DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2019 | XII LEGISLATURA | Núm. 131 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 26

celebrada el jueves 14 de febrero de 2019 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

---

cve: DSCG-12-CM-131

Se abre la sesión a las diez de la mañana.

COMPARECENCIAS. POR ACUERDO DE LA COMISIÓN MIXTA DE SEGURIDAD NACIONAL:

— DEL SEÑOR SECRETARIO DE ESTADO DIRECTOR DEL CENTRO NACIONAL DE INTELIGENCIA (SANZ ROLDÁN), PARA INFORMAR CON CARÁCTER GENERAL SOBRE LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/002361 y número de expediente del Senado 713/001147).

El señor **PRESIDENTE:** Buenos días, señorías.

Vamos a empezar la comparecencia. Es una agenda cargada y en el día de hoy todos tenemos acomodaciones de viaje para estar preparados para oír mañana las palabras del presidente. Por tanto seré muy riguroso en los tiempos. Advierto de que el objeto de esta comparecencia es hablar sobre la ciberseguridad en España. Tenemos con nosotros al director del Centro Nacional de Inteligencia. Ruego a sus señorías que se ciñan estrictamente al objeto de la comparecencia; por elevados que sean sus pensamientos o sus reflexiones en otras materias, me veré obligado a desecharlas si se empeñan en ponerlas ante este foro.

General, director del Centro Nacional de Inteligencia, tiene usted la palabra. Habrá un turno de intervención de los portavoces, una nueva intervención por su parte y un segundo turno, muy breve, para los representantes de las distintas formaciones parlamentarias. Esa es la liturgia de esta casa y a ella nos vamos a atener.

General.

El señor **SECRETARIO DE ESTADO DIRECTOR DEL CENTRO NACIONAL DE INTELIGENCIA** (Sanz Roldán): Muchas gracias, señor presidente.

Señorías, aunque parezca un lugar común, desde luego les garantizo que para mí no lo es, y es un honor estar en el Parlamento. Es un honor poder venir a cumplir con un deber democrático como es informar en esta Comisión sobre aquello de lo que humildemente pueda informar. Y digo humildemente porque sé que por aquí han pasado personas que, especialmente en lo técnico, están mucho más cualificadas que yo. Quizá lo que falte —esa es mi intención: que lo pretendo cubrir— es decirles a ustedes cómo desde el Consejo Nacional de Ciberseguridad que presido se ve la ciberseguridad en España. Esto es algo que nadie excepto yo puede decir puesto que, como es obvio, solo hay un presidente del Consejo Ciber. Esa es mi intención además, y espero que sea útil a los efectos de esta Comisión Mixta sobre Seguridad Nacional.

No sé si es muy correcto, señor presidente, pero me gustaría poner un vídeo de tres minutos de duración, porque creo que define muy bien la magnitud del problema. **(Se proyecta un vídeo).**

Les ruego disculpen el tono vehemente y que en algún momento de la presentación pueda parecer propagandístico, pero la realidad es que dice dos o tres cosas que me traen precisamente ante esta Comisión: ¿quiere usted trabajar para otros? ¿Quiere usted trabajar para los demás sin sueldo? ¿Quiere usted darle sus beneficios empresariales a alguien sin recibir nada a cambio? ¿Quiere usted poner en manos de alguien su seguridad? Todo esto es lo que está diciendo este pequeño vídeo que hemos visto, y ese es precisamente el asunto que nos ocupa. Esta no es una cuestión que ocurra ahora. El progreso siempre ha traído consigo riesgos, amenazas e inquietudes; ha ocurrido durante toda nuestra historia y ocurre ahora aquí. Internet nos ha traído sin duda muchos beneficios, pero también nos ha traído algunos problemas. La red ahora es una y única, una y única e incluso las redes corporativas tienen como objetivo fundamental estar en la red general. En la red estamos todos, estamos los buenos y los malos, y por tanto todo el que quiere a través de la red cometer algún delito, robar información o cualquier otra actividad como las que hemos dicho, no lo tiene demasiado difícil.

¿Por qué los malos van a la red? Esto me recuerda una anécdota que se cuenta, y que no sé si es cierta, sobre Jesse James. Cuando tenía veintinueve años fue detenido por el *sheriff* de una ciudad de Minnessota —a quien imagino mayor, con cierta bonhomía—; se acercó a él y le dijo, con esas formas en que estos señores mayores en los Estados Unidos de finales del siglo XX se dirigían a las personas: hijo, ¿por qué robas bancos? Y Jesse James le contesta: porque es ahí donde está el dinero. Pues lo mismo ocurre con la red. ¿Por qué van los malos a la red? Pues porque ahí está todo, y porque ahí pueden pescar, pueden ejercer sus actividades ilícitas, porque de ahí pueden obtener información, etcétera. Por tanto encuentro absolutamente justificado que en esta Comisión, que trata sobre la

cve: DSCG-12-CM-131

seguridad nacional, se hable de ciberseguridad, porque es efectivamente uno de los retos en que el mundo moderno nos pone.

Se dan muchísimas estadísticas al respecto y si alguna de sus señorías las desea se las puedo ofrecer, pero la realidad es que los ataques a la red y los usuarios de la misma, ambos, progresan de forma exponencial. Cada vez hay más usuarios en la red y cada vez hay más personas que quieren utilizarla de forma aviesa. Hemos llegado a un punto en el que hasta las cosas se hablan a través de la red. Dicen los técnicos que ya hay más de un 50 %, cerca de un 60 % del tráfico de Internet en el que no intervienen personas, son las cosas las que se hablan. Hace unos días asistí a una empresa de seguridad que nos mostró, a través de lo que hoy se llaman elementos que se pueden vestir, que se pueden usar cotidianamente, cómo se podría saber perfectamente dónde estaban todos y cada uno de los agentes de la policía que tomaban parte en un determinado acto que requería seguridad, sin que los policías hicieran nada; simplemente un chip colocado en algún lugar del uniforme era más que suficiente ya para emitir y transmitir su situación, incluso —y dejen volar su imaginación— lo que estaban percibiendo sobre la propia manifestación a través del índice de calor corporal o de la agitación de su corazón. En fin, es algo que parece que entra en el campo de la ciencia-ficción, pero no lo es. Ya una de las cuestiones que tenemos que ir pensando es precisamente que el Internet de las cosas, es decir, que las cosas a través de Internet se hablarán y tomarán determinadas decisiones, y que naturalmente quien quiera subvertir esta misión, inicialmente útil, podrá hacerlo sin problema. La última estadística que he leído es que durante este año puede haber ya más de 35000 millones de dispositivos interconectados; es decir, la nevera de casa con la tienda de El Corte Inglés o de un establecimiento comercial, etcétera. Por tanto, sin que yo quiera incidir más en la importancia de este tema, creo que alguien más habrá hablado, pero si hace unos días que no se reúne esta Comisión para hablar con alguien de ciberseguridad pueden haber aumentado en un número importantísimo, tanto el uso de la red como el número de personas conectadas como la capacidad de la propia red para el objetivo para el que está trazada.

No obstante el asunto que nos ocupa hoy es el de que esta red esté segura, y desde luego supongo que nos ocupará cómo se está trabajando en el seno del Consejo Nacional de Seguridad para que la red esté lo más segura posible. Les debo decir, en primer lugar, que el problema es muy complejo, y que mantener el aseguramiento de la red es muy complejo; a veces nos van bien las cosas, y hasta ahora nos han ido prácticamente siempre bien. Yo siempre cuento el ejemplo del virus WannaCry, aquel famoso virus que colapsó toda la sanidad del Reino Unido, y que en cambio aquí, aunque a algunas empresas tecnológicas les afectó, la realidad es que, que sepamos, un solo equipo de la sanidad de una comunidad autónoma fue víctima del virus, y por tanto el daño fue muy pequeño. Pero además les añado otros datos a sus señorías: una vez que se detecta el virus WannaCry a la 1:30 de un viernes, alrededor de las 6 de esa misma tarde España tenía la vacuna contra el virus, se colgó en la página del Centro Criptológico Nacional a las 5:40 de ese día, y una hora después 600000 personas, no todas españolas, se habían descargado la vacuna del virus WannaCry, entre ellas tres Estados. Por tanto esto es lo que les quiero ofrecer como detalle, pero tampoco piensen que porque ya nos ha ocurrido esto nos dormimos en los laureles y decimos que estamos bien, porque, primero, en casi todas las actividades de la red hay un factor muy importante de estar encima, de estar preocupado, de estar preparado, de tener las ondas suficientes, pero también hay un factor de que tengamos la suerte de reaccionar pronto y bien, y que tengamos la suerte de contar con las herramientas *ad hoc* para ese particular virus, eso puede no ocurrir siempre. Esta es una realidad, y lo que pretendo transmitir a sus señorías es precisamente esa realidad.

La red nos sirve para muchas cosas, y también sirve como les decía a los malos. Nosotros sabemos que el sistema de mando y control del Daesh ha sido la red, no se han preocupado de establecer un propio sistema de mando y control, sino que han dicho: pero si ya tenemos uno, simplemente situando tabletas en ciertos lugares y utilizando la red han sido capaces de transmitirse órdenes, directivas y consignas. Por ejemplo, durante el asalto a Mosul, que duró del orden de trece o catorce días, el Daesh usó unos 40000 tuits para dar órdenes. Por tanto no se trata solo de que la red esté protegida, se trata también de que hemos de saber qué circula por la red. Es decir, a nosotros los 40000 mensajes que circularon en el asalto a Mosul por la red no nos hicieron de manera directa ningún daño, sí nos resultaba absolutamente interesante saber lo que estaba ocurriendo, primero, para las fuerzas que se defendían, y segundo, para las implicaciones que podría tener en nuestra seguridad, especialmente en el caso de la lucha contra el terrorismo yihadista.

Ahí está, y además es un recurso barato y además que puede reincidir varias veces. Si ustedes me permiten el símil de un ataque, un ataque de forma tradicional si falla, a lo mejor necesitamos reconstituir

cve: DSCG-12-CM-131

la unidad que ataca durante un mes o dos, y a ver si hay suerte la vez siguiente, o a lo mejor el coste es tan alto que a nadie se le ocurre volver a hacerlo. En el caso de los ataques ciber pueden reincidir todo lo que quieran hasta ver si nos cogen dormidos o despistados en un determinado asunto, o incluso si deducen por qué el ataque ha sido rechazado, a lo mejor con una ligera modificación de una APT pueden volver momentos después y encontrarnos con que el ataque se produce de forma consistente durante mucho tiempo, hasta ver si pueden tener éxito.

Esta es la situación; la podríamos describir con más detalle, y si sus señorías lo desean aquí estoy. Pero yo quería hablarles más de qué ha hecho España, de qué se hace en España para que este problema, esta amenaza o este riesgo puedan estar bajo control de la mejor manera. En primer lugar, les diré que dependiendo del Consejo de Seguridad Nacional se creó el Consejo Nacional de Ciberseguridad, que me honro en presidir, no sé si ya estoy en el séptimo año, y recibo la responsabilidad del Consejo de Seguridad Nacional de proteger a las administraciones, al sector público, a las infraestructuras críticas y a los ciudadanos de los ataques ciber. Esto, que es una misión amplísima y que es difícil, la ejecuto con el concurso de muchos, por tanto ese es un elemento que debemos conocer, que básicamente esos muchos son casi todos los departamentos ministeriales, pero hay una organización de cierta fortaleza para enfrentarse precisamente a esta cuestión. Esa organización está distribuida en capas, y en cada capa tiene un responsable primario, pero que siempre puede recurrir al resto de los elementos del sistema. En primer lugar, hay que proteger a las administraciones, sea la local, sea la autonómica, sea la Administración General del Estado. Esa parte de mi misión la cumple el Centro Criptológico Nacional. Por tanto, en cualquier ocasión en que alguna Administración reciba un ataque ciber, el primero que tiene la responsabilidad de conocerlo y después de reaccionar ante él es el Centro Criptológico Nacional, que yo me apresuro a decirles a sus señorías que está colocado con el Centro Nacional de Inteligencia, pero que no es el Centro Nacional de Inteligencia. Yo tengo dos o tres sombreros —como ahora tradicionalmente se dice— o dos o tres responsabilidades: una es ser director del CNI —y creo que ustedes piensan que soy solo eso—, pero también soy director del Centro Criptológico Nacional y también soy presidente del Consejo Nacional de Ciberseguridad, a los efectos de esta Comisión.

Cuando el ataque se produce a una infraestructura crítica el responsable es el Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras Críticas, que depende de la Secretaría de Estado de Interior. Pero también en España todos los ciudadanos y las pequeñas y medianas empresas tienen un lugar al que acudir si tienen un ataque de este estilo, el Incibe, el Instituto Nacional de Ciberseguridad, que está en León. Por tanto hay un problema grande, magnífico, pero tenemos alguna organización que va haciendo que la misión se vaya compartiendo en trozos para que sea un poco más fácil su cumplimiento.

