar las capacidades necesarias de respuesta en la lucha contra el cibercrimen? Efectivamente, en esta Comisión hemos preguntado recurrentemente por lo que se conoce en los medios como la ciberreserva, a la que usted se ha referido. Como bien sabe, se trata de una herramienta orientada hacia la ciberdefensa de la nación, pero ¿consideraría acertada la adopción de un modelo UME para que, en caso de grave crisis en materia de seguridad interior, parte de los recursos disponibles a través de esta ciberreserva fuesen puestos a disposición del Ministerio del Interior? ¿Cómo evaluaría los riesgos para la seguridad interior de España de las acciones de desinformación orientadas a socavar nuestro Estado de derecho por parte de actores de cualquier tipo? ¿Considera adecuados los medios disponibles para la detección de este tipo de acciones por parte de las Fuerzas y Cuerpos de Seguridad del Estado? ¿Qué planes de acción propondría tanto para la detección como para la mitigación de las amenazas detectadas en esta materia? ¿Qué opinión podría ofrecernos sobre posibles acciones de inteligencia económica ejecutadas contra nuestro tejido productivo, fundamentalmente las pymes que, como todos sabemos, generan la mayor parte de los puestos de trabajo en nuestro país? ¿Podría glosarnos alguna acción de índole legislativa que pretendiese mejorar la efectividad de las Fuerzas y Cuerpos de Seguridad del Estado para una mayor protección más allá de toparse con ello o de la mera detección? Por último, coronel Hernández García, ¿considera que los actuales modelos de carrera profesional, así como los sistemas de retribución y recompensa —también se ha referido brevemente a ello— son adecuados para retener al mejor talento dentro de las filas de la Guardia Civil? ¿Tendría usted alguna propuesta que hacernos en este sentido?

Muchas gracias.

El señor **VICEPRESIDENTE:** Finalizado el turno de intervenciones, vamos a dar nuevamente la palabra al señor compareciente, el coronel don Luis Fernando Hernández, para que en aquello que pueda contestar dé respuesta a las distintas preguntas que se le han formulado. Tiene usted la palabra.

El señor **HERNÁNDEZ GARCÍA** (coronel del área técnica de la Jefatura de Información de la Guardia Civil): Gracias, señor presidente.

Yo esperaba que me hicieran más o menos las mismas preguntas, pero la verdad es que han sido muy dispares, con lo cual no sé de qué tiempo disponen ustedes, pero contestar a todo esto va a llevar su tiempo.

Bien, empezando por orden, el señor Legarda, del Grupo Parlamentario Vasco, se interesaba por los mecanismos de coordinación, y entiendo que su pregunta iba enfocada a la coordinación en este caso con la Policía autonómica del País Vasco, con la Ertzaintza. Bien, afortunadamente existen esos mecanismos de coordinación. Hay dos niveles de coordinación: a nivel técnico y a nivel operativo. La coordinación a nivel operativo se desarrolla en la Secretaría de Estado de Seguridad a través del Citco, en el que la Policía autónoma vasca se integró ya hace años. También, afortunadamente —aprovecho y contesto—, la Policía autónoma catalana se ha integrado recientemente. Es bueno que estemos todos allí porque es la forma de poder trabajar en equipo. En cuanto a la coordinación técnica, en la estructura de seguridad nacional los tres centros de respuesta públicos tienen cada uno un cometido muy claro. Empiezo hablando del Mando de Ciberdefensa que tiene como finalidad proteger las redes militares y ciertos servicios esenciales que por ley así se determinan. Luego está el CERT de Seguridad e Industria, dependiente del Incibe y del Ministerio de Industria, que se responsabiliza precisamente de apoyar a los cuerpos de seguridad en la seguridad hacia terceros, en este caso priorizadas las infraestructuras críticas, pero sin olvidar —además fue su origen— a las pequeñas y medianas empresas y a los ciudadanos. Y he dejado

cve: DSCG-12-CM-111

para el final el Centro Criptológico Nacional que, como saben, depende del Centro Nacional de Inteligencia y que en este momento ha retornado al Ministerio de Defensa. En la anterior legislatura estuvo en el Ministerio de la Presidencia, en qué ministerio esté es lo de menos. El hecho objetivo es que ese centro de coordinación nacional, el CCN, es el que tiene la responsabilidad de interactuar con ciertos CERT que hay a nivel autonómico. En concreto, en España tenemos los CERT autonómicos en Cataluña, en la Comunidad Valenciana, en Andalucía y, recientemente, ha empezado a andar el del País Vasco. Entonces, todos esos centros, podríamos decir de ámbito autonómico, están coordinados y entran dentro de la red nacional de coordinación a través del Centro Criptológico Nacional. Me preguntaba también por debilidades y fortalezas en el tema de la coordinación. Pues bien, le digo que la respuesta es la misma tanto para combatir las debilidades como para reforzar las fortalezas, se llama voluntad; hay que tener voluntad de querer coordinarse que, muchas veces, lamentablemente en esta querida España es lo que nos falta, la voluntad de coordinarse.

El señor Castellana, de Esquerra Republicana, me preguntaba por los estándares de código abierto. Y yo, que llevo veintiún años en el mundo informático, le puedo decir que los estándares de código abierto son un arma de doble filo porque, efectivamente, puede parecer que se libera uno de las siempre comentadas puertas traseras de los *software* comerciales, pero en realidad donde más puertas traseras se detectan es en el *software* libre. ¿Por qué? Pues porque hay múltiples actores o lo que se llaman comunidades interactuando y, lamentablemente, no todas lo hacen con un ánimo digamos altruista. De hecho, le puedo decir que en este momento la mayoría de las vulnerabilidades se están desarrollando en el ámbito de la telefonía móvil. El sistema operativo más extendido —no voy a decir el nombre, aunque lo pueden entender—, que es casi el 90 % del parque de teléfonos móviles tipo smartphone que hay en el planeta, utiliza una tecnología de *software* libre. Como consecuencia de ello, la mayor penetración de *malware* embebido en aplicaciones, que incluso se distribuye y se puede adquirir en las plataformas de descarga de APP, es precisamente esa plataforma de *software* libre, es la que más *malware* alberga y la que más fácil tiene la intromisión, porque los controles que se hacen cuando una aplicación se difunde son controles técnicos, son controles de compatibilidad básicamente, pero no entran en profundizar en el código fuente. Entonces, yo personalmente utilizo *software* libre, pero reconozco que tiene sus riesgos.

Luego me preguntaba usted por el ciberterrorismo, que no existe, aunque puede haber otro tipo de acepciones. Igual me he expresado mal, sí existe, lo que pasa es que está en un estado incipiente. Esto puede ir hilado con una pregunta, más que pregunta ha sido una reflexión, del señor Ramírez, del Grupo Parlamentario Popular, sobre el nivel de incertidumbre, etcétera. ¿Ha habido acciones de ciberterrorismo? Sí. ¿Han sido de gran intensidad? Afortunadamente, no. Hace un par de años hubo un incidente que afectó a unas instalaciones de unas depuradoras de agua en una ciudad inglesa, que reivindicó un grupo considerado por el Gobierno británico como *hackactivista,* pero la acción no era *hackactivista;* la acción era ciberterrorista. ¿Por qué? Porque manipuló los parámetros del centro de depuración y, de hecho, el propio informe que hizo público el Gobierno británico afirmaba que, si no lo hubieran detectado a tiempo, podría haber causado graves daños en la población. Entonces, eso va mucho más allá de lo que es *hackactivismo,* eso entraría ya en lo que es terrorismo. Tengan en cuenta que hay muchísimos incidentes, cada vez más, de seguridad informática, y para hablar de una acción de terrorismo lo que tiene que haber detrás es una reivindicación; si no hay una reivindicación queda como la mayoría de los incidentes, sin autoría conocida, pero las capacidades están ahí. Las organizaciones terroristas lo saben y, especialmente las vinculadas con el Dáesh, están haciendo grandes esfuerzos en esta materia. Estamos detectando constantemente esfuerzos en la recluta de informáticos, haciendo llamamientos por Twitter y por Telegram para reclutar informáticos. Llegaron a tener una estructura relativamente potente que trabajaba para Al Hayat Media Center, una estructura mediática orientada más bien a la propaganda, a la recluta, a la financiación, pero con la pérdida de soberanía —entre comillas— territorial, o sea, con la pérdida de espacio físico en Siria y en Irak, pues se ve que en esas acciones de combate se vieron directamente afectados porque su actividad en la red ha decaído. Y sabemos porque, por ejemplo, los Estados Unidos lo han reconocido, que algunos de sus objetivos de primer nivel en las acciones bélicas que han desarrollado en la zona fueron precisamente contra los dirigentes de las estructuras ciber del Dáesh. Estar están ahí y existir existen, otra cosa es hasta qué nivel están llegando en este momento. Por eso les hablaba antes de hipótesis más probable más peligrosa.

Por seguir el orden y no dispersarme, también me preguntaba por la investigación de delitos de opinión. Mire usted, la Guardia Civil investiga delitos tipificados en el Código Penal, siempre con la tutela judicial efectiva de un juez de instrucción, y cuando luego eso llega a juicio oral, va además con

cve: DSCG-12-CM-111

el aval de la acusación pública que ejerce la Fiscalía General del Estado a través del fiscal competente. Nosotros somos auxiliares de la justicia. Que luego otros Estados hagan interpretaciones, ya les dije que el Convenio contra el cibercrimen solo lo han ratificado ochenta de 196 países, cada Estado es soberano en interpretar sus propias leyes, pero de la interpretación que haga otro Estado no tenemos que extrapolar que nuestro Estado hace interpretaciones erróneas. Es mi opinión y, en cualquier caso, la función de la Guardia Civil como auxiliar de la autoridad judicial es cumplir y hacer cumplir las leyes.

El señor Salvador, del Grupo Parlamentario Ciudadanos, me preguntaba si se debería hacer un pacto nacional sobre ciberseguridad. Personalmente creo que sí, eso no quiere decir que el plan nacional que hay actualmente en vigor no sea el adecuado, ni mucho menos. De hecho, considero que el modelo actual que estamos desarrollando en España es bastante bueno. No lo digo yo, lo dicen las autoridades de la Unión Europea, lo dicen países amigos y, de hecho, estamos exportando el modelo. Les puedo decir, para satisfacción de todos, que el modelo de seguridad que estamos desarrollando en España lo estamos exportando, a través de la Organización de Estados Americanos, a todos los países de Latinoamérica porque se considera un buen modelo. Y dentro del *ranking* de la Unión Europea somos uno de los cuatro países más desarrollados en materia de ciberseguridad. Pero, claro, eso no implica decir: hemos alcanzado la gloria, podemos descansar. No, porque, como les he dicho, este mundo genera muchas incertidumbres y los pactos siempre han sido buenos; el elevar cualquier actuación a política de Estado es bueno, y que ustedes consideren que la ciberseguridad se debe tratar como una política de Estado, como es la lucha antiterrorista, por ejemplo, personalmente creo que es una idea muy acertada. Les ruego que trabajen en esa línea porque considero que será bueno para todos.

Respecto a la cultura de ciberseguridad y los niños, ese es un tema muy escabroso porque, efectivamente, la ciberseguridad empieza en el ciudadano. Es un absurdo implementar medidas de seguridad muy sofisticadas si luego el que las tiene que utilizar o desarrollar no las cumple o las cumple inadecuadamente. Siempre se ha dicho que el eslabón más débil de la seguridad es el ser humano, y es así. La seguridad es incómoda, la seguridad es engorrosa, pero es necesaria. No me contesten pero les lanzaría simplemente una pregunta: ¿cuántos de ustedes tienen un *software* específico de seguridad, un antivirus, en su teléfono móvil? Probablemente muy pocos de ustedes y, trasladado a la población, esa es la realidad. Los jóvenes están enganchados a la tecnología. En mi época estabas esperando a hacer la comunión para que te regalaran el reloj, ahora les regalan el smartphone. Ahora a los jóvenes los profesores les envían los deberes y los hacen a través de wasap, cosas que a mi personalmente me parecen barbaridades, pero bueno, llevo muchos años en esto y quizás sea porque soy viejo. Lo cierto es que los jóvenes no perciben el riesgo, no tenemos más que ver que hay mucho esfuerzo por una ley del olvido, por la privacidad, por el derecho al honor, etcétera, pero luego en las plataformas de redes sociales y de mensajería instantánea son absolutamente transparentes. Y en Internet no existe derecho al olvido, eso es una entelequia; entonces, lo que hacen hoy sigue hoy y mañana. ¿Cómo hay que combatir esto? Con educación, evidentemente. Yo sé que se están desarrollando muchas campañas de concienciación dirigidas a los jóvenes para que usen adecuada y correctamente la tecnología, pero cualquier esfuerzo que se esté desarrollando en este momento es poco. Les invito a que precisamente en esas conclusiones valoren enfatizar las campañas de concienciación dirigidas a los jóvenes, que son los adultos de mañana, porque hacen un uso muy ligero y muy banal de la tecnología.