Queda una cuarta pata del sistema de protección ciber que es el Centro de Ciberseguridad de la Defensa, que se hace en reflejo de las decisiones internacionales —especialmente en el ámbito de la Alianza Atlántica— para crear un elemento de protección ciber de las comunicaciones militares y de las organizaciones militares en su conjunto o de las organizaciones de la defensa. Por tanto eso es lo que tengo a mi disposición en el Consejo Nacional de Ciberseguridad ¿Es mucho o es poco? Yo creo que cuantas más organizaciones haya que coordinar, más difícil será la coordinación. Cuando me pregunta algún jefe de servicio secreto extranjero que qué tal se coordina en España el servicio secreto interior con el servicio secreto exterior, siempre le digo: de maravilla, porque yo me coordino conmigo mismo. **(Risas).**

Son cuatro elementos, pero tienen su responsabilidad absolutamente compartida y trabajan con alguna eficacia. ¿Por qué digo alguna eficacia? Porque la eficacia absoluta en el ámbito ciber es prácticamente imposible. Nosotros recibimos —tengo aquí el último dato, que me han dado esta mañana—, solo durante el mes de enero, más de 4000 incidentes. En el periodo que estamos viendo —año 2018, ya terminado— hemos tenido 38000 incidentes. Es verdad que de los 38000 incidentes la inmensa mayoría o no tienen importancia, desde el punto de vista de la seguridad, o de forma automática con los sistemas que tenemos establecidos se van neutralizando. Pero sí es verdad que hay algunos incidentes que son críticos, y los que tenemos clasificados como críticos son del orden de uno cada tres o cuatro días. En esos es en los que verdaderamente tenemos que hacer un gran esfuerzo. Un incidente crítico lo que trata es de controlar una infraestructura crítica, por ejemplo, entrar en un ministerio para obtener una determinada estrategia en un ámbito de la Administración del Estado. Esos son los que tenemos que impedir que, si se manifiestan, progresen.

El instrumento principal para que esto sea así son las herramientas que el propio Centro Criptológico Nacional ha diseñado. Es decir, este *software* para hacer frente a ataques normalmente si se compra ya

cve: DSCG-12-CM-131

nace con problemas. De hecho se ha acuñado, en la terminología de los que de esto entienden, como los defectos día cero, es decir, que el día que sale un instrumento —por ejemplo un teléfono móvil— sale ya con los suficientes defectos como para que puedan ser introducidos en los mercados negros de la ciberseguridad, y ser utilizados ya al día siguiente de forma aviesa. Este es el caso WannaCry. Me parece recordar que cuando el Iphone 7, de Apple, se lanzó al mercado, ese mismo día —en el entorno de los propios fabricantes— descubrieron su debilidad, la vendieron y a continuación, utilizando esa debilidad, entraron en todos los sistemas. Por tanto son las propias debilidades día cero las que nos ponen en riesgo.

Aprovecho —aunque a lo mejor les parece un poco deslavazada esta pequeña presentación— para decirles algo que sí que creo, presidente, que es de esta Comisión. Si alguien diseña una nevera, un vehículo o un instrumento de sonido, que no sea el ordenador, la legislación nacional le exige unas pautas de seguridad. De hecho, al comprar una televisión, nos dicen antes que ha pasado todos los controles de la Unión Europea y de no sé qué otro sitio. Pero, fíjense, cuando nos compramos una tableta, la única norma de seguridad que tiene es la de su cargador; a la tableta no se le aplica ninguna norma de seguridad. Nadie ha sido capaz de regular que esa tableta tiene que traer por ejemplo cortafuegos, tiene que traer sistemas fáciles de usar para poder estar seguros de que solo entramos nosotros. No, no, la tableta es libre, nuestros ordenadores son libres; en cambio a los cargadores sí les exigimos unas normas de seguridad, no sea que vaya a quemarse alguien mientras se está cargando. En alguna ocasión habrá que legislar en ese sentido, y puesto que a un coche le exigimos que tenga una capacidad de frenada determinada, y si no, no se pone en el mercado, a un ordenador habrá que decirle que tiene que tener estas capacidades de detección de un intruso, y si no, no se vende. Creo que esto es tan razonable que quizá sea un punto que mereciera la consideración de esta Comisión —no soy quién para decirlo—. Es decir, aquí los elementos que se ponen a la venta tienen que facilitarle al usuario su trabajo seguro.

Pues bien, siguiendo con esto, el Centro Criptológico Nacional ha dado luz a sus herramientas para controlar lo que pasa por la red. Herramientas que, de forma voluntaria, las Administraciones, los entes de seguridad privados, etcétera, pueden admitir que se coloquen en su red. Saco también este tema por algo. Fíjense, cuando llegué al Centro Nacional de Inteligencia y hablé por primera vez con el Centro Criptológico Nacional teníamos situadas diecinueve herramientas en la Administración para detectar la intrusión de alguien. Y cuando queríamos instalar la herramienta número veinte el rechazo siempre era el mismo. Nos decían que para qué quería poner allí el Centro Criptológico Nacional una herramienta; decían que lo que quería el CNI con esto era enterarse de lo que pasaba por su red. No es verdad. Cuando hemos conseguido crear un clima de confianza, que es fundamental con el usuario; cuando los usuarios se dan cuenta de que es bueno tener en su red un instrumento de detección de intrusos, y cuando a la vez el ciudadano o el usuario se ha dado cuenta de que lo que hace este Centro Criptológico Nacional es ayudarle y solo ayudarle, y cuando es más que patente que nunca jamás con origen en el Centro Criptológico Nacional hay una filtración de algo que circula por una red, nos está ocurriendo lo contrario. En este momento tenemos ya cerca de doscientas sondas instaladas, y la lista de usuarios que vienen todos los días a preguntarnos si les podemos instalar una sonda es larguísima. Por tanto vamos a este segundo punto. Primero, legislar; segundo, crear confianza. El Estado y los instrumentos que el Estado tiene son precisamente para ayudar, y si necesitan algún elemento que lo diga de forma más clara es este: nadie quería que el CNI —en este caso el Centro Criptológico Nacional— le pusiera una sonda, y ahora en cambio ven las virtudes de tenerla.

El tercer elemento sin duda alguna es que esta división de funciones que en la Administración está declarada, escrita, reglada y se hace, se cumpla. Pero también las empresas y los ciudadanos tienen que hacer lo mismo. En la inmensa mayoría de los ataques, quienes los han sufrido y han visto que se ha producido algún daño en su empresa, lo ocultan porque creen que lleva consigo una pérdida reputacional. Y es por tanto difícil que una gran corporación que ha recibido un ataque lo declare. Esto es tremendo para los que nos tenemos que dedicar a protegerlos. Esto es como si a alguien le asaltaran en su casa y se lo ocultara a la Policía, a la Guardia Civil y a todo el mundo. Entonces, ¿qué vamos a hacer? Este es un tercer llamamiento a quienes están recibiendo de alguna forma los efectos de los ataques ciber para que no los oculten. Del mismo modo que en relación con el Centro Criptológico Nacional después de diez años ya es más que patente que de ahí no se produce ningún elemento informativo que pueda tener como efecto la pérdida de la intimidad de alguien, tenemos que decirles a los usuarios de Internet exactamente lo mismo. Díganoslo, que le queremos ayudar desde el convencimiento de que lo que nos diga nunca va a ser usado para que su reputación quede disminuida en el ámbito de la actividad que usted tenga.

cve: DSCG-12-CM-131

El cuarto y último es que también necesitamos alguna legislación internacional en la que apoyarnos. Es verdad que se ha incorporado la Directiva NIS, pero deberíamos hacer algo quizá con un poco más sentido de amplitud. Me explicaré. Los elementos que Naciones Unidas ha diseñado para reglar, no para impedir, porque eso es imposible, pero sí para reglar cuando se produce un ataque de un Estado a otro, han ido evolucionando con los tiempos. Las agresiones al inicio de la actividad de Naciones Unidas eran solo atribuidas a agresiones de tipo militar, de tipo bélico clásico, y la propia Carta decía los derechos que los Estados tenían ante una agresión de este tipo para poder reaccionar. Después vinieron las armas nucleares y la propia Carta de Naciones Unidas dice que, en caso de un ataque nuclear, declaran que es una agresión y también le da derechos a los agredidos para hacer algo ante ataques de este tiempo. Y lo mismo con armas bacteriológicas, químicas, etcétera. Podría ser momento de que en ese nivel y para ampararnos a todos que queremos legislar tanto a nivel nacional como de coaliciones, que alguien reconociera en el ámbito internacional de este nivel que las agresiones ciber son unas agresiones, es un acto de agresión como han sido otras y, en consecuencia, recoja también Naciones Unidas aquellos métodos, procedimientos e incluso derechos —creo que se puede decir— de los que puede gozar el agredido, porque el último elemento conexo con el anterior es la atribución de los ataques. Hay muchísima dificultad todavía hoy para atribuir los ataques. Se atribuyen en la inmensa mayoría de los casos sin el 100 % de exactitud en la determinación. Es verdad que para muchos —y esto es una idea que está creciendo en la comunidad internacional— si tenemos un 95 % de que ha sido usted el que me ha atacado, lo más probable es que usted lo sea, pero la realidad es que atribuir al 100 % los ataques es muy complejo. También quizá si se nos diera otro tipo de capacidades, pudiéramos atribuirlos.

No querría hablar mucho más. He traído tres o cuatro puntos como resumen. Naturalmente, estoy dispuesto a contestar cualquiera de sus preguntas, pero resumo simplemente estas tres o cuatro cosas que he dicho. Primero, España tiene un esquema nacional para protección de los españoles, tanto como individuos como empresas u otras actividades y a la Administración, de actividades ciber. Estas responsabilidades se han dividido en tres o cuatro partes y cada uno tiene su lugar en el que ejercerlas, pero hay un principio de coordinación y de dirección que se hace desde el Consejo Nacional de Ciberseguridad, dependiente del Consejo de Seguridad Nacional. Segundo, tenemos instrumentos suficientes, aunque la amenaza crece a cierta velocidad, para ir enfrentándonos con posibilidades de éxito. El éxito absoluto no lo garantiza nadie ni aquí ni en ningún lugar de la tierra, pero hasta ahora, atribuyan ustedes las razones que quieran, hemos sido capaces de que no afecte demasiado a España y a sus actividades los ataques ciber. En algunos casos incluso nos hemos podido poner al frente de las actividades para remediarlos. Tercero, necesitamos que todos confíen en nosotros. Ya sé que puede ser intrusivo entrar en su red para ver qué circula por ella, pero la razón para entrar únicamente es para poder protegerle a usted y a los demás. Finalmente, todavía se puede legislar algo más. Se ha adelantado mucho, pero se puede legislar algo más.

Para terminar, aunque no es de ciberseguridad, me permito decirles solo una cosa: no confundan la ciberseguridad —permítanme ustedes que lo diga en este tono, no quiero decir que estén confundidos— con el empleado desleal. En el 90 % de los casos son empleados desleales. El gran caso Snowden es un caso —no se sí será correcto decir empleado— de deslealtad. Aquí, en España, ha habido momentos críticos para empresas estratégicas que han sido también deslealtades de sus propios empleados. Por tanto, aunque sé que no es objeto de esta Comisión, pero quién sabe si en algún momento tendremos que reglar también, en el Código Penal o donde proceda, la regulación de los desleales, porque verdaderamente en la mayor parte de los casos y desde luego los que más daño han hecho no han sido ataques cibernéticos puros sino un desleal.

Creo que es mejor —y digo creo, pero estoy a su disposición— que sus señorías pregunten aquello que siempre le quisieron preguntar al director del Centro Criptológico Nacional y nunca tuvieron la oportunidad. En cualquier caso, estoy para dar respuesta a todas sus inquietudes y espero que les sea útil esta pequeña presentación del problema.

Muchas gracias.

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

Vamos a empezar el turno de portavoces. Intervendrán dos portavoces por el Grupo Mixto, el señor Xuclà y el señor Yanguas. A los dos les pido la continencia verbal a la que nos tienen acostumbrados.

cve: DSCG-12-CM-131

El señor **XUCLÀ I COSTA:** Muchas gracias, señor presidente, por invitarnos a la contención.

Señor secretario de Estado, una vez más es extraordinariamente interesante escucharle y poderle formular algunas preguntas sobre el particular. Ha hablado de la protección de este mundo presente en nuestras vidas y de los ataques en materia de ciberseguridad. Me gustaría empezar por lo privado y por los peligros de ciberataques en el ámbito privado, bien sea a título individual o bien sea en el ámbito del espionaje industrial, porque creo que también debe ser responsabilidad del Estado acompañar a aquellas empresas que sufren espionaje industrial y creo que en la red este es un campo de batalla importante en cuanto a proyectos e investigación, bien sea en el campo farmacéutico, médico o en el campo, por ejemplo, de la automoción.

Respecto a la ciberseguridad y lo público, usted ha hablado de la dificultad de la atribución de ataques de terceros porque a veces terceros actores estatales pueden encargar estos ataques a personas o grupos y de ahí esta dificultad de imputación de ataques de terceros. Bien, si hay datos del 95 o del 96 %, no sé si usted puede perfilar el mapa de los países o de los Estados que encargan por delegación estas injerencias. Me gustaría saber, porque ha habido mucha literatura de la buena y de la mala, si en los últimos procesos electorales en España en los últimos años se han producido injerencias de países terceros o de particulares con un alto grado de probabilidad de ser invitados por países terceros. No sé si soy suficientemente claro o diplomático o se me entiende. También me gustaría saber si un caso que está en la esfera de las empresas privadas, como Cambridge Analytica, ha tenido algún tipo de penetración o de posibilidad, porque estamos hablando de una empresa privada y del manejo de datos de ciudadanos que estamos en la red en el ámbito de la influencia y de la conducción de usos de consumo o políticos en España.