Respecto a la formación, pues miren voy a romper una lanza a favor de la formación en nuestro país, somos un país líder en formación. Los jóvenes que salen de nuestras universidades están muy bien formados. De hecho, tenemos una alta reputación a nivel internacional, pero ¿cuál es el problema? Que esos activos se van a otros países porque las ofertas son insuficientes o no son suficientemente gratificantes. Estamos formando a los especialistas de seguridad de la práctica totalidad de los países de la Unión Europea, se nos están yendo y tenemos graves carencias en todos los sentidos. Y esto implica concienciación y compromiso de todas las partes porque, evidentemente, si una empresa equis no está dispuesta a invertir en seguridad, no estará dispuesta a invertir en personal de seguridad y a retribuir su trabajo de forma adecuada. Entonces, ese especialista se va a otra empresa que le valore más. También donde tendrían que enfatizar ustedes es en conciencia en materia de ciberseguridad de los CEO de las compañías, que lamentablemente tienen todavía unas ideas me atrevería a decir casi decimonónicas de la seguridad. De hecho, las estadísticas y los estudios que hacen ciertas organizaciones y fundaciones a nivel nacional siempre llegan a las mismas conclusiones: falta de concienciación de la alta dirección de las compañías.

cve: DSCG-12-CM-111

Me hablaban también de la guerra híbrida de Internet, que se ha convertido en un instrumento perfecto porque precisamente la dificultad en atribución y, por lo tanto, la falta de atribución concreta hace que la mayoría de las acciones queden impunes. Planteaba usted que desde instancias internacionales se fomentara o propiciara luchar contra esto. Mire, voy a ser sincero, esas instancias son los países más poderosos, los países con derecho a veto, por ejemplo, en la ONU, los países que tienen más capacidades de realizar este tipo de acciones. Por ejemplo, en la definición de ciberarma Naciones Unidas lleva más de una década intentando definir el concepto; unas veces por unos, otras por otros, a día de hoy no lo han conseguido, no han llegado a acuerdos, interfieren los intereses de Estado y el interés global o general se queda un poco colgado.

Respecto a la desinformación, es un problema al que esta sociedad, si no quiere verse gravemente afectada, tiene que hacer frente. Y una vez más, la forma más efectiva de luchar contra la desinformación es la educación porque conseguir mecanismos de detección es muy complicado. No existe una varita mágica que detecte los trols o los bots en Twitter. ¿Se pueden llegar a detectar? Sí. ¿Hay herramientas? Sí. ¿Las tenemos los cuerpos de seguridad? Sí, pero da igual porque una vez que detectas uno, aparecen cien. Hay que intentar que la ciudadanía, los jóvenes, adquieran espíritu crítico, que no se crean todo lo que vean en el minuto uno, no retuitear sin pensar porque al final la desinformación se basa en las cadenas. El problema es que las cadenas somos nosotros y retuiteamos rápidamente aquello que va con nuestras ideas, con nuestra tendencia. Entonces, es un juego difícil, ahí la tecnología puede ayudar, pero difícilmente.

En cuanto al control de los datos, los macrodatos o *big data,* es un gran problema. Recientemente hemos tenido casos muy serios de fugas de información o de revelaciones de información procedentes de grandes compañías, de multinacionales. El problema viene de ese concepto multinacional. ¿A qué legislación debe de obedecer? ¿Con qué marco normativo actúa? Ese es el problema. Voy a decir algo, porque a veces existe un poco de leyenda negra. La ciudadanía cree que los Estados o que los cuerpos de seguridad del Estado tenemos grandes macrodatos o bases de datos. Eso no es así, ojalá fuera así porque nos facilitaría mucho el trabajo. Quienes tienen los datos son las corporaciones. A mí lo que me preocupa personalmente es que vamos más hacia un futuro —esto puede sonar a una novela de ciencia ficción— de corporaciones que de Estados, donde el liderazgo lo ejercen las corporaciones por encima de los Estados. Cuando existen compañías que tienen un capital superior al producto interior bruto de un Estado, evidentemente la supremacía de la compañía sobre ese Estado es total.

El señor Alonso del Grupo Parlamentario de Unidos Podemos-En Comú Podem-En Marea ha hecho una serie de reflexiones, que personalmente —lo siento— creo que no forman parte de mi función en esta comparecencia, pero sí le voy a decir un par de cosas para su tranquilidad. Voy a enfatizar dos cuestiones. La primera de ellas es que la Guardia Civil, al igual que la Policía Nacional, siempre actuamos como auxilio de la autoridad judicial, y la autoridad judicial actúa cuando ha habido un quebrantamiento del ordenamiento jurídico. Luego cada uno podrá hacer la lectura que quiera, pero nosotros actuamos sobre la base del cumplimiento de las leyes.

Respecto a la coordinación le puedo asegurar que nuestra relación con el cuerpo de Mossos d'Esquadra es francamente buena. Tenemos relaciones y colaboración. Muchas veces nosotros mismos nos aislamos de la capa política, en la que son ustedes los que tienen que actuar, porque nosotros no somos políticos sino funcionarios y nuestra obligación es ser lo más efectivo posibles. Evidentemente para ser efectivos tenemos que interactuar entre nosotros y existe una magnífica relación, me atrevo a decir los cuerpos de seguridad, pero, desde luego, entre la Guardia Civil y el cuerpo de Mossos d'Esquadra. En ese sentido no hay ningún problema, aunque siempre haya alguien que tenga un gesto o un acto fuera de lugar. Sin embargo, en condiciones generales le puedo asegurar que las relaciones son francamente buenas. A fin de cuentas somos cuerpos de policía del Estado español. Aunque los Mossos d'Esquadra estén centrados en la Comunidad Autónoma de Cataluña, forman parte de los cuerpos de seguridad pública.

El señor Hernando me ha preguntado por el terrorismo, el *hacktivismo* y las acciones de Estado. Antes he contestado un poquito sobre el ciberterrorismo. Nosotros llevamos muchos años trabajando en este tema y, efectivamente, cuando hablamos de ciberterrorismo hacemos una diferenciación. Por un lado, está la acepción del ciberterrorismo como medio o instrumento que se utiliza para reclutas, financiación, proselitismo, captación, comunicaciones, etcétera. Toda la vida se ha estado utilizando y combatiendo y, por eso, tenemos especialistas en análisis forense, etcétera. Esa es la hipótesis más probable y ese es el 95% de nuestro trabajo. Nosotros trabajamos en el día a día para combatir ese uso que hacen, porque

cve: DSCG-12-CM-111

cada vez más pruebas inculpatorias se obtienen del mundo digital. Es decir, en la carga probatoria en los procesos penales contra células terroristas, cada vez tienen una mayor carga las evidencias y pruebas obtenidas del mundo digital.

Por otro lado, vuelvo a la hipótesis más peligrosa, está ese otro 5% que es el resto de nuestro trabajo. Observamos el escenario, hablamos con nuestros colegas nacionales e internacionales y les reitero que estamos detectando patrones y comportamientos preocupantes en el terrorismo yihadista. Además, tengan en cuenta otra cosa. Hay un concepto en ciberdelito, que se utiliza mucho ahora, que es el de cibercrimen como servicio. Existen cibercriminales con altas capacidades que venden sus servicios a otros cibercriminales. Tenemos una gran preocupación de que organizaciones terroristas tengan acceso a ese mercado de cibercriminales de alta tecnología. ¿Por qué? Pues porque esos cibercriminales nos están dando pruebas constantes de la debilidad de Internet y de la tecnología que soporta la Red. A nosotros nos preocupa mucho que esos dos mundos intersecciones.

El *hacktivismo* —que no es lo mismo que ciberactivismo, ya que es una acción legítima y legal, aunque muchas veces esté al límite de la legalidad— sencillamente se produce cuando cruzan la línea, cuando sus acciones están tipificadas en el Código Penal. Hasta la modificación del Código Penal de diciembre de 2015 el participar voluntariamente en una acción de negación de servicio, un ataque 2, muy típica en este tipo de organizaciones, no tenía ninguna repercusión penal para la persona que lo hacía en España, y desde entonces sí lo tiene. Me refiero a la acción voluntaria, no la acción a través de una red de ordenadores zombies que se denominan botnets. Por ejemplo, hemos notado claramente un descenso drástico de las acciones *hacktivistas* en España. Ha habido algunos incidentes, pero no pasan de la mera anécdota, en el último año vinculados con el postulado o posicionamiento a favor de una u otra tendencia en la situación que se está dando en Cataluña. Hay algunos como La Novena Legión que han protagonizado acciones, pero son acciones de muy baja intensidad. Afortunadamente en España el *hacktivismo* no es un problema grave, pero hay otros países donde sí lo es. Por ejemplo, en Latinoamérica tienen un problema muy serio con el *hacktivismo,* pero en España afortunadamente no lo hay.

Las acciones de Estado, lo ha dicho usted bien, las denuncias de distintos países, dejando a un lado los extremos si aplicamos la campana de Gauss, dejando a un lado a Rusia y a Estados Unidos y centrándonos más en los países próximos de la Unión Europea, pues es una realidad constante. Lo que se está detectando constantemente son pruebas de tanteo, no acciones que busquen directamente el daño, pero sí de verificación de capacidades de hacer daño en infraestructuras esenciales, especialmente en los sistemas eléctricos. Sin embargo, eso sucede a nivel mundial. De hecho ha habido casos muy concretos, ha habido acciones que han ido más allá de la mera verificación de capacidades, como ha sucedido en Israel, como ha sucedido reiteradas veces en un Ucrania, y es una realidad. De hecho a raíz de este tipo de acciones es por lo que la Unión Europea ha buscado una alianza estratégica con el CERT de la OTAN para sumar esfuerzos. Respecto a las acciones concretas no le puedo dar detalles, pero sí le puedo decir que a través de los canales de cooperación de Europol se nos ha pedido información de acciones concretas. Allí donde tenemos información, se la facilitamos a nuestros colegas a través de estos canales de cooperación policial y donde no llegamos, no llegamos. Pero sí está habiendo un intercambio de información que lo está supervisando Europol.

El señor Ramírez hablaba de la incertidumbre en su intervención. Yo soy muy pesimista, quizás porque llevo muchos años en esto ya lo veo con una cierta perspectiva, por los años. Le soy sincero: la situación a día de hoy es infinitamente más complicada que lo era hace cinco años, y a su vez, hace cinco años era infinitamente más complicada que lo era hace diez. Entonces por una mera aplicación de lógica si cada año la situación es más complicada, debemos de pensar que esto solo es susceptible de empeorar, como en las leyes de Murphy.

A continuación intentaré responder a sus preguntas. En cuanto a la formación de talento, nosotros en concreto, la Guardia Civil, tenemos un programa de formación bastante amplio con diferentes universidades. Quizás los dos programas más relevantes sean el programa que tenemos con la Escuela Politécnica de la Universidad de Alcalá de Henares y el programa que nació en el Centro Nacional de Excelencia en Ciberseguridad de la Universidad Autónoma de Madrid, donde se está dedicando mayores esfuerzos. En este programa empezamos colaborando en la creación de ese centro sobre la base de un convenio firmado por la Secretaría de Estado de Seguridad hace siete años. Este proyecto vino de Europa, que estaba potenciando la creación de una red de centros de excelencia a nivel de la Unión Europea, la denominada Red 2CENTRE. Concretamente, la Guardia Civil en los últimos cuatro años lleva desarrollando programas académicos, de formación de personal del cuerpo de altos estudios básicamente

cve: DSCG-12-CM-111

en materia de ciberseguridad y ciencia forense informática. Tocamos otras disciplinas, pero el principal objetivo es el de ciberseguridad y la lucha contra el cibercrimen. Realmente les digo que estamos bastante satisfechos de los rendimientos y resultados que estamos obteniendo hasta este momento.

Evidentemente cuando hablamos de formación, ¿tenemos activos dentro de la institución muy valiosos? Sí, pero escasos. ¿Dónde está el talento? En la universidad. ¿En qué nos apoyamos? En la universidad. En este momento nos encontramos precisamente en la fase inicial de desarrollo de un programa de promoción del talento a nivel nacional con ocasión del 175.º aniversario y recientemente hicimos el lanzamiento piloto en la Universidad de Salamanca con ocasión de su VIII centenario. Estamos fomentando desde la Guardia Civil el desarrollo de un campeonato interuniversitario de detección de talento. Asimismo, durante el año 2019 vamos a llevar acciones formativas y de entrenamiento cibernético a calculamos una veintena de universidades de todo el país, pretendemos llegar a todas las comunidades autónomas de España. ¿Nuestra estructura orgánica es la adecuada? Más nos vale. Yo creo que sí. ¿Todo es mejorable? Por supuesto, pero tenemos una estructura en la que diferenciamos las capacidades operativas, de las capacidades de gestión. Tenemos perfectamente delimitadas las estructuras en los ámbitos de Policía judicial e información. Además, existe una estructura de coordinación que depende directamente del director adjunto operativo. ¿Para qué? Para optimizar recursos humanos, la adquisición de medios y la formación, además de para coordinar. Tenemos una estructura coordinadora a nivel de la más alta instancia en la Guardia Civil. Después del director general está nuestro oficial general de mayor rango, que es el director adjunto operativo, que sirve además para reforzar el trabajo de los dos pilares de unidades de investigación tecnológica que están en la jefatura de Información y en la jefatura de Policía Judicial, como les he dicho.