Le quería preguntar también si se debe legislar. Usted en parte ya nos ha respondido, cuando dice que una *tablet* tiene cero reservas de protección, quizás el dedo —por cierto, yo tengo hijas gemelas univitelinas y las dos pueden abrir con los ojos el móvil la una de la otra— o las huellas dactilares, aunque usted seguramente nos está hablando de cosas más sofisticadas. También nos ha hablado de la vacuna de WannaCry y de su éxito. Creo que casi nos ha invitado —a mí o a otros portavoces— a que le formulemos la pregunta. Si España fue tan eficiente en la fabricación de la vacuna de WannaCry es porque alguien la fabricó y debía ser alguien que conocía bien los fondos de la red, y supongo que al final algún *hacker* también tiene que pasar al lado bueno de la seguridad para ayudar y dar respuesta a la seguridad. ¿Quién la fabricó? ¿Quién tuvo la capacidad de esta reacción, que incluso fue utilizada por tres países, según nos ha dicho? Nos ha hablado de 38 000 incidencias en este año; supongo que muchas de estas son en el ámbito privado. Ha apuntado un aspecto que me parece importante, que es cuando a los privados les da vergüenza denunciar que han sido vulnerados en su privacidad en la red y cómo esto se puede revertir. Finalmente, ha apuntado algo que existe en todas partes, que son los empleados desleales en las filas de la seguridad y también en las filas de otros ámbitos de actividad.

Muchas gracias, señor presidente, porque debo compartir el turno —y creo que lo he hecho disciplinadamente— con mi colega de grupo.

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

Señor Yanguas.

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

Muchas gracias por su comparecencia y bienvenido al Congreso de los Diputados, señor secretario de Estado director del Centro Nacional de Inteligencia.

Preguntas, dudas, me asalta muchas, muchísimas, lo que ocurre es que ya nos ha advertido el presidente de la Comisión de que algunas no se las podríamos preguntar, con lo cual antes de que él no me las autorice le voy a ahorrar ese trabajo y esas no se las voy a hacer. Sí que le haré una pregunta que me ha surgido al hilo de su comparecencia: ¿Cómo es la colaboración de las Fuerzas y Cuerpos de Seguridad del Estado en este tema, sobre todo con un cuerpo policial como es la Policía Foral de Navarra? No se lo he dicho, aunque usted como persona mejor informada de España lo sabrá, que soy senador de Unión del Pueblo Navarro. ¿Cómo es esa coordinación? ¿Puede arrojar usted alguna luz sobre eso? Entiendo que será una colaboración fluida, pero me gustaría conocer algo más. Por lo demás, en su comparecencia me ha parecido que nos ha aclarado muchas cosas que podrán venir bien para esta Comisión y creo que será positivo.

Muchas gracias.

cve: DSCG-12-CM-131

El señor **PRESIDENTE:** Gracias, señor Yanguas.
Señor Legarda.

El señor **LEGARDA URIARTE:** Muchas gracias, presidente, y muchas gracias también a nuestro compareciente, el director del CNI.

Mis cuestiones girarán sobre dos ejes, uno sobre el esquema de protección de redes y sistemas, y otro sobre los instrumentos. Sobre redes y sistemas se ha traspuesto recientemente la Directiva NIS a través de un decreto-ley que íbamos a tramitar luego como ley, pero no sé si nos va a dar tiempo a efectos de enmiendas. Nosotros votamos a favor de la convalidación del decreto-ley, pero manifestamos ciertas observaciones, sobre todo —y esta va a ser mi pregunta— porque considerábamos que así como en infraestructuras críticas, protección de datos y trasposición de reglamento europeo se había trabajado en esquemas de colaboración entre las distintas administraciones públicas competentes, la trasposición de la Directiva NIS se había hecho —desde nuestro punto de vista— desde una arquitectura jerárquica. Es decir, era el CNI, a través del Centro Criptológico Nacional, o era el Ministerio del Interior para el sector público, para el sector empresarial —en este caso era de las comunidades autónomas y hablábamos, en nuestro caso, del País Vasco—, lo que mostraba una gran desconfianza, porque no se nos reconocía una capacidad de trabajar en red en el sistema y se nos ponía en los aspectos de prevención, detección, neutralización y resiliencia o bien en el CNI, en el Centro Criptológico Nacional, o en la secretaría de Estado. Nosotros discrepábamos de esta arquitectura; creíamos que, lo mismo que en infraestructuras críticas, podíamos tener nuestros centros CSIRT certificados y establecer una leal colaboración, porque, no nos podemos engañar —usted lo ha dicho al final, en ese epílogo que ha hecho—, es entrar en la red sólo para defender. Usted comprenderá, porque estamos donde estamos y vivimos en el mundo en que vivimos, que nos digan que el CNI o la secretaria de Estado va a entrar en nuestra red —y no voy a poner situaciones o ejemplos recientes que ha vivido y está viviendo este país— de hecho suscita una gran suspicacia, cuando la alternativa era: vamos a funcionar todos con los mismos estándares, yo hago la inspección de mis propios sistemas con unos estándares homogéneos y establecemos la colaboración. En definitiva, centros habilitados. Mi pregunta es: ¿considera usted que una arquitectura más en red, con centros de decisión —claro, también con responsabilidad—, en distintos nodos sería más eficiente que una estructura en redes y sistemas como por la que ha optado el Gobierno del Estado y, en este caso, el decreto-ley que, desde nuestro punto de vista, es una arquitectura más jerárquica?

La segunda cuestión que le quería plantear es sobre las herramientas. Creo que el gran problema que vamos a vivir —y que ya vivimos, porque nos estamos metiendo de lleno— en el mundo de los datos es que plantean una gran superficie de abordaje, necesidad de respuestas en tiempo real y muchos centros de decisión y eso, al final, no lo podemos gestionar los humanos, lo gestiona la inteligencia artificial, que en realidad son programas que van respondiendo ante incidentes que se le van planteando a modo de árbol, respuestas binarias. Si pasa esto, hago esto; si pasa lo otro, hago lo otro. Esa es la inteligencia artificial, que todavía no es de propósito general pero que tiene capacidad de aprendizaje para, ante situaciones nuevas, con los datos que tenía como un pixelado interpolar una realidad. Yo le preguntaba sobre el gran problema de las herramientas que es la inteligencia artificial y lo que se llaman los sesgos en la inteligencia artificial, bien sesgos maliciosos o sesgos del programador de los datos que se introducen no maliciosamente pero que pueden dar situaciones caóticas, porque ya no controlamos cómo van a funcionar esos programas. Creemos cuando los diseñamos que van a funcionar de una manera, pero muchas veces no sabemos cómo funcionan. Al final, de igual modo que la mayoría de los ataques son con inteligencia artificial porque son ataques robotizados con algoritmos, la defensa es también artificial, con inteligencia artificial. Mi pregunta es qué criterios siguen ustedes en la adquisición de estos programas de inteligencia artificial para la defensa en cuanto al control de los sesgos. En Naciones Unidas y en el Parlamento Europeo se está considerando que los algoritmos tienen capacidad de incidir en los derechos humanos. Recientemente, se ha creado una agencia —sé que lo digo incorrectamente, pero no me sale la palabra—, la IA4 de la Unión Europea, que es un órgano que va a certificar los algoritmos que se fabrican en Europa o que se adquieren en Europa a fin de que no incidan en nuestros valores. Es una regulación más allá de la regulación de la Unión. Me gustaría saber qué grado de conexión tienen ustedes con ello o si están incorporados a este programa de la Unión, el IA4.

Muchas gracias, presidente.

cve: DSCG-12-CM-131

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

Le aclaro que hace quince días hubo una sentencia del Tribunal Constitucional ratificando la naturaleza de competencia exclusiva del Estado relativa a las materias a las que usted se refiere.

Tiene ahora la palabra el señor Salvador.

El señor **SALVADOR GARCÍA:** Gracias, señor presidente.

Bienvenido, general don Félix Sanz. Es un placer contar con usted en esta Comisión. Ya lo hemos dicho en varias ocasiones, han comparecido ya muchísimas personas, todas especializadas y con una visión muy importante que aportar, y usted ha dado una visión global que, a mí personalmente, me transmite una cierta confianza; digo cierta porque no todo depende, como muy bien ha dicho, de ustedes, sino también de la parcela exterior. Entre otras cosas, porque ha puesto encima de la mesa cuestiones que en el transcurso de todas estas comparecencias hemos puesto nosotros con otros comparecientes como, por ejemplo, en relación con Naciones Unidas y en los conflictos entre Estados, que tendría que existir algún tipo de acuerdo internacional que estableciera qué es una agresión, quién es el agredido, quién es el agresor y qué medidas se pueden tomar, porque si no, esto sale gratis, que es el problema que sucede hoy. También ha puesto de manifiesto algo que para nosotros es muy importante y son los elementos de legislación que tienen que ver con el usuario final y con el uso de los elementos que le conectan al Internet de las cosas y la utilización de nuestro mundo digital. Las personas se conectan y navegan por la red, pero también usan aplicaciones, terminales y dispositivos que tienen fabricantes que, en todos los casos, te convierten después a ti en propietario. Es la primera persona que ha comparecido que ha puesto el foco en este sentido que estábamos hablando. Resalto esto porque usted desempeña la responsabilidad que tiene y, por tanto, es muy importante que esto se entienda. Quisiera preguntarle también —no le voy a preguntar por la fecha de las elecciones ni nada de eso— **(risas),** porque ha salido publicado recientemente, por la Oficina de Inteligencia Militar, que se ha dicho que podría estar para 2020, si tiene algo que ver también con la parte del mundo ciber y cómo iría eso.

Dentro de todo lo que usted ha comentado, es verdad que en este momentos estamos preparados para la dimensión que tienen las cosas en el presente, que estamos dando buena respuesta porque nos hemos preparado antes, que estamos bien organizados, que tenemos profesionales y nuestra estructura está respondiendo, pero también en esta Comisión se ha puesto sobre la mesa uno de los elementos fundamentales, que lo voy a ligar con otro elemento más. Por una parte, estamos en una transición todavía al mundo digital. Esa transición no se desarrollará completamente —y lo que estoy diciendo no es un deseo de este portavoz, constato una realidad— hasta que no afecte absolutamente a todo en nuestra vida; el mercado laboral, que es el que más preocupa y el que más nos tiene que ocupar en este momento y, al mismo tiempo, con todas las ventajas que puede conllevar el mundo digital y las facilidades que nos pueda otorgar, pero también con los nuevos riesgos. Respecto al *big data,* los datos, hoy mismo leía una noticia en la que se decía que en una serie que se está emitiendo ahora en Netflix que habla sobre el mundo presente y futuro, los usuarios podían dar distintas posibilidades a la hora de ver qué trayecto seguía la serie y que todo eso se había almacenado y guardado. Todos los datos que tienen las redes sociales son datos personales. Por mucho que la gente dé a «aceptar» en la cláusula —porque si no, estoy fuera de la red o no la puedo utilizar—, si a un usuario le dan dos millones de páginas para leerlas y o estás de acuerdo o no estás en Facebook o la que sea, es obvio que todo el mundo va a dar a «aceptar» sin mirar porque es lo que hay. Esa aceptación implícita por parte de los ciudadanos no lleva a una lectura real de saber qué sí o qué no, sino a estás dentro del mundo o estás fuera. Esa acumulación de datos y esa inteligencia artificial, que puede tener un buen uso, también es programada en cierta medida para tomar sus decisiones. En relación con esto, quiero preguntarle de forma genérica por el tema de las *fake news*. Podemos personalizar los datos de las personas, qué productos les gustaría consumir, qué cosas les gustaría tener, qué cosas les parecen mejor o peor y, al mismo tiempo, tenemos la capacidad para construir herramientas de comunicación que distorsionen la realidad con medias verdades o con medias mentiras bien fabricadas y que eso afecte a la sociedad, y se ha visto en grandes procesos en el mundo, por lo que la gente ha tomado conciencia. Pero además de esos grandes procesos que pueden cambiar en un momento determinado una opinión pública, también están los procesos de los ciudadanos cotidianos, que día a día están recibiendo un tipo u otro de información. Quisiera saber si están profundizando un poco en esto que es tan complejo de resolver —y más con la cantidad de comunicación que existe en este momento y la cantidad de emisores de comunicación de las distintas credibilidades de las fuentes—, si han abierto alguna vía para detectar qué cosas pueden afectarnos como sociedad. Es

cve: DSCG-12-CM-131

más, si estamos viendo con el VAR que la interpretación, aun con tecnología, genera controversia y problemática, esto, evidentemente, genera más.

Para terminar, estamos organizados en este momento, pero, ¿tenemos los medios suficientes? Digo esto porque en el mundo analógico, por diferenciarlo del digital, todos sabemos que tenemos un ejército, un Ministerio de Defensa, una estructura, las Fuerzas y Cuerpos de Seguridad del Estado, el CNI; todos lo sabemos. Todo esto ocupa la gran mayoría de los recursos que se necesitan porque ahí no pueden faltar. Pero estamos hablando de que donde los malos van a buscar el dinero, donde van a efectuar sus actuaciones es donde está el dinero, es decir, al final va a ser en Internet. ¿Estamos dotándonos y somos conscientes como Estado de la importancia que tiene derivar los fondos necesarios para proteger a nuestras empresas? Nosotros entendemos que puede ser una inversión, o sea, que después evite costes muchísimo más altos. Quisiera saber si podemos hacer algo más para que los medios con los que cuentan y con los que tienen que contar son los adecuados. Finalmente, me gustaría que me dijera qué opina sobre la formación en todos estos aspectos desde la universidad y desde más ámbitos, es decir, una parte educación en valores, también asociada al mundo digital para que la gente sepa prevenir o qué cosas pueden suceder y así atajarlas, como sucede con la seguridad vial o con cualquier otra, pero orientado a la red. Por otro lado, estamos tirando mucho de los grandes *hackers,* de la gente que consigue demostrar que desmonta sistemas. ¿Estamos preparados en este momento para preparar a personas que contribuyan a que no se puedan desmontar sistemas?

Muchas gracias.