¿Son suficientes los recursos humanos y materiales? Evidentemente no. Después de los años que llevo en la Guardia Civil, soy consciente de que los recursos humanos y materiales son limitados. Por eso buscamos siempre, más allá de la eficacia, la eficiencia. Por todo lo que les dije en la exposición, porque llevamos unos años que entendemos que han sido malos para todos, porque llevamos unos años con restricciones económicas y con tasas de reposición de un 0 o 10 %, pues evidentemente eso nos ha afectado. No sé si se lo dije antes, pero se lo digo ahora. Calculamos que llevamos un retraso de seis años en el plan de desarrollo que nuestra alta dirección había aprobado, motivado por la crisis. Entendemos que según vaya mejorando la situación, irán recuperando los niveles y los ritmos preestablecidos. Hay que esforzarse en ello, eso está claro.

En cuanto a adecuar los actuales métodos de captación, tienen que tener en cuenta que en nuestros métodos de captación, si es para agentes, solo podemos captar del personal que ingresa en las academias. Evidentemente nosotros hacemos un seguimiento del perfil de todos los aspirantes a guardias civiles y los currículums de todos los alumnos que ingresan en las academias son muy estudiados. Nos estamos encontrando, motivado por la crisis, que el nivel de titulados de grado superior ha crecido porcentualmente, lamentablemente para ellos, porque está claro que no era su primera opción. Sin embargo, en este caso, para nosotros es una oportunidad y sí estamos reclutando activos muy interesantes de las estructuras de base de la Guardia Civil.

Preguntaba por el modelo UME y la ciberreserva. Se le llama ciberreserva, pero en su origen era algo así como reserva estratégica de talento en materia ciber. Y quiero enfatizar eso: reserva de talento. En esto ha habido mucho ruido, sobre todo en redes sociales por parte de algunos elementos que en realidad estaban defendiendo su negocio. Algunos que se autodefinen como gurús de la seguridad informática han hecho unas campañas muy agresivas en contra de ese concepto. Vaya por delante, que ese modelo está implantado con mucho éxito ya en muchos países. Se hablaba de Estonia como un ejemplo, pues Estonia tiene activada una ciberreserva. La idea de conformar una ciberreserva a nivel nacional no es interesante sino que es necesaria, el poder activar a ciudadanos que tienen y atesoran unos conocimientos y una experiencia que en un momento determinado están dispuestos a poner a disposición del resto de los ciudadanos. Es algo parecido a un voluntariado en las ONG, en este caso sería un voluntariado con el Estado. Se tendrían que estudiar —y me consta que se está estudiando— mecanismos de compensación, mecanismos de reconocimiento, etcétera, que son, en todo caso, necesarios.

Respecto al modelo UME muchas veces se ha criticado diciendo que qué hacían los militares en los incendios. En este momento nadie concibe que ante una gran catástrofe o una situación de grave crisis nacional, ya sea una inundación o un gran incendio forestal, no haya un refuerzo de la UME —con sus virtudes y sus defectos— a los recursos normales de protección civil de las comunidades autónomas. En este caso es lo mismo. ¿Que nacen con una finalidad de defensa nacional? Perfecto, pero sería bueno

cve: DSCG-12-CM-111

que se arbitrara un mecanismo análogo al de la UME para que también pudieran actuar en una situación de emergencia nacional, que en este caso activa el Ministerio del Interior.

Me preguntaron por la desinformación, pero creo que ya he contestado a ese respecto. En cuanto a las medidas es algo muy complicado, ya les hablé de la educación, que las personas tengan un espíritu crítico, que sepan interpretar lo que leen, que contrasten información, que no se crean todo lo que hay. Si hacen un esfuerzo, por mi trabajo les puedo decir que yo todos los días veo varias cadenas de televisión y reviso varios medios de prensa escrita, podrán comprobar que no hay dos versiones iguales, son parecidas. No voy a decir que unas sean mejores o peores que otras, sencillamente son interpretaciones. Sin embargo, con una visión de conjunto puedes llegar a tener una idea más o menos aproximada de por dónde van las cosas. Si lógicamente te ciñes a ver una cadena de televisión o te ciñes a leer un solo periódico, vas a terminar lobotomizado. Lo que hace falta es espíritu crítico.

La inteligencia económica en las pymes es un punto que nos preocupa muchísimo desde hace años. Les puedo decir que estamos en este momento intentado ponerlo en marcha, pero tiene dificultades técnicas. No es una cuestión de voluntad sino de dificultades técnicas entre mecanismos colaborativos —entre el Incibe, la industria y la Guardia Civil— para apoyar en la alerta temprana de vulnerabilidades de seguridad informática a las pymes. El Incibe atesora una gran información, recolectada en sus tecnovigilancias, que en muchos casos puede afectar a las pequeñas y medianas empresas; empresas que no están dentro de los circuitos privados o que no son infraestructuras críticas de las redes de alerta de los propios organismos públicos. Por todo ello, están un poco desamparadas. Desde la Guardia Civil tenemos la voluntad de actuar como ese nexo, que a día de hoy no existe, entre el Incibe y las empresas más humildes. No olvidemos que las empresas más humildes son las que soportan la mayor masa de puestos de trabajo en el país, o sea, que son críticas.

En cuanto al modelo de carrera profesional, lógicamente somos guardias civiles. Estamos integrados en una estructura y seguimos unos modelos de proyección como cualquier otra especialidad. Lo único que intentamos, y ya se está trabajando en ello, es armonizar el modelo de promoción —vamos a decirlo claro: ascensos—, dando continuidad a esa especialización. Era y sigue siendo muy típico que un guardia civil a lo largo de treinta años de servicio empiece en seguridad ciudadana, lo que toda la vida se ha dicho rural, y a mucha honra porque yo empecé en rural y además fue una experiencia muy gratificante; luego se va a Seprona, o a Tráfico, o al Servicio Marítimo, y de ahí salta a otra especialidad. Después de treinta años el guardia civil ha tocado dos, tres o cuatro especialidades, algo que es muy enriquecedor en nuestro trabajo. Sin embargo, en el caso de tecnología lo que pretendemos, siempre que los agentes así lo deseen, es poder ofrecerles una continuidad. ¿Por qué? Pues porque son activos de formación muy complicada, muy costosa para el Estado y tenemos que optimizar.

Discúlpenme si he dejado alguna pregunta sin contestar, aunque creo que he respondido a todas. Muchas gracias.

El señor **VICEPRESIDENTE:** Muchas gracias, coronel, por las interesantes, instructivas y sinceras reflexiones que nos ha dado.

Si los portavoces lo consideran oportuno y quieren intervenir, lo haríamos por un tiempo muy limitado de tres minutos y finalmente contestaría el señor compareciente. ¿Algún portavoz quiere intervenir? **(Pausa)**. Siguiendo el mismo orden, por Esquerra Republicana de Catalunya, tiene la palabra el señor Castellana.

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

Muchas gracias, coronel, por sus reflexiones porque han sido muy interesantes, algunas son compartidas y otras quizás puedan llegar debatirse en un futuro.

Las reflexiones que ha hecho sobre la ONU, la definición del ciberarma y el papel de los Estados me reafirman en mi opinión, aunque al final quizás lo expresemos de forma diferente. Usted ha puesto el ejemplo de Dáesh como la amenaza fantasma, pero lo que tenemos que explicar al ciudadano es que los fantasmas no existen, porque detrás de los fantasmas hay gente de carne y hueso. Por ejemplo, en el caso de Dáesh usted ha hablado del control de territorio, características de pseudo-Estado. En el inicio de Dáesh hay financiamiento de Estados y en la cúspide de Dáesh hay financiación a través del contrabando de petróleo con la colaboración de un Estado de la OTAN.

Ha hablado de desinformación, cuestión que me parece muy interesante. Multiplicaría por cien su afirmación: es muy importante combatir la desinformación e intoxicación en Internet. Sin embargo, si vas a un quiosco hay desinformación e intoxicación a mansalva e incluso ha habido ministros y presidentes

cve: DSCG-12-CM-111

del Gobierno, en un pasado reciente o en un pasado más lejano, que han emitido públicamente informaciones claramente falsas.

Comparto también su reflexión sobre las grandes corporaciones. Solamente los fanáticos del capitalismo como su gran religión son incapaces de ver cómo va convergiendo el tema de las grandes corporaciones y el Estado. Un ejemplo lo tenemos en China, en el sentido contrario al del mundo occidental, pero que al final acabará, si no lo podemos evitar, en lo mismo.

Hay un tema en el que quizás podemos discrepar. Muchos ciudadanos apreciamos un sesgo ideológico —es una apreciación— sobre determinadas actuaciones. No obstante, usted ha definido muy bien el papel de la Guardia Civil como auxiliar de la Administración de Justicia en un momento donde hay resoluciones del Tribunal Supremo en temas muy importantes, que solo pueden ser calificadas de derecho ficción. Entiendo que hay tanto debate que no lo podemos tener hoy.

Muchas gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Castellana.

A continuación, por el Grupo Parlamentario Ciudadanos, tiene la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Muchas gracias, señor presidente.

Vuelvo a mostrarle mi agradecimiento por su sinceridad. Cuando me refería, por ejemplo, a la necesidad de formación no significa que nosotros no seamos buenos en formación, significa que no tenemos estudios especializados en las universidades y que no hay planes de estudio vinculados a todo este tema, y es una realidad. En el tema de la cultura, usted mismo ha dicho que no existe esa cultura de la ciberseguridad ni de un uso adecuado, pero no solo de los jóvenes y las pymes sino también de las personas adultas. Usted ha puesto un ejemplo en esta misma sala cuando ha preguntado que quiénes tenemos un *software* de protección dentro de los móviles.

Cuando he mencionado el pacto de Estado por la ciberseguridad no lo he hecho para hacer ver que somos unos chicos buenos que decimos que esto es una política de Estado. Digo esto porque precisamente hoy se ha puesto de manifiesto aquí, así como en otras Comisiones, que cuando tratamos de este tema existe la tentación por parte de algunos grupos políticos de entrar en las competencias: esto es tuyo, esto es mío, a quién le corresponde, etcétera. Sin embargo, cuando estamos hablando de ciberseguridad los buenos que se defienden no pueden estar en eso, cuando los malos no tienen fronteras ni competencias, ni tampoco escasez de medios, y además tienen toda la tabla salarial posible para fichar todo el talento que quieran. Por tanto, cuando decimos que hay que hacer un pacto de Estado es para intentar sensibilizar a todos los grupos de esta Cámara y hacerles entender que esto no tiene nada que ver ni con el Estado de las autonomías, ni con una España centralizada, sino que estamos hablando del mundo y cómo podemos actuar sobre él.

Por otra parte, respecto al tema de la comunidad internacional le ha salido la vena pesimista en algunas partes de su intervención. Cuando hablamos de crímenes de guerra de lesa humanidad, son las instituciones internacionales las que han definido qué es eso y cómo acometerlo. Cuando hablamos de qué hay que hacer con los prisioneros en tiempos de guerra, hay tratados que se acuerdan para este asunto. Usted mismo ha reconocido cuando he mencionado el tema de los macrodatos, que quizás en el futuro no estemos acercando más que a un mundo de dominio de los Estados, a un mundo de las grandes corporaciones que pueden controlar esos macrodatos, y la gente que entiende un poquito sabe lo que eso puede suponer. Razón de más para que vayamos sensibilizándonos sobre la adopción de grandes acuerdos dentro de la comunidad internacional. Usted ha dicho una cosa en la que tiene razón, los grandes Estados que deberían tener mayor interés son también los que tienen más confluencias en un doble sentido: por una parte, con estas mismas corporaciones y, por otra, tampoco demuestran mucho interés en regular y entrar en esto demasiado porque son los usuarios y benefactores de esas malas prácticas; razón de más para que tengan que contar a la comunidad internacional si están en contra de estos temas que mayoritariamente la comunidad internacional no ve así. Si no se llevan estos temas a la comunidad internacional, entonces viven fantástico, o sea, siguen haciéndolo y encima no tienen que responder ante nadie. Por tanto, queremos escuchar a las grandes potencias que tienen poder de veto y ver si vetan decisiones en temas relacionados con el Gobierno mundial, dada la globalización y hacia donde nos estamos dirigiendo. No sirve una actitud de defensa —con esto termino definitivamente— y de ver cómo nos protegemos de los ataques y las amenazas. Usted mismo ha dejado entrever en el ámbito del ciberterrorismo que en este momento estamos como estamos, pero puede ser peor en el futuro, por lo tanto, precaución; o sea, recursos humanos, recursos técnicos, de formación, cultura, pactos de Estado,

cve: DSCG-12-CM-111

todo es poco para poner remedio a las amenazas contra la seguridad y, repito, sin perder libertades porque no se trata de eso.