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

Señor Mayoral.

El señor **MAYORAL PERALES:** Gracias, señor presidente.

Agradezco al secretario de Estado su presencia en la Comisión. Siempre es un placer poder escucharle y también haber podido ver el video informativo del principio. Creo que sería interesante que se facilitara a los miembros de la Comisión —si no hay ningún problema— porque, a pesar de que es dinámico, incluye información que creo que es interesante para los miembros de la Comisión porque traza algunas líneas estratégicas de cuáles son los puntos de defensa para los problemas de ciberseguridad.

Mi grupo quiere referirse a uno de los casos que ha comentado en su intervención, el caso del WannaCry. Quisiera saber si puede darnos información de si existen estimaciones del impacto económico que tuvo el ataque en nuestro país. Tanto el Gobierno anterior como usted en su intervención nos han manifestado que los impactos en nuestro país fueron menores que los sucedidos en otros países. Le rogaría que nos pudiera facilitar algún tipo de dato económico sobre el impacto que pudo tener en nuestro país e incluso sobre si hay algún tipo de comparativa respecto de otros países.

Tenemos algunos datos, que usted ha facilitado también, por una parte, en cuanto al aumento de los ciberataques y, por otra, de los ataques a las infraestructuras críticas. Voy a plantear una serie de preguntas por si pudiera ilustrarnos a la Comisión. La primera es especialmente genérica: ¿Cree que nuestro país está preparado para poder afrontar estos ataques a escala mundial? Asimismo, querríamos saber si son ciertas las afirmaciones —supongo que nos dirá que la suya sí— de que ha sido escaso el impacto en nuestra economía y, en ese caso, sobre si fue grave o no el impacto y nos puede facilitar algún tipo de cifra. Querríamos saber también cuáles son los efectos que han podido tener estos ataques durante estos últimos años en España, si hay alguna estimación general sobre el impacto económico de estos ataques a la economía española y cuánto han repercutido estos ataques en los consumidores, no solamente las organizaciones; es decir, hemos visto quizás una orientación muy centrada en el impacto que tiene en las organizaciones, pero nos gustaría conocer el impacto que ha tenido en los consumidores y en la población en general. Querríamos que nos ilustrase sobre cuáles son los mecanismos adoptados por el actual Gobierno relativos a la concienciación, prevención, detección, reacción, análisis, recuperación, respuesta e investigación sobre estos incidentes que se han podido producir en los últimos tiempos.

Tenemos especial interés en que pueda ilustrarnos sobre la utilización generalizada de *smartphones,* amén de la utilización de los correos electrónicos de forma masiva, la conexión vía red de diferentes dispositivos, que van desde el Internet de las cosas a lo que viene a ser la conexión vía wifi de múltiples cámaras, de organismos públicos y organismos privados, al igual que nos informase acerca de la detección que ha realizado su centro sobre la intervención ilegal de comunicaciones en nuestro país, si las ha habido y cuántas, si tienen algún tipo de datos, y cuántas personas, grupos u organizaciones han sido puestas a disposición judicial por realizar intervenciones ilegales. Quisiera que nos informara sobre

cve: DSCG-12-CM-131

qué vulnerabilidad existe en estos momentos por el desarrollo de la cibernética en torno a la capacidad de intervenir comunicaciones porque hay una diferencia obvia entre la intervención ilegal de comunicaciones entre el momento en que había comunicaciones analógicas al momento actual. Tenemos especial interés en que nos pueda informar respecto de ataques a la ciberseguridad, en concreto del Ministerio del Interior, de las Fuerzas y Cuerpos de Seguridad del Estado, es decir, si se han producido intervenciones ilegales en las comunicaciones de las Fuerzas y Cuerpos de Seguridad del Estado por parte de organizaciones criminales para eludir la acción de la justicia. Asimismo, queríamos saber si ustedes han evaluado el impacto que ha podido tener, se ha comentado antes, la actuación de diferentes organizaciones criminales u organizaciones ilegales que hayan querido intervenir en diferentes procesos electorales. Quizá el último, el más reciente, y donde han existido y existen procedimientos judiciales al respecto, lo hemos podido ver en la campaña brasileña, en concreto con la participación en esa campaña de dispositivos controlados y coordinados desde Estados Unidos con terminales norteamericanos para lanzar mensajes, y en concreto *fake news*, desde esas redes con sede en los Estados Unidos y la capacidad de los Estados para poder defenderse partiendo de que las dificultades en la investigación que se están produciendo en este momento en Brasil proceden fundamentalmente de que esos terminales que emitían de forma masiva esos mensajes no pueden ser perseguidos en la medida en que se encuentran en otros países y si ha habido análisis por parte de Centro Nacional de Inteligencia respecto a estos hechos, que a mí me parecen de excepcional gravedad en la medida en que pueden afectar de forma importante a los procesos electorales y entendiendo, además, que algunas de estas cuestiones se encuentran *sub iudice* en países con los que mantenemos relaciones de amistad.

Desde ese punto de vista, nos gustaría que pudiera ilustrarnos sobre cuáles son los mecanismos que se articulan desde el Estado para la protección de la privacidad de las comunicaciones del conjunto de la población de nuestro país, de las organizaciones, de los centros críticos y también cuál es la coordinación que existe desde el Centro Criptológico Nacional con las Fuerzas y Cuerpos de Seguridad del Estado. En ese sentido, nos parece importante que nos pueda dar su opinión respecto de la relación que existe entre todo lo que son los mecanismos de defensa frente a los ciberdelitos y el Poder Judicial y, en concreto, en ese Consejo Nacional de Ciberseguridad, cuáles son los mecanismos de coordinación con el Poder Judicial porque, evidentemente, ante los ilícitos, en un Estado de derecho es precisamente el Poder Judicial —voy terminando ya, presidente— el que tiene la última palabra para declarar la ilicitud o no de las conductas y para evitar la posibilidad de que existan esferas de impunidad en el Estado de derecho.

Muchísimas gracias.

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

Tiene la palabra el señor Hernando.

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

Buenos días y muchas gracias al director del CNI, general Félix Sanz Roldán.

Sabe usted, general, que hoy terminan las comparecencias en esta Comisión y de alguna manera su comparecencia era y es para la Comisión un colofón y, digamos, un broche de oro a una serie amplia de comparecientes que nos han estado ilustrando en los trabajos que tiene que seguir haciendo esta Comisión de cara al informe final y a las recomendaciones que tiene que hacer. En este sentido le agradecemos especialmente su comparecencia hoy para poder cerrar, creemos que más adecuadamente, los trabajos de la Comisión. Perdóneme por reiterarme en algunas de las preguntas que le han hecho, en todo caso intentaré hacerlo muy brevemente. Voy a seguir el esquema de trabajo que siguen en los excelentes informes que tienen colgados en la red, que están sin clasificar y en los que hay cifras de todo tipo y respecto de todo tipo de casos y con muchísima transparencia, he de decirlo. *Ciberamenazas y tendencias*, edición de 2018; la ejecutiva de octubre de 2018 o también la de 2017. Aquí lo dicen casi todo y está casi todo, si bien, a pesar de eso, quiero incidir especialmente en algunos aspectos. Influencia en la opinión pública, que es el informe de 2018, *Ciberamenazas y tendencias,* edición de 2018. Ataques a la CDU, a En Marche y al Partido Demócrata y al Partido Republicano en los Estados Unidos. ¿Han tenido o tienen constancia o han detectado acciones similares en España respecto de formaciones políticas? ¿Están tranquilos respecto de esta cuestión?

Segundo tema. El papel de los agentes estatales como promotores o amparadores de este tipo de actuaciones de influencia en la opinión pública, del que también se habla en el informe, aunque me gustaría que nos pudiese ampliar el tema, si es posible. ¿Cómo defendemos a las democracias de este tipo de actuaciones? ¿Qué estrategia tienen diseñadas el centro y el consejo para defender la democracia

cve: DSCG-12-CM-131

española? En este caso de este tipo de actuaciones, que no dejan de ser graves, especialmente ante el año que tenemos, que es un año necesariamente electoral porque hay elecciones el 26 de mayo, al menos. ¿Podemos estar tranquilos en cuanto a que en los próximos procesos electorales, y ese día hay varias convocatorias de ámbito nacional, no haya interferencias? Como usted dice, el riesgo cero no existe, pero tenemos las suficientes herramientas y hemos trabajado lo suficiente como para que no haya interferencias en esos procesos electorales o para que no haya intentos de persuadir malignamente a la opinión pública y digo entrecomillas lo de malignamente.

En cuanto a las *fake news,* de las que le he escuchado hablar en varias ocasiones en distintas conferencias, el mensaje es que se pueden hacer muchas más cosas en el ámbito de la seguridad para que las *fake news* se puedan descubrir y contrarrestar. Díganos alguna o algunas. Esto es importante y en la Comisión ha salido reiteradamente, como le habrán dicho, pero usted lo ha contextualizado bien y ha dicho que no es una guerra y que hay exageraciones respecto a este tema. Ha dicho que no se trata de una guerra, que no exageremos. Pongámoslo en su justa medida.

Me parece importante, y usted lo ha dicho, cómo reaccionar a los ciberataques. Sabíamos cómo teníamos que reaccionar ante un ataque con armas convencionales, pero no cómo reaccionar ante los ciberataques. ¿Han avanzado un poco más en qué tipo de legislación se podría hacer a nivel nacional e internacional en este tema? ¿Hay algún avance mayor sobre cómo reaccionar, sobre si nosotros podemos utilizar nuestra fuerza ciber para reaccionar frente a los malos? Me refiero no ya a cuando sean agentes estatales terceros, sino cuando sean simplemente terceros que estén en determinados ámbitos.

Por último, el pasado mes de julio se reunió el Consejo de Seguridad Nacional, presidido en este caso por el jefe del Estado y por el presidente del Gobierno. Se encargó una nueva estrategia de ciberseguridad, la que tenemos es de 2013; no hay que alarmarse porque la que tiene Alemania es de 2011. Cierto es que hay países que tienen una estrategia de 2017 e incluso 2017-2021. Simplemente le pregunto en qué fase está ahora mismo el proceso de elaboración de esa nueva estrategia de ciberseguridad que fue encargada el pasado mes de julio en ese consejo. Después de poco más de un año en vigor del acuerdo para el esquema del nuevo Consejo Nacional de Ciberseguridad, esto es del 22 enero 2018, como han evolucionado tanto las cosas, ¿cree usted que es necesario algún ajuste como consecuencia de dicha evolución? Esto tiene que ver también con lo que le decía el señor Legarda del esquema. Usted ha dicho que es más fácil partirlo en cuatro trozos y coordinarlo. ¿Sigue eso siendo así? Hay algunos profesionales aquí que nos han dicho que no es buena la compartimentación pero a lo mejor por motivos de especialización esto es algo absolutamente necesario en este caso.

Permítame, señor presidente, antes de terminar —como no sé si habrá nueva oportunidad de decírselo al general Sanz Roldán en esta Comisión—, que felicite en nombre de mi grupo a él y a los agentes a su mando por el trabajo y el servicio que viene prestando para la seguridad de este país como garantía de los derechos y las libertades de los ciudadanos.

Gracias.

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

Señor Mateu.

El señor **MATEU ISTÚRIZ:** Buenos días. Muchas gracias, señor presidente.

Mi general, señor Sanz Roldán, secretario de Estado, muchísimas gracias por su presencia. Ha sido brillante en su exposición. Ha entrado en lo que ha podido usted hablar, porque usted es de las personas de las que se puede decir, en términos coloquiales, que más vale por lo que calla que por lo que dice. Evidentemente, debido a su gran currículum los servicios de información e inteligencia españoles están en buenas manos. Porque no hay que olvidar todos su currículum, las fases por las que pasó en su vida y que ha estado en todas las actividades y estamentos, desde el militar, seguridad exterior, ahora mismo en inteligencia. Además, hay que recordar, para todavía asentar más que la inteligencia española está en buenas manos, las leyes que se promulgaron bajo su mandato como Jemad. No hay que olvidar que se fundamentó la Directiva de Defensa Nacional, la Ley de Defensa Nacional, la Ley de tropa y marinería y también se creó una unidad fantástica, como es la UME, y también se creó el Cifas, que es el Centro de Inteligencia de las Fuerzas Armadas.

Quiero recordarle una frase para ilustrar mi exposición que precisamente aparece en la página web del CNI, que se atribuye a Sun Tzu y que dice: Conoce a tu enemigo y conócete a ti mismo; lograrás cien victorias en cien batallas. Evidentemente, eso es lo que con su actuación se pretende y lo que pretende contando con la colaboración del CNI el Gobierno de España y, sobre todo, el ciudadano español que

cve: DSCG-12-CM-131

confía plenamente en la inteligencia española. Ha hablado usted, además de los medios técnicos, de los medios humanos, que son evidentemente la base del éxito de la actuación del CNI y de que los españoles confiemos y podamos vivir en libertad. No quiero que dejar en el olvido a esos siete héroes asesinados el 29 de noviembre del año 2003 en una emboscada en Latifiya, en Irak. También quiero recordar con especial cariño a un comandante de la Guardia Civil, a Gonzalo Pérez García, que fue asesinado el año siguiente en Diwaniya, en Hamza. Precisamente ustedes luego estuvieron investigando las causas del fallecimiento de este comandante. Mi recuerdo emocionado y el del Grupo Parlamentario Popular para todas las personas que, en aras de la libertad y por la patria, entregaron sus propias vidas.