El señor **VICEPRESIDENTE:** Tiene que ir terminando.

El señor **SALVADOR GARCÍA:** Sí, señor presidente, ya he terminado. Muchas gracias.

El señor **VICEPRESIDENTE:** Por el Grupo Parlamentario Confederal Unidos Podemos-En Comú Podem-En Marea, tiene la palabra el señor Alonso.

El señor **ALONSO CANTORNÉ:** Muchas gracias.

Muchas gracias, señor Hernández. Me ha preocupado sobre todo un tema que ha repetido usted dos veces, y es que llevamos seis años de retraso, porque en este mundo del que estamos hablando lógicamente seis años son muchos, podríamos estar en la Edad del Hierro porque todo avanza muy deprisa. Por tanto, de qué forma piensan recuperar esos seis años porque entendemos que será complicado. Me ha gustado también que haya hecho constar en sede parlamentaria algo que a mí que consta, que es la buena relación y coordinación que existe entre los Mossos d'Esquadra y los cuerpos de seguridad del Estado, en concreto, con la Guardia Civil. Es bueno que se diga en sede parlamentaria porque muchas veces eso no se escucha o se escuchan otras cosas. Para acabar, efectivamente, me ha gustado mucho la pregunta del señor Hernando, no de cosas de España a las que no va a contestar, pero sí de otros países como Holanda, Inglaterra, etcétera. Y ya que puedo hablar del extranjero, querría preguntarle si considera que el año pasado hubo falta de coordinación entre el área técnica de información del Gobierno de Estonia y ustedes, o sea, si hubo deslealtad entre Estonia y España.

Muchas gracias.

El señor **VICEPRESIDENTE:** Gracias, señor Alonso.

Por el Grupo Parlamentario Socialista, tiene la palabra el señor Hernando.

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

Una brevísima consideración respecto a un tema que me ha parecido sugerente e importante, que es el pacto de Estado en esta materia. Coronel, sinceramente creo que en este tema los miembros de la Comisión estamos mucho más de acuerdo de lo que podría parecer. Yo intentaría que no hubiese afán diferenciador cuando no es necesario el afán diferenciador, porque en este tema hay mucha coincidencia en la posición de todos los grupos, y prueba de ello es con qué mayoría se aprueban determinadas leyes que son las que dan lugar a la creación de esta Comisión. Claro, si uno no está de acuerdo con la ley o no vota la ley es que muy de acuerdo no va a estar ni tan siquiera en la entrada en un pacto de Estado de estas características. Soy muy partidario de los pactos en cuestiones de Estado, que vaya eso por delante, muy partidario, y además en alguno he tenido participación activa, pero cuando no es necesario porque hay una enorme coincidencia tanto en la aprobación de la ley como en la Estrategia de Seguridad Nacional, es decir, en el desarrollo de la ley, no sé hasta qué punto sería necesario un pacto de esas características porque, sinceramente, creo que en el fondo en esta materia, afortunadamente, hay mucha coincidencia de la mayoría de los grupos, aunque siempre habrá algún grupo que legítimamente considere que no está de acuerdo con esa opinión o posicionamiento mayoritario en este tema.

El señor **VICEPRESIDENTE:** Gracias, señor Hernando.

Por el Grupo Parlamentario Popular, tiene la palabra el señor Ramírez.

El señor **RAMÍREZ RODRÍGUEZ:** Gracias, señor presidente.

A modo de conclusión diré brevísimamente, por una parte, que uno se queda con la impresión de que somos meros espectadores, que la película está transcurriendo y vamos tarde. No vamos tarde seis años, como decía el portavoz del Grupo Parlamentario Confederal Unidos Podemos-En Comú Podem-En Marea, es la tasa de reposición la que lleva seis años de retraso, no las políticas de ciberseguridad en general. Creo que tenemos que felicitarnos por cómo se llevan las políticas de ciberseguridad, por cuál es la acción en general del Gobierno, de las estructuras del Estado y de la Guardia Civil; sin embargo, tenemos que decir que vamos un poquito a remolque. Ha sido muy llamativo el ejemplo que usted nos ha relatado sucintamente del ataque ciberterrorista sobre el tratamiento de las aguas en Gran Bretaña, pero que verdaderamente pone de manifiesto lo gravísima que puede llegar a ser esa amenaza de

cve: DSCG-12-CM-111

ciberterrorismo que todavía está en un nivel muy elemental. También ha sido muy significativa su manifestación de que estamos formando a los especialistas en ciberseguridad de la Unión Europea porque estamos a muy alto nivel en formación, pero ese prurito español de pagar tan poco y tan mal, esos sueldos tan bajos que venimos pagando hace ya mucho tiempo desde la crisis, están haciendo que realmente perdamos grandes valores en este campo.

Coronel, nos quedamos con una sensación agridulce en tanto en cuanto se hace muy buena labor desde las estructuras del Estado, tenemos que celebrar, como ha dicho el portavoz del Grupo Parlamentario Socialista, el señor Hernando, esa especie de acuerdo de base donde no hace falta diferenciarnos, pero uno también se queda con la sensación de que nos queda mucho por hacer, nos queda mucha labor de concienciación, necesitamos que los jóvenes se pongan al día y se tomen en serio todo esto. Usted nos ha puesto un ejemplo con los smartphones, y nos ha preguntado cuántos miembros de esta Comisión tienen un sistema de detección de virus suficiente. Mi compañera, Ana Belén Vázquez, me decía que ninguno. Creo que no está mal que tengamos un arranque de sinceridad y digamos ninguno, aunque estemos exagerando; lo mismo hay uno o dos que sí lo tienen, pero en general no. Señor Hernando, respecto al pacto de Estado, estoy de acuerdo con usted en que no hace falta hacer pactos de Estado de todo, pero me parece que el asunto de la ciberseguridad, la necesidad de concienciación de nuestra sociedad, así como de acercarnos lo más posible al conocimiento, sí ponen de manifiesto que elevar a política de Estado esta cuestión es absolutamente necesario.

Muchas gracias, coronel.

El señor **VICEPRESIDENTE:** Gracias, señor Ramírez.

Para finalizar vamos a dar nuevamente la palabra al señor compareciente, para que usted dé respuesta a las preguntas y hacer las reflexiones que considere.

El señor **HERNÁNDEZ GARCÍA** (coronel del área técnica de la Jefatura de Información de la Guardia Civil): Gracias, señor presidente.

El señor Castellana, de Esquerra Republicana, ha hablado del sesgo ideológico. ¿Quién no tiene sesgo ideológico?, pero le puedo asegurar una cosa; los guardias civiles, como cualquier miembro de las Fuerzas y Cuerpos de Seguridad del Estado —yo hablo de la Guardia Civil porque soy guardia civil—, cuando nos ponemos la guerrera dejamos la ideología en casa, y cuando llegamos a casa y nos ponemos en zapatillas recuperamos nuestro perfil de ciudadano. Y nos pueden gustar más o menos las cosas, cómo están, cómo se hacen o se dejan de hacer y, evidentemente, ejercemos nuestro derecho al voto y orientamos el voto de acuerdo con el sesgo ideológico, pero lo que le puedo garantizar es que cuando vestimos el uniforme actuamos con absoluta neutralidad. De hecho, solo voy a hacer una reflexión; con lo difícil que fue el siglo XIX en España, con lo complicado que fue el siglo XX en España y, afortunadamente, no es comparable, como está empezando el siglo XXI, aunque también tenemos nuestras cositas, todo hay que decirlo, con los vaivenes políticos que ha habido en España en estos siglos, ¿cree de verdad que si la Guardia Civil no hubiera sido un cuerpo absolutamente neutral y absolutamente leal al poder legítimo, seguiríamos existiendo? Hubiéramos cambiado de nombre, hubiéramos cambiado de color el uniforme, hubiéramos cambiado en mil cosas, pero no hemos cambiado en nada porque mantenemos la esencia, y una de nuestras esencias fundamentales es la absoluta neutralidad. Eso que le quede claro.

El señor Salvador, de Ciudadanos, se ha referido al pacto de Estado. Veo que tienen discrepancias entre ustedes. En mi humilde opinión lo único que puedo decir, porque he visto que ha salido varias veces, es que en mi limitado entender un pacto de Estado lo que permite es garantizar inversiones, garantizar proyectos, garantizar actuaciones más allá de la acción política del momento; o sea, marcar una línea no tan cortoplacista como pueden ser una o dos legislaturas, sino marcar un horizonte con unos objetivos más lejanos e intentar no desviarse de ellos con independencia del día a día de la política, pero, claro, esa es una decisión que tienen que adoptar ustedes. Este es el valor que yo doy a un pacto de Estado. ¿Por qué? Porque hemos vivido experiencias muy favorables y muy positivas como el Pacto de Estado en la lucha contra el terrorismo, el Pacto de Estado en la lucha contra ETA fue una pieza clave y fundamental. Más recientemente tenemos el Pacto de Estado de lucha contra el yihadismo, y confiamos en que sea una pieza fundamental. Cualquier acción que rebase la acción política y entre en la acción estratégica o de Estado, personalmente creo que es buena, pero, insisto, no soy quien ni siquiera para opinar. Por otra parte, los grandes acuerdos a nivel internacional son imprescindibles, lo que pasa es que yo veo poca voluntad de llegar a acuerdos a nivel internacional por lo que usted bien ha dicho, porque interfieren con los intereses de los propios Estados o de las alianzas entre Estados, hay corrientes, hay ejes.

cve: DSCG-12-CM-111

Evidentemente, lo deseable es que fuéramos capaces de ponernos todos de acuerdo y convivir en este planeta sin estar matándonos unos a otros, sin estar robándonos unos a otros y sin estar extorsionándonos unos a otros, pero eso es una Arcadia feliz que ojalá llegara.

Señor Alonso, del Grupo Parlamentario Confederal Unidos Podemos-En Comú Podem-En Marea, matizo, no ha sido un retraso de seis años, ha sido ralentización, o sea, los programas que teníamos de evolución han seguido. De hecho, yo me considero afortunado porque a pesar de la crisis, la unidad que ahora dirijo todos los años ha crecido, todos los años ha recibido recursos humanos y materiales, o sea, no hemos parado; lo que sucede es que no han llegado en la cantidad y en los tiempos inicialmente previstos, ha habido un retardo y, evidentemente, confiamos en poder recuperarlos. Usted me ha preguntado por lo de Estonia-España, España-Estonia, sé que no debo meterme; no sé nada, no sé más allá de la prensa, pero a título personal yo le digo que si Estonia hubiera llegado a algún tipo de acuerdos con la Generalidad de Cataluña a espaldas del Gobierno español, evidentemente Estonia habría cometido una gran deslealtad con el Estado español, de eso no cabe duda, es así de claro.

Señor Hernando, del Grupo Parlamentario Socialista, usted ha enfatizado mucho en el pacto de Estado y creo que ya está contestado. En las demás líneas argumentales estamos totalmente en sintonía. En respuesta al señor Ramírez, le voy a dar un dato sobre el talento universitario. Es cierto que, como ha dicho también el señor Salvador, en los programas académicos de las carreras de ciencias se está notando que la parte de seguridad no tiene el peso adecuado. Nos consta que son conscientes y están corrigiendo esas tendencias. Es normal que en algunas ingenierías la seguridad solo ocupe una asignatura cuatrimestral en una carrera de cuatro años, claramente poco, y se está corrigiendo. Insisto, a pesar de eso, tenemos un talento realmente sorprendente. Les voy a dar un dato, el Incibe selecciona de distintas universidades y crea un equipo nacional de jóvenes universitarios que compiten en los ejercicios europeos. ¿Saben que en los dos últimos años ha sido España la que ha ganado? Evidentemente, esto no es el fútbol, no hay titulares en el telediario, pero sepan ustedes que los dos últimos años el equipo interuniversitario español es el que ha ganado el campeonato europeo. Esperemos que este año en octubre gane por tercera vez. Ahora bien, si me preguntan dónde están ahora los jóvenes que ganaron hace dos años, ahí es donde nos podemos deprimir. Y lamento mucho dejarles una sensación agridulce, pero es que mi responsabilidad y mi obligación era trasladarles la visión más objetiva posible. Lamentablemente, no venía a contarles una historia bonita, venía a contarles lo que hay y lo que hay, evidentemente, es preocupante.

El señor **VICEPRESIDENTE:** Muchas gracias, coronel don Luis Fernando Hernández García, por su extensa, interesante, instructiva y sincera comparecencia.

Sin más asuntos que tratar, se levanta la sesión. Muchas gracias.

Eran las doce y veinte minutos del mediodía.

CORRECCIÓN DE ERROR.

En el *Diario de Sesiones* número 105, correspondiente a la Comisión Mixta de Seguridad Nacional, sesión número 18, en la portada, en los puntos correspondientes a la elección de vacantes, donde dice: «Número de expediente del Senado 570/000005», debe decir: «571/000005».

cve: DSCG-12-CM-111