Yo no quiero entrar en recordarle lo que usted nos ha contado y tampoco lo que hemos visto perfectamente en el plan para presentar una estrategia de seguridad nacional, en el informe anual de seguridad nacional del año 2017, que es el último que ha sido presentado y que ha sido perfectamente estudiado por el Grupo Parlamentario Popular. Tampoco voy a entrar a recordarle cuáles son los problemas que acucian más ahora mismo en materia de actuación del CNI, aparte de la ciberdefensa, como es el terrorismo transaccional, las amenazas híbridas que restan libertad de movimiento y de actuación a la sociedad española, y los flujos migratorios, así como el riesgo, porque ustedes también tienen que proteger las operaciones militares exteriores que se realizan por parte de nuestras Fuerzas Armadas, y evidentemente las *fake news,* que generan un desasosiego en cuanto a su actuación en elecciones y en otros supuestos que intoxican a la sociedad y que hacen perder confianza y seguridad.

Podría hablar de muchas cosas, porque la seguridad es un tema apasionante y prioritario para los españoles. Aquí podemos construir carreteras, podemos construir hospitales —que, evidentemente, recuperen y den la vida—, podemos hacer lo que sea, pero el español, al salir a la calle o en su cotidianeidad y su quehacer diario desde que coge un *smartphone* por la mañana hasta que se acuesta —lo que conduce absolutamente nuestra vida—, necesita garantía en eso. Sin esa garantía de seguridad no se da lugar a que podamos vivir en libertad. Por eso le quiero hacer una serie de preguntas que pueden esclarecer perfectamente y garantizar —algunas más que otras— esa libertad y seguridad de la cual quieren gozar los ciudadanos españoles. Así, aunque usted ya lo ha mencionado, voy a empezar por la primera pregunta. ¿Podría darnos del número e importancia de los ciberataques realizados contra administraciones españolas a lo largo del último año? Ha hablado de que en enero hubo 4000 incidencias y de que en el año 2018 hubo 38000 incidencias. De esas, ¿cuántas más o menos, en porcentaje, han afectado a administraciones públicas? En cuanto al tema de recursos humanos, ¿podría darnos razón sobre si los recursos de talento, de captación de la mejor gente y de gente formada que manejan las administraciones públicas para su autoprotección y coordinación con el CCN-CERT —como CERT que son ustedes de referencia— son adecuados? ¿Hay alguna sugerencia que pueda hacer usted para mejorar los procesos de detección temprana, reclutamiento, formación y retención del talento acerca de la materia que usted coordina dentro del seno de las administraciones públicas? ¿Qué impacto ha tenido el Real Decreto 12/2018 que transmutó la Directiva NIS, afección sobre sus propios recursos en su labor de CERT de referencia para las administraciones públicas? ¿Podría valorar el posible impacto que está recogido en el artículo 20 del real decreto-ley citado de la figura del filtrador, sobre posibles incomplementos normativos en materia de ciberseguridad en las administraciones públicas? Le voy a formular una pregunta que ya ha sido reiterada, ¿podría darnos algún detalle relacionado con campañas ejecutadas por cualquier actor del ciberespacio: Estado, organización o grupo organizado de desinformación contra nuestro Estado? ¿Qué posibles contramedidas nos sugiere, como legisladores, para que hagamos en materia legislativa, a pesar de que ha mencionado usted que hay que reforzar fundamentalmente la actividad legislativa internacional derivada de la obsolescencia de la Carta Internacional de Naciones Unidas? Háganos una glosa, si es posible, de la cultura de la inteligencia para seducir todavía más a los ciudadanos sobre que su actuación no es una injerencia en su vida cotidiana. Me gustaría que nos hablara de la cobertura jurídica de la cual disponen ustedes para sus propias actuaciones, algo muy importante que ha salido a colación, en cuanto a la interceptación de llamadas, registros domiciliarios y otra serie de actuaciones que ustedes realizan. Una pregunta que no es capciosa pero de la que se ha hablado en muchas ocasiones, ¿La actuación del CNI genera Estado dentro de otro Estado? ¿Qué tipo de ayuda efectúan ustedes a empresas que o bien se quieren desarrollar en el extranjero o bien ya existen y quieren desarrollarse allí? A pesar de lo que ha establecido sobre que lo que crean ustedes es lo más seguro, ¿la ciberseguridad, a su juicio, es una opción que usted considera para el desarrollo industrial, económico y social? Voy terminando, señor presidente. ¿Podemos asociar la calidad de los productos —ahora mismo se demanda más la seguridad— a la colaboración público-privada en el ámbito de la protección a la

cve: DSCG-12-CM-131

ciberseguridad? También quisiera que nos hablara sobre la ciberreserva, es decir, gente preparada y capaz que está dispuesta a colaborar con ustedes en momentos de gran crítica.

Por último, supongo que usted tiene conocimiento de lo que ayer hoy en una emisora de radio y que esta mañana ha sacado una noticia de Europa Press que dice: *Hackean* los datos de los ministerios de Hacienda y Justicia para denunciar su falta de seguridad a través de un grupo de *hackers* que se denomina Digital Research Team. **(Muestra una fotocopia).** Dicen que ha sido un *hackeo* ético para advertir sobre las vulnerabilidades. Han entrado en once universidades públicas españolas, en otras instituciones como ayuntamientos, en sindicatos como Comisiones Obreras, en algún Gobierno como el de Perú, y además, han digitalizado parte de los DNI de directivos políticos como Albert Rivera, Carlos Carrizosa y el ministro de Fomento, el socialista José Luis Ábalos.

Es todo. Le agradezco mucho su presencia en esta mañana de hoy.

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

Señor secretario de Estado.

El señor **SECRETARIO DE ESTADO DIRECTOR DEL CENTRO NACIONAL DE INTELIGENCIA** (Sanz Roldán): Muchas gracias a todos, porque sus intervenciones dan muestra de un altísimo interés en este asunto. Lo que pretendo es dar una respuesta general y que en ella estén contenidas todas sus inquietudes. Naturalmente, si no es así, me lo pueden advertir y volveré sobre el asunto, porque la lista de preguntas es amplísima y a ver cómo las cuadro todas.

Empiezo con una del señor Xuclà, que ha hablado de privacidad. La privacidad, más que en otra cosa, está en nuestras manos. Como se ha dicho, nos ponen las condiciones en las que queremos bajar a nuestro teléfono móvil o a nuestro ordenador una determinada aplicación. Respecto a esto les voy a contar una anécdota. Una organización italiana hizo una web que parecía que era de contactos, pero lo que pretendía era ver hasta qué punto entregamos nuestra intimidad al primero que aparece. La web de contactos tenía unas condiciones para acceder a ella y decía: si usted entra aquí, yo podré vender su alma al diablo. Y en la primera hora 7500 personas dijeron que sí. **(Risas).** Por tanto, hay que tener un poco de cuidado. Sé que esto es muy complejo. Yo hablo con mis hijos, que como es lógico son mucho más jóvenes que yo, y me dicen: y a mí qué me importa, nadie tiene interés en mí, qué más da; sin embargo, a mí me viene muy bien saber qué tiempo hace en Tegucigalpa porque viajo allí una vez cada doscientos años. ¡Por Dios! Cuanto más convertimos nuestro teléfono en ordenador, más indiscreto es. Es el uso de nuestro libre albedrío. Si queremos que todo el mundo sepa todo, pues estupendo, pero también tenemos que estar seguros de que, cada vez que aceptamos las condiciones de uso de una aplicación, estamos aceptando otras cosas más, entre otras y muy importante el comercio de nuestros datos, que es una situación que en algún momento habrá que poner en sus justos límites. ¿Por qué en este momento en cualquier proveedor móvil de telefonía es gratis la palabra? Porque la palabra no interesa, lo que interesa son los datos, y con los datos se comercia y se saca mucho dinero. El presidente de una multinacional española decía: si un producto es gratis para ti, es porque tú eres el producto. Y eso es una realidad y la habrán visto sus señorías un millón de veces. Yo una vez iba a hacer un viaje muy raro, en agosto, y como ya tengo poco pelo creí que se me iba a quemar la cabeza y quise comprarme un sombrero. Estuve un año recibiendo información de sombreros nada más abrir mi ordenador. Y lo mismo ocurre si se escucha una determinada música. Eso todos ustedes lo saben. Por tanto, efectivamente la privacidad es una cuestión muy compleja, pero también es verdad que sobre ella nosotros podemos hacer más cosas de las que hacemos. El caso más notable de esto —nadie se lo cree, espero que sus señorías me crean— es el que les voy a contar. Una señora norteamericana supo que estaba embarazada por una felicitación de la cadena Walmart antes de que tuviera un informe médico o un dato de los que usen las señoras para saber si estaban embarazadas o no, que desconozco. Hasta ese punto estamos llegando. ¿Por qué? Porque entregamos todo a la red y lo hacemos de forma libre, porque nadie nos obliga a entregarlo, pero lo entregamos. Por tanto, ahí está nuestra libertad, en saber hasta dónde podemos llegar.

Espionaje industrial, claro que lo hay y mucho. Una de las primeras cosas que me encontré cuando llegué al Centro Nacional de Inteligencia es que todo el proyecto para fabricar un coche eléctrico en España se había llevado a un tercer país, donde ya se estaba fabricando en los mismos días en que se iba a hacer una presentación oficial de la intención de una determinada empresa española de fabricar ese vehículo eléctrico. Esto ocurre con mucha frecuencia y llega hasta tal extremo que tenemos una definición específica para esto y un grupo específico de trabajo para espionaje industrial, porque hay una potencia que precisamente se dedica a esto. En el mundo de la ciberseguridad básicamente hay dos grandes

cve: DSCG-12-CM-131

campos: los que quieren obtener información sin dedicarse a grandes procesos de I+D+i —dicen: vemos cómo lo hacen y yo luego se lo robo— y los que quieren desestabilizar nuestro sistema de vida. Esos son los dos grandes grupos y de ellos hay uno que es singularmente eficiente en llevarse los resultados de los grandes procesos de I+D+i o los grandes procesos de diseño. Por ejemplo, nosotros hemos sabido que alguna empresa española de infraestructura —de todos es conocida la fortaleza de nuestras empresas de infraestructura— ha coincidido con otros países concursando para la construcción de una autopista en un tercer país y se ha encontrado con su propio proyecto ofrecido un poco más barato. Todo esto es absolutamente cierto. Hay que dejar volar la imaginación. El Centro Nacional de Inteligencia de España en una ocasión sufrió lo que consideramos una suplantación de identidad, de la que pudimos darnos cuenta un poco antes de que esto ocurriera. Si hubiera tenido éxito esa suplantación de identidad, alguien me hubiera atribuido una actividad contra un Estado que yo no había hecho, con las consecuencias que todo eso tiene. Por tanto, la ejecución de estas actividades en muchas ocasiones son delictivas, criminales, de eso no tenemos ni la menor duda y las sufrimos todos los días.

También me ha dicho que citara un caso concreto, pero le voy a pedir no hacerlo, porque la atribución no está asegurada al cien por cien y es una acusación muy grave, y más hecha en un Parlamento. Como puedo dar más datos en la Comisión de Secretos Oficiales, estoy dispuesto a, si se convoca, ofrecer allí los datos, pero atribuir la comisión de un acto delictivo a un Estado o a un grupo de personas es algo que hecho desde aquí tiene muchísima trascendencia y en eso tengo que ser prudente. He ido creo que quince veces a la Comisión de Secretos Oficiales —sus señorías lo saben— y no me importa nada ir dieciséis para hablar precisamente de esto. En cualquier caso, todo lo que les he contado es verdad.

Hay algo que me gustaría comentarles a ustedes para utilizarlo como elemento visual de lo que estamos hablando. ¿Quién desarrolló la vacuna del WannaCry? Por favor, ponte en pie. **(Don Luis Giménez, asesor, así lo hace).** Ahí lo tienen. ¿Y cómo sabemos que no va a utilizar esa capacidad que Dios le ha dado —que naturalmente no es suya sino de su equipo— para hacer maldades? Tendré que estar pendiente. **(Risas).** La realidad es que ya lleva un largo historial de trabajo en beneficio de la sociedad, en beneficio de España y de los españoles, y no para que España y los españoles tengan problemas. Además, se hace mucho más. Una de las cosas de las que los españoles podemos estar orgullosos es del trabajo del Centro Criptológico Nacional, que no me canso de decir que, en puridad, no es el CNI, sino que está colocado con el CNI y su gente es del CNI, lo que tiene algunas ventajas. Fíjense, en el caso de la atribución, siempre que por medios técnicos Luis —que acaba de levantarse— y su gente tratan de conocer el origen de un ataque, se encuentran siempre con un servidor en vaya usted a saber qué país exótico, muy lejano o en mitad del desierto. Cuando llegamos allí, resulta que efectivamente encontramos el servidor, pero nadie sabe quién lo ha puesto allí ni quién lo paga ni quién enciende la luz por las mañanas y la apaga por las noches. ¿Cuál es la virtud de que el Centro Criptológico Nacional esté integrado en un servicio de inteligencia? Que cuando se le acaban las capacidades técnicas, podemos empezar con las capacidades de inteligencia y podemos empezar a deducir algo, por ejemplo, por el escudo que llevaba en el mono quien montó el servidor. A lo mejor, con datos de ese tipo podemos tirar para adelante y saber quién lo hizo, o cualquier otra cosa que sean procedimientos de inteligencia y contrainteligencia. Por tanto, es una virtud —repito, estoy convencido de ello— que el Centro Criptológico Nacional y el Centro de Inteligencia estén colocados, pero también digo que no es lo mismo el Centro Nacional de Inteligencia que el Centro Criptológico Nacional, y esto lo digo tantas veces porque es bueno, porque genera inquietud si el CNI entra en mi casa —que no es el CNI, sino el Centro Criptológico Nacional— y lo mismo sucede con otras cosas. Todos los casos que ha dicho, como el caso de Cambridge Analytica y algún otro, son deslealtades; es decir, si un señor va a una gran empresa de las que operan en Internet y le compra sus datos, eso no es ciberseguridad, es simplemente que las empresas que compran y venden datos no están utilizando, con parámetros éticos, esa capacidad de comerciar que se les ha dado por omisión, porque nadie les ha dado la capacidad de vender datos, sino que, a través de estos sistemas de dar a aceptar, que están muy próximos a la omisión, se les ha dicho que hagan lo que quieran con nuestros datos. No son casos absolutos de ciberseguridad, sino de no hacer una buena utilización. De ahí las capacidades que uno tiene y algo que ya hemos dicho, y que posiblemente salga más de una vez en este turno de respuestas, que es el comercio de datos. Damos demasiado, entregamos demasiado de nuestra privacidad y autorizamos demasiado a aquellos que tienen nuestra privacidad. Esto puede ser un motivo de reflexión para ver qué se puede hacer al respecto, pero igual que antes me preocupaba de decirle al usuario que no dé a aceptar tan rápidamente, también hay que decirles a quienes

cve: DSCG-12-CM-131

reciben —aceptándolo nosotros— estos datos que sean prudentes en su uso. Además, ellos saben de sobra que a lo que se les autoriza no es a venderlos y a comerciar con ellos, sino a otro tipo de cosas.

La relación entre el Centro Criptológico Nacional y el Consejo Nacional de Ciberseguridad con las Fuerzas y Cuerpos de Seguridad del Estado se realiza a través de los representantes del Ministerio del Interior que hay en el consejo, donde están las organizaciones nacionales, pero yo sé que tanto la Policía Nacional como la Policía foral, en el fondo, en el caso de la ciberseguridad actúan bajo dos condicionantes: uno, reciben una denuncia y entonces es un cuerpo policial el que actúa —supongo que el ciudadano navarro, y lo digo porque estuve el viernes pasado precisamente en Pamplona, que recibe un ataque irá a su policía y lo denunciará— o, lo contrario, cuando es de arriba abajo, ya sea el Centro Nacional de Protección de Infraestructuras Críticas o cualquiera de ellos. Lo que le quiero decir, señor Yanguas, es que a mí nadie me ha reportado un problema y, por tanto, supongo que las cosas irán bien. De no ser así, este es foro suficiente para que denuncien ante el presidente del Consejo Nacional de Ciberseguridad que algo se debió hacer con la Policía foral y no se hizo.

Se ha hablado mucho de la jerarquía en el consejo. En mi opinión —naturalmente, todo es mejorable y lo estamos estudiando—, la jerarquía fue necesaria especialmente muy al principio y fue preciso establecer una norma firme al comienzo del desarrollo del Consejo Nacional de Ciberseguridad. En ningún sitio —y fíjese que llevo sirviendo al Estado cincuenta y siete años ininterrumpidos— he encontrado un lugar en el que se aplicara con más diligencia la ley de los gases perfectos. Cuando se empieza a hablar de ciberseguridad, todos quieren ocupar los espacios que sea, pensando quizá que con eso van a tener una mayor proyección en el ámbito de la Administración, más recursos o, sencillamente, porque les atraía el cumplimiento de la misión. Tuve que ser muy firme al principio —es mi experiencia personal— para establecer un criterio con el que pusiera orden, y me costó mucho tiempo, mucho menos del que me debía haber costado. Pero la realidad es que a partir de un momento se crea el consejo por un acuerdo del Consejo Nacional de Seguridad, que está publicado —si quiere le doy una copia, que la tengo—, y yo intuyo que, verdaderamente, en el funcionamiento del consejo no hay una relación jerárquica tan estrecha como parece. Lo que ocurre con muchísima frecuencia, y sigue ocurriendo hoy —y es lo mismo que les decía a sus señorías en el caso de instalación de las ondas—, es que todavía siguen diciendo que ahí quiere meter la nariz el CNI, y seguro que eso lo ha oído su señoría. Y en la mayor parte de las ocasiones, cuando se quiere establecer como una dependencia jerárquica inusitada, siempre se hace referencia no al presidente del consejo, que es quien la tiene, sino al Centro Nacional de Inteligencia y eso, sencillamente, no es verdad. El Centro Nacional de Inteligencia no tiene ninguna relación jerárquica, en absoluto, con todas las instituciones que trabajan en beneficio de que España sea un espacio seguro en el ámbito ciber, ninguna. Y si un día —bien sabe Dios que es un ejemplo— el Centro Nacional de Protección de Infraestructuras Críticas u otro cualquiera, o el Mando Conjunto de Ciberdefensa dice que tiene una relación jerárquica con el CNI, es absolutamente falso, es inexistente, no existe. El CNI no está en el Consejo de Seguridad Nacional más que como otro vocal; hay una persona del CNI sentada junto con otros dieciocho. Claro, ahora resulta que el presidente del Comité Nacional de Ciberseguridad es el general Sanz, a quien todo el mundo identifica, como posiblemente sus señorías, con el director del CNI. Bien, eso es razonable, pero cuando yo me siento en el Consejo Nacional de Seguridad no me siento con mi sombrero de director del CNI, me siento como presidente del Consejo Nacional de Ciberseguridad. Por tanto, le digo, de verdad —me gustaría convencerles, por lo menos a su señoría—, que no existe ninguna relación jerárquica entre el CNI y los componentes del Consejo de Seguridad Nacional. Es verdad que el consejo funciona con una norma según la cual el voto del presidente rompe el empate. Pues estas cosas que ocurren en otras muchas organizaciones, no ha ocurrido jamás. Hasta ahora, en los años que llevamos en el consejo todas las decisiones se han tomado por unanimidad. Me ha costado en muchos casos —ahora ya soy muy mayor y, a lo mejor, por respeto a mis canas me dicen que sí—, pero la realidad es que todo se ha aprobado por unanimidad; no ha habido ninguna decisión del consejo en la que no haya sido así.

Dicho esto, una vez que se toman las decisiones del consejo, a veces no se ejecutan como cualquier orden. Mi vida ha sido dar órdenes y recibirlas y a veces, porque no se entienden bien o porque no se interpretan bien las palabras de quien las ha dado o al revés, las órdenes luego se cumplen de alguna otra manera y es preciso corregirlo. Pero esa corrección desde el consejo a alguien a quien hemos dado una instrucción y está haciéndolo de otra manera creo que tampoco se puede interpretar como un impacto del Centro Nacional de Inteligencia en el sistema de ciberseguridad. O sea, yo hago lo que tengo que hacer, que es proteger mi propio sistema, y esas son las mismas palabras que su señoría ha dicho; es decir, aquí

cve: DSCG-12-CM-131

cada uno debería proteger su propio sistema. Esa es la situación ideal para el Centro Nacional de Inteligencia. Pero también es verdad que yo me ofrezco a los demás para echar un cable desde el consejo o desde el Centro Criptológico Nacional.

Se ha dicho que la arquitectura del consejo debería, posiblemente, estar más en red, ser más una red. En eso, de momento, no puedo más que darle la razón. Podría usted decir que si le doy la razón, por qué no se hace algo. Pues porque sí estamos haciendo algo. Ya estamos en estadios más que iniciales de crear el centro de operaciones de ciberseguridad. El centro de operaciones de ciberseguridad ya tiene edificio y lugar donde instalarse, si Dios quiere, porque ya tenemos también presupuesto para la parte que se va a hacer este año, y allí estaremos todos sentados, todos en un mismo centro de operaciones: la Guarda Civil, la Policía, el Centro Criptológico Nacional, el Incibe, todos aquellos que quieran estar en el centro de operaciones de ciberseguridad, allí estarán sentados 24 horas al día, los 365 días del año. En el centro de operaciones de ciberseguridad se va a ver en tiempo real lo que está pasando en la red, y cada uno podrá pinchar aquellos sistemas que le interesen en cada momento. Y desde allí, desde el centro de operaciones de ciberseguridad, igual que si fuera un centro de operaciones militar u otros que sus señorías han conocido, por ejemplo, el centro de control del espacio aéreo, las decisiones se tomarán en tiempo real, allí estarán todos representados, por lo que las decisiones nos representarán a todos, y además tendrán un enlace, que es otra cosa importante. En España ya hay dos centros de operaciones de seguridad y, posiblemente, este año habrá alguno más. Hay ya dos entidades privadas que han creado su propio centro de operaciones de ciberseguridad y que están deseando enlazarse con el centro de operaciones de ciberseguridad nacional. Ahí estaremos; ojalá sea este año. Con eso creo que alguna de las inquietudes que su señoría tiene y también algunos de los defectos que el sistema tiene, que naturalmente los tiene, quedarán resueltos.

En cuanto a la inteligencia artificial, yo creo que no está en el grado desarrollo que creo intuir de su presentación. La inteligencia artificial está todavía donde está, está en desarrollo. Acaba de publicar un libro Microsoft, en el que señala cuál es su estrategia de desarrollo de la inteligencia artificial. Es verdad que a partir de determinado momento, del momento en el que tengamos una máquina que toma decisiones podremos ya decir que existe, pero la inteligencia artificial quiere ir a más. Y es verdad, como su señoría dice, que puede generar problemas. En este momento, con los desarrollos de inteligencia artificial, muy unidos a los desarrollos de la matemática, algoritmos etcétera, vamos a crear una inteligencia que es absolutamente neutra, que no siente. Y si, verdaderamente, lo que queremos es dar forma a un cerebro igual que el cerebro humano, o lo más parecido posible, a la inteligencia artificial habrá que ponerle elementos éticos, elementos morales, elementos sociales, elementos de comportamiento, de forma tal que cuando alguien ponga una máquina dotada de inteligencia artificial a trabajar, considere no solo la puridad de los datos, sino que al trabajar con esos datos, igual que cada uno de los presentes, los impregnamos de principios éticos, de creencias o de lo que queramos, y eso es lo que saldría; eso, en este momento, está en debate. Y yo quiero decirle, señoría, que en este momento el mayor número de profesionales que ha contratado Microsoft son sociólogos y también alguna persona cuya carrera está relacionada con la ética o con el comportamiento humano. Por tanto, por el estado en que está la cuestión, todavía falta mucho para llegar al estado que queremos que tenga; naturalmente tenemos que hacer que se llegue lo máximo posible a esa situación en la que sea verdaderamente inteligencia parecida a la humana, y en ese momento los sesgos los reduciremos al máximo. Pero los sesgos también los tenemos los humanos. Todos los días leemos en los periódicos sobre personas cuyo comportamiento es sesgado respecto a los parámetros éticos, morales o de comportamiento general que hemos establecido en la sociedad. A mí esto me interesa mucho y leo sobre ello, pero no quiero darles la lata. No obstante, es verdad que la inteligencia artificial todavía no está desarrollada del todo.

Y les digo a todos los que han tenido alguna inquietud con las *fake news* que cuando la inteligencia artificial llegue a su estado de desarrollo, muchas de esas cosas que nos preocupan ahora del uso de la red, etcétera, quedarán resueltas simplemente por la inteligencia artificial. Es decir, las *fake news* no están aquí para durar eternamente, están aquí para durar hasta que tengamos un verdadero ordenador con inteligencia artificial que diga: pero esto es una tontería y no lo voy a enseñar porque es una tontería. Hablando de *fake news* les diré una cosa: las *fake news* han existido toda la vida. Engañar al enemigo en un combate, por ejemplo. Hay un caso que yo comento mucho porque soy lo que soy y todas sus señorías lo saben: al general Patton, el general más avezado en el empleo del arma acorazada, le hicieron una división hinchable de tanques y la pusieron en el Reino Unido, y él estaba de mal humor todos los días porque lo que mandaba era una división hinchable. Pero, ¿por qué mandaba una división hinchable?

cve: DSCG-12-CM-131

Porque los otros decían: mientras la división de Patton esté en el Reino Unido, no habrá invasión. Y el general Patton, tan aguerrido, tuvo que soportar que le diera la novedad un sargento hinchable **(risas),** pero ¡qué le vamos a hacer! Siempre han existido, como siempre ha existido el progreso, y el progreso no se puede parar. Y en este momento, con nuestros ordenadores, con nuestras máquinas y todo eso, nos vemos en la situación en la que alguien, utilizando el progreso, quiere convencernos de que una mentira es verdad o de muchas otras cosas. Pero eso no se puede parar. Yo he dicho en muchas ocasiones que nos vendrá muy bien el desarrollo de la inteligencia artificial, porque todas estas inquietudes que sus señorías manifiestan respecto a las *fake news* quedarán muy reducidas, si no anuladas.

Lo de Naciones Unidas, cartas entre Estados también lo han mencionado varias de las personas que han intervenido. Esto verdaderamente es así; si ha evolucionado la Carta de Naciones Unidas y la legislación internacional a medida que han ido evolucionando los métodos de agresión, por qué no van a evolucionar con este. Alguien tiene que reconocer en el derecho internacional que es una agresión. Porque, ¿qué agresión más grande puede haber que, por ejemplo, dificultar nuestros procesos democráticos o causar gravísimos perjuicios económicos en nuestras empresas, en nuestra economía? Naturalmente, de ahí tiene que deducirse la capacidad que se da cada Estado cuando se ve sometido a un ataque como este. El representante de Ciudadanos ha dicho que sale gratis y es verdad. Ahora la mayor parte de los ataques salen gratis, y lo único que podemos hacer es decir en los periódicos: el malo es aquel. Y nos hemos convencido hasta tal extremo de que hasta ahí podemos llegar, que me acuerdo que el gran paso que dio el año pasado la Wehrkunde, la Conferencia de Seguridad que se celebra en Munich todos los años, fue que el Reino Unido y Estados Unidos juntos, dijeron: el malo para el tipo WannaCry y para el NotPetya es este. Y lo que nos dicen a los que trabajamos en esto es: oigan, aunque no tengan la atribución completa, díganlo, vayan señalando al malo, porque lo único que podemos decir es que el malo es aquel. Aunque tenemos algunos problemas, sin duda alguna.

Sobre los datos y su comercio, creo que algo les he dicho. Desde luego, será difícil que la legislación sea exclusivamente nacional, porque una vez que pones tus intereses en la red, ya lo utiliza quien quiere. Podemos tener perfectamente un servidor que no es español, como Deutsche Telekom, o cualquier otro por la capacidad que tienen todos de ofrecer el producto gratis, que, vuelvo a decir, no es gratis, lo estamos pagando al entregar nuestros datos. Posiblemente, los que utilicen Vodafone no estén muy seguros de que estén entregando sus datos exclusivamente a un servidor español —y no quiero con esto equivocarme porque con todos es igual, es decir, el ejemplo a lo mejor no es el adecuado y les pido que lo olviden—, porque la realidad es que nosotros entregamos nuestros datos a un operador, el de nuestro teléfono, y esos datos ya dejan de ser posesión de un particular ámbito geográfico. Por lo tanto, la legislación en este sentido es un poco más compleja.

Respecto a las *fake news,* les vuelvo a decir lo que les he dicho: tenemos que ser capaces de ver que esto ha ocurrido siempre. Entramos en el debate de si se regula o no el uso de Internet —seguro que sus señorías sobre esto han debatido con otros más que conmigo—, pero el debate al final es privacidad o no y libertad o no. Este es un debate muy complejo que, desde luego, no me corresponde a mí hacer.

Medios suficientes. No creo que haya nadie —aunque sea el jefe del centro de ciberseguridad de los Estados Unidos de América o del Reino Unido— que diga que tiene suficiente. Yo solo les digo a sus señorías una cosa: en España no hay presupuesto para ciberseguridad. Entonces, cada uno se apaña como puede. Yo mismo me apaño como puedo; es decir, el CNI recibe su presupuesto anual, en el que incluye los gastos de personal del Centro Criptológico Nacional, etcétera, y yo, de mi presupuesto normal —como puede hacer Interior o cualquier otro ministerio— ataco la ciberseguridad. ¿Eso es bueno o es malo? Si en la redacción de los presupuestos, cuando se pide dinero para hacer las cosas cada uno considera los gastos que le ocasiona —que yo lo hago—, está bien. Creo que sería interesante mandar un mensaje a la sociedad y que, igual que se habla en el Reino Unido de 1300 millones de euros más para la ciberseguridad, no estaría mal que aquí viéramos que para una actividad tan concreta hay unos recursos concretos y que después se pudieran pedir explicaciones sobre el uso de esos recursos para tan importante misión. Pero, como digo, aquí todavía no los hay.

En cuanto a la formación, se hace mucho. Me he sorprendido de lo que hacen la universidad española y las empresas privadas para ciber. Es verdad que muchísima gente trabaja en esto. El premio de ciberseguridad que da el Centro Criptológico Nacional cada año se lo hemos dado este año a un profesor de la Universidad de Alcalá de Henares porque dedica su vida a describir este problema, a enseñar a sus alumnos a luchar contra él, a que tengan imaginación para diseñar máquinas y productos. En el Centro Criptológico Nacional damos unos veinte cursos anuales de ciberseguridad para toda la Administración;

cve: DSCG-12-CM-131

inicialmente era solo para la Administración central pero ya asisten también personas de la Administración local, de algunos ayuntamientos. El problema de la enseñanza de las técnicas ciber, etcétera, es que tenemos que ser capaces, incluso los que no tenemos esta responsabilidad, de participar. Siempre que se da un curso en el CNI les pregunto a los alumnos: ¿os ha interesado el curso? Y me dicen: muchísimo. Y les pregunto: ¿lo vais a implantar en vuestra organización, sea esta cual sea? Y siempre me dicen: lo tengo muy difícil. Y les pregunto: ¿y por qué? Y me dicen: porque no sé si me va a dejar mi jefe. ¿Y por qué no le va a dejar su jefe —que a lo mejor es una respuesta genérica—? Porque si su jefe quiere un dato de un ordenador que no está protegido, lo tiene ya, y si quiere un dato de un ordenador protegido, le dicen: tiene usted que esperar siete minutos a que hagan sus pruebas. El jefe suele decir: no, hombre, no. Ya estáis los pesados de la ciberseguridad; no quiero más ciberseguridad en mi ordenador, que sea abierto. Aquí hay un ejemplo palmario que les ofrezco a todas sus señorías. Aquí ha habido muchísimas organizaciones que han sido atacadas con algún éxito. En el Centro Nacional de Inteligencia de España no ha entrado nunca nadie. Punto. A lo mejor están entrando en este momento. **(Risas).** Hasta que yo he llegado aquí, no ha entrado nunca nadie. Si yo tengo a mi cargo 3500 personas, en números redondos, y 300 millones de euros, en números redondos, de presupuesto y no entra nadie en el Centro Nacional de Inteligencia, ¿por qué entran en una organización que tiene 160000 personas y todo el dinero del mundo? Este es un mensaje que creo que es fácil de entender. Vamos a ver, si yo solo tengo 3500 trabajadores y 300 millones de euros y en el CNI no entra nadie, ¿cómo usted, que tiene 160000 empleados y todo el dinero del mundo, me viene a llorar porque le entran todos los días? Haga usted lo que hago yo, preocúpese de su seguridad, porque es posible. Este es un mensaje que debiera de algún modo reflejarse en los resultados. Presidente, ni siquiera lo digo como sugerencia pero calculo que es de interés. Es decir, es posible defenderse; tiene que haber una voluntad de defenderse y hay procedimientos. Si no, que vengan a preguntárselo al Centro Criptológico Nacional. Si una gran empresa española es atacada todos los días, no porque —que también ocurre— un funcionario se lleva por la noche el ordenador a casa, sino porque la atacan de verdad, haga usted lo necesario para que esto no ocurra. Y nosotros descubrimos con la educación y los cursos que a veces enseñamos a utilizar los medios y después no se utilizan.

Naturalmente, señor Mayoral, y cualquiera de los presentes, pueden contar con el vídeo. Tenemos otros dos más y, si el señor presidente quiere, puedo mandar los vídeos aquí para que haga la distribución. Y hay más cosas, porque la mayor parte de los documentos —si no todos— que edita el Centro Criptológico Nacional son abiertos, como ha señalado su señoría, el representante del Grupo Socialista. Todos los documentos del Centro Criptológico Nacional son libres y 500000 personas se han bajado el vídeo porque entran en la página www.ccn.cni.es, donde creo que es muy interesante entrar, porque ahí están las vacunas, las herramientas que tenemos y los servicios que podemos prestar. Ahí tenemos también un procedimiento —iba a decir de reportar, pero ya sé que es una barbaridad utilizar esa palabra, que empleamos los que hemos tenido que vivir alguna vez con el inglés— de notificar las agresiones que se tienen. Entren en la página web y verán todo lo que hay y que está a su disposición, e incluso algunas cosas que pueden ser un poco más delicadas, porque en el fondo queremos que esto vaya bien. Hay muy pocas cosas clasificadas. A veces clasificamos hasta que los estudios están terminados. Por ejemplo, si hay alguna empresa de *software* que está haciendo trampa, inicialmente lo clasificamos porque no vamos a acusar sin tener todas las pruebas en la mano.

El impacto económico y otros impactos me parecen muy interesantes, pero no le puedo ofrecer esos datos en este momento porque no he venido preparado, aunque, naturalmente, me comprometo, en un plazo muy breve —el que el señor presidente quiera—, a tener este informe y remitirlo a la Comisión para su distribución. También me gustaría decir que los impactos a veces son muy difíciles de cuantificar. Una empresa española de infraestructuras quiere hacer un trabajo en un tercer país y se encuentra con que a través de los sistemas ciber están entrando en su proyecto. Hemos tenido los dos casos: aquellos en los que, a pesar de entrar, como al exponer el proyecto era infinitamente más sólido el que lo hace que el que lo roba, el que lo hace sigue haciéndolo y por tanto el impacto es cero; y, en cambio, hay otros casos en que es al revés, que hay quien mira solamente el final y dice: yo tengo poco dinero, así que si este me lo hace por 500 millones menos, que lo haga. A pesar de todo, vamos a hacer ese informe y yo se lo ofreceré. A lo mejor, está ya hecho.

En cuanto al caso del *smartphone* y la interpretación legal o ilegal de comunicaciones, quiero hacer un aserto, quizá muy amplio, que tiene que ser sin clasificar. En España la interceptación de telefonía móvil por métodos tradicionales es muy difícil. Puede haber gente con mucha capacidad adquisitiva que encuentre un *software* en no sé qué lugar, pero sus señorías pueden estar tranquilos en el sentido de que

cve: DSCG-12-CM-131

su vecino o su adversario político, en general, no tiene capacidad. ¿Y por qué no tiene capacidad? Los teléfonos móviles en España van muy protegidos porque la mayor parte del tráfico de móviles va con fibra óptica. Aquí el único espacio abierto en un teléfono móvil es el que hay desde donde está el teléfono y el primer poste repetidor. A partir de ese momento, ya es imposible. No sucede lo mismo en otros países. En algún lugar al presidente de ese país le han interceptado, pero es porque iba por onda radio y eso es más fácil. En España eso es muy complejo. Pero de nuevo volvemos al caso de las deslealtades. Si en un operador hay un desleal que quiere dejar que allí pinche alguien, a ver si le encontramos y le denunciamos a un juez. Pero por el uso técnico —que es a lo que yo interpreto que se refiere— es complejo hacerlo aquí, por lo que puede estar bastante tranquilo. Los únicos que pueden interceptar comunicaciones son las Fuerzas y Cuerpos de Seguridad del Estado, bajo un mandamiento judicial, y el CNI ni más ni menos que con una autorización de un magistrado del Tribunal Supremo. Por tanto, no es muy frecuente que se dé aquí. ¿Que haya alguien que sea capaz de encontrar un *software* maligno muy importante? A lo mejor hay alguien, pero, en realidad, para el día a día aquí es muy complejo hacer eso.

Me ha dicho una cosa sobre los *botnets*. No he visto ninguno, pero sé que existen. Los *botnets* son unos aparatos en los que entra un mensaje y salen cien a la hora. Aquí algunas veces en algún caso hemos visto que una sola persona ponía 24000 mensajes a la hora, cosa que es metafísicamente imposible. Quiere decir que estaba utilizando *botnets;* desgraciadamente el estado del arte es este. No conozco ninguno, pero sí hemos podido identificar a quiénes los utilizan en un caso particular que estamos investigando porque, como le digo, lo que sí deja siempre es dato del origen. Su señoría no puede poner 24000 mensajes a la hora; a lo mejor 23000 sí, pero 24000 ya es mucho. **(Risas).**

El ataque a partidos políticos y a agentes estatales se ha dado y los que lo han recibido han sido informados. Pasar de aquí es un poco complicado pero, cuando lo hemos detectado, lo hemos comunicado. No quiere esto decir que hayamos detectado todos los casos, pero cuando lo hemos detectado, y algún partido político ha sido atacado, ha sido informado su presidente o su dirección de que esto se había producido y en qué términos. Lo que sí le puedo decir es que los ataques a partidos políticos que hemos detectado han sido muy breves y no se han llevado nada importante. Parece que han sido ataques de tanteo; no ha sido un ataque persistente, no ha sido que un partido político tenga un gato metido seis meses para saber su estrategia, quizá también porque, al sentirse descubiertos, han dejado de actuar; pero se ha producido.

Creo que vamos a proteger mejor nuestra democracia con el establecimiento del Centro de Operaciones de Ciberseguridad, así esto va a estar más coordinado. En un año electoral hay dos cosas de gran interés. Por un lado, las *fake news* —las acciones de influencia, que es como las llamamos nosotros— para que la opinión pública vaya por un camino, pero ese camino no es fruto de esa opinión pública, sino de poner datos falsos en la opinión pública y que, por tanto, se desvíe nuestra capacidad de decidir. Las acciones de influencia pueden existir y habrá que estar prevenido. Y, por otro lado, la seguridad informática en nuestro proceso electoral. Nuestro proceso electoral va a estar seguro, no va a haber nadie que se meta en las cuentas y las haga mal. Naturalmente, estoy hablando con los parámetros de hasta hoy. Nosotros, en todos los procesos electorales que ha habido en España, podemos certificar —y, de hecho, el Centro Criptológico Nacional ha certificado los procesos— que nadie ha entrado. Ahora, acciones de influencia hay muchas, y no solo a través de la red, sino también a través de otras muchas cosas.

La estrategia, si Dios quiere, en la próxima reunión del Consejo de Seguridad Nacional se presentará para su aprobación porque está ya escrita. No tiene muchos cambios. Lo que nos mueve es la propia experiencia, que no es mala, y desde luego lo que está ocurriendo con los nuevos desarrollos.

En cuanto al número de los ciberataques, le decía que nosotros en 2018 recibimos 38000; graves, a los que hemos tenido que dedicar tiempo, esfuerza, etcétera, 102. Depende de cómo se digan las cosas. Decimos 38000 ataques y parece que estamos todos los días con ellos, pero que me hayan preocupado han sido entre 100 y 200 y de los que no hemos salido mal. Es verdad que algunos han triunfado y han entrado en sitios donde no queríamos que entraran. Cada tres o cuatro días hay uno al que hay que hacer frente con esfuerzo.

Cómo se maneja en la Administración este esquema. Los recursos humanos que dedicamos a la ciberseguridad desde mi punto de vista en España son insuficientes y además porque a veces son *part-time*. Esto es algo que con el tiempo tendremos que mejorar. Quizá, el haber tenido la buena suerte o la eficiencia de parar los ataques gordos que hemos tenido nos hace pensar que vivimos en el paraíso y que, por tanto, no hay que dedicar más dinero ni más recursos, pero no es verdad. Tendremos que tener más cuidado. Muy pocas organizaciones tienen una plantilla de personas dedicadas a ciber. Lo que les decía es verdad, en

cve: DSCG-12-CM-131

muchas organizaciones el de ciber es *part-time*. Es el no sé qué, que además se dedica a ciber. También tienen que tener en cuenta que no hay puestos de trabajo específicos. El otro día en la universidad decía: Miren, si quieren tener un buen futuro, háganse ingenieros ciber. Y casi seguro que es verdad, pero vemos muy pocas veces en las plantillas de las grandes corporaciones que sea así. Por tanto, en el ámbito de la Administración básicamente, que es a lo que nos dedicamos, los catálogos de puestos de trabajo tienen que tener gente ciber, igual que tienen gente de seguridad física. Tenemos que aumentar el esfuerzo en formación. Yo hago veinte cursos al año —es bastante— y formamos a unas quinientas personas al año, pero teniendo en cuenta el estado de la cuestión no son muchos. Mis subordinados dicen que, como mínimo, habría que multiplicar por diez esta cifra.

También es muy importante concienciar a los altos cargos —lo digo así porque estoy en la Administración si no diría a los responsables de determinado nivel en el organigrama— de que la ciberseguridad no juega contra ellos sino que juega a su favor y de que no se opongan a que estas cosas se hagan bien.

En cuanto al impacto del real decreto…

El señor **PRESIDENTE:** Perdone que le interrumpa. Tenemos un problema logístico. La siguiente comparecencia es por videoconferencia con Estados Unidos y el compareciente tiene que ausentarse exactamente a la una porque tiene una clase y, por tanto, tenemos el tiempo limitado. Entonces, yo voy a pedir al secretario de Estado que vaya terminando y consideren si necesitamos un segundo turno en esta comparecencia o no, porque si utilizan el segundo turno y no lo hacen de forma breve lo que arruinamos es la comparecencia siguiente, que tiene un límite de tiempo cerrado.

Adelante.

El señor **SECRETARIO DE ESTADO DIRECTOR DEL CENTRO NACIONAL DE INTELIGENCIA** (Sanz Roldán): Termino. No sé si lo que ha querido decir es que el papel del denunciante es el papel del desleal. Naturalmente, yo no puedo estar más de acuerdo con que en algún código, ya sea el Código Penal u otro, tiene que estar porque es un delito muy grave que a veces causa estragos.

Me queda solo decir una cosa que me ha impresionado: contratar *hackers*. Eso es algo que yo no les aconsejo. Todos los *hackers* dicen que saben mucho y alguno habrá, pero, en general, la sabiduría propia de los temas ciber está en quien se dedica a esto desde la universidad, en su servicio. Por tanto, si se quieren proteger, vayamos a lo seguro y lo seguro es la gente que se ha formado en asuntos ciber.

Termino agradeciendo los elogios al centro. Ojalá que sean merecidos y el pésame por los que han entregado su vida en esta actividad.

Muchas gracias.

El señor **PRESIDENTE:** Como les he anunciado, sepan que si utilizan el segundo turno estamos arruinando la segunda comparecencia y estoy seguro de que ninguno de ustedes lo quiere. **(Pausa).** Les agradezco su comprensión y agradezco al secretario de Estado su presencia. **(Pausa).**

— DEL SEÑOR LESACA ESQUIROZ (DOCTOR EN HISTORIA CONTEMPORÁNEA E INVESTIGADOR VISITANTE EN LA UNIVERSIDAD DE COLUMBIA), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA MEDIANTE EL SISTEMA DE VIDEOCONFERENCIA. (Número de expediente del Congreso de los Diputados 219/001551 y número de expediente del Senado 715/000625).

El señor **PRESIDENTE:** Ahora tenemos la comparecencia de don Javier Lesaca Esquiroz, doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia, para informar sobre diversas cuestiones relativas a la ciberseguridad en España, como ven, mediante el sistema de videoconferencia.

Don Javier Lesaca, buenos días. El toro es suyo.

El señor **LESACA ESQUIROZ** (doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia): Muchas gracias, presidente.

Señorías, muchas gracias por considerar que mi intervención puede ser de utilidad para este asunto. Después de la presentación que voy a defender ante ustedes quedo a su disposición para cualquier duda o comentario. En ella tienen mis datos de contacto por si quieren contactar conmigo en el transcurso de la conferencia o *a posteriori*.

cve: DSCG-12-CM-131

Quería empezar esta comparecencia, titulada *Origen y metodología de las campañas de desinformación* **(apoya si intervención en un *powerpoint),*** haciendo una pequeña introducción, digamos, conceptual sobre el marco histórico en el que se están produciendo estas campañas de desinformación. Creo que es importante porque es precisamente en torno a estas dos cuestiones donde se están produciendo los ataques de desinformación digital. Las actuales democracias liberales —y creo que en esto podemos tener un consenso en la sala en la que se está produciendo esta comparecencia—, entre las que se encuentran España y otros países de la Unión Europea, se basan básicamente en dos pilares: una esfera pública libre y bien informada, lo que Jürgen Habermas definiría como la piedra angular de una democracia, y el contrato social, que es el pacto entre ciudadanos y gobernantes por el cual los ciudadanos tienen unas expectativas de cumplimiento de una serie de servicios públicos por parte de una administración.

En cuanto a la esfera pública libre y bien informada, durante el siglo XX e incluso comienzos del siglo XXI había un cierto consenso entre los agentes que conformaban esa esfera pública libre y bien informada, incluso había un cierto consenso en la manera en que la opinión pública se formaba: en función de la relación entre tres agentes, que eran las instituciones públicas, los medios de comunicación y los ciudadanos. De la deliberación entre estos tres agentes perfectamente identificados nacían los mensajes hegemónicos en torno a los que se cohesionaba la opinión pública. Sin embargo, a comienzos del siglo XXI empieza a haber una fractura tanto en el contrato social como en la esfera pública libre y bien informada, es decir, en los dos pilares sobre los que se asienta una democracia liberal. No se impacienten que ahora iré al grano, pero creo que es importante este marco introductorio. Las diversas encuestas nos han ido advirtiendo desde comienzos del siglo XXI de que el contrato social entre los ciudadanos y las instituciones públicas se iba debilitando de manera progresiva. Aquí tienen una encuesta de este mismo año en la que se ve de qué manera están decreciendo los niveles de confianza de los ciudadanos en sus instituciones políticas. Menos de la mitad de los ciudadanos de los países desarrollados confían en sus instituciones públicas. Este es un informe del Edelman Trust Barometer hecho público en el año 2018. Vemos que en España el 47 % de los ciudadanos desconfían de sus instituciones y solamente en países como China, Indonesia, India o Emiratos Árabes Unidos hay unos índices de confianza mayores del 60 %. Esto demuestra que se ha producido un nivel de desconfianza importante en las instituciones públicas, con lo cual hay una quiebra del contrato social.

Otro de los elementos clave a la hora de conformar una democracia liberal es la opinión pública, como hemos dicho, y uno de sus principales agentes, los medios de comunicación, también se encuentran en una profunda crisis. Este es el mismo barómetro pero en relación con los medios de comunicación. Vemos que gran parte de los países desarrollados tienen una confianza bastante débil en sus medios de comunicación tradicionales. Por tanto, nos encontramos con que los dos pilares sobre los que se asienta una democracia liberal están en crisis.

A esto hay que añadir que la irrupción de las herramientas de comunicación también ha alterado en gran manera la forma en que se configuraba la opinión pública o la deliberación pública. Hemos pasado de una opinión pública que se creaba en torno a un debate a una opinión pública en la que las redes sociales no están favoreciendo de manera explícita el debate. Aquí ven dos análisis sobre dos conversaciones digitales realizadas en los últimos tres años. La de la izquierda, en verde y rojo, es un análisis realizado con el apoyo de una empresa española con la que suelo realizar investigaciones, que es Alto Analytics —de hecho, prácticamente todas las visualizaciones que van a ver son fruto del software que utilizo con la empresa española Alto Analytics—, en el que se ve cuál es el debate sobre la inmigración en Italia. Se ve que la comunidad que apoya la inmigración y la que está en contra de la inmigración apenas dialogan entre sí, es decir, no se produce una deliberación. Los algoritmos de las plataformas de comunicación no están favoreciendo un debate sobre los temas clave de una sociedad, con lo cual se está produciendo una polarización entre los ciudadanos sobre temas clave de la sociedad. Y la imagen de la derecha es una imagen hecha por el MIT, Massachusetts Institute of Technology, es el análisis de la conversación digital sobre la campaña electoral en Estados Unidos de 2016. Pueden ver el mismo fenómeno: los ciudadanos que apoyaban al presidente Trump y los ciudadanos que apoyaban a la candidata Clinton no dialogaban entre sí, sino que los propios algoritmos de las plataformas de comunicación digital estaban favoreciendo que cada comunidad hablase solo entre sí. Por tanto, volviendo a la primera diapositiva, esa esfera pública libre y bien informada sobre la cual se asienta una democracia liberal está siendo dañada no solamente por la falta de confianza en los medios de comunicación tradicionales, sino también por los propios algoritmos, que están favoreciendo la creación de cámaras en

cve: DSCG-12-CM-131

las que simplemente vemos reforzadas nuestras ideas. Con lo cual vivimos en una situación en la que la revolución tecnológica y la crisis de credibilidad, fruto en gran manera de la crisis económica de 2007 y 2008, han producido una situación de quiebra de la naturaleza de las democracias liberales. Evidentemente, este es el momento perfecto o el caldo de cultivo perfecto para que se produzca lo que estamos llamando la desinformación como arma de guerra.

Esta imagen que ven aquí es una imagen ficticia sacada de Google, es un juego de palabras en el que se ve un teclado convertido en una granada de mano. La realidad nos demuestra que este dibujo no es solo un ejercicio conceptual, sino que hay grupos subnacionales y otros Estados que se han tomado muy en serio la utilización de la comunicación como un arma de guerra en este contexto de crisis de las democracias liberales. Esta imagen que ven aquí es de una de las facciones de Al Qaeda en Siria, del Frente al Nusra, del año 2014. Ellos mismos, en una de sus comunicaciones oficiales en *Al Risalah,* una revista oficial del Frente Al Nusra, decía que una de las armas que iban a emplear en el futuro iba a ser la comunicación, y aquí tienen una imagen hecha por un grupo terrorista en la que un Kaláshnikov es sustituido por unas herramientas de comunicación. Es decir, los propios grupos subnacionales u otros Estados tienen muy claro que la comunicación se va a convertir en un arma de guerra para favorecer esta crisis de las democracias liberales.

No estamos hablando de un fenómeno nuevo, hace 2500 años Sun Tzu dijo que el arte de la guerra es el engaño, es decir, desde hace más de 2500 años existe la evidencia de que la comunicación puede ser empleada como un elemento de desestabilización de otros Estados considerados como adversarios. También es cierto que, aunque hace 2500 años que todos somos conscientes del poder disruptor de la comunicación, en los últimos años, y sobre todo a comienzos del siglo XXI, la escala y la magnitud de estos ataques están aumentando, y algunos Estados lo están reconociendo de manera muy abierta. No hace falta buscar causalidades o intentar buscar agendas ocultas porque algunos Estados de manera muy clara ya están reconociendo que como parte de sus guerras híbridas están auténticas campañas de comunicación. En 1999 dos generales chinos en un libro —*La guerra irrestricta*— que lo pueden encontrar en abierto en PDF, ya decían que los nuevos métodos para una guerra no militar serán la guerra psicológica y las guerras de comunicación, que ellos definían como manipular lo que los ciudadanos ven y oyen para liderar la opinión pública. Es una declaración pública de dos generales de muy alto nivel de un Gobierno que ya anunciaba que tenían en mente este escenario. Son muy famosas las declaraciones de un general ruso, Valeri Guerásimov, en las que decía que el futuro de las guerras pasaría medios militares de carácter oculto que incluyen acciones informativas. El propio Gobierno de España en su Estrategia de Seguridad Nacional del año 2017 ya reconoció que una de las principales amenazas para España son las acciones combinadas de medios militares, ciberataques y operaciones de manipulación de la información. Por tanto, ya no estamos hablando de teorías, sino de realidades reconocidas por los propios Estados.

Lo que me gustaría en esta comparecencia es ir al detalle de en qué consisten exactamente las guerras de comunicación o de desinformación. Mi principal hipótesis es que van mucho más allá de lo que conocemos como el fenómeno de las *fake news,* de las noticias falsas. Como vamos a ver en esta presentación, las noticias falsas son solamente una pequeña parte de esta estrategia de disrupción. Lo que voy a mostrar son las conclusiones de la evidencia científica después de analizar diversas conversaciones digitales de temas políticos clave o muy polémicos en diferentes países. La conclusión básica es esta: las guerras de desinformación o las guerras de disrupción digital consisten en un proceso de cuatro pasos. Uno es el análisis y la detección de vulnerabilidades de un país considerado como adversario; dos, la creación de unas narrativas transmedia que potencian estas vulnerabilidades detectadas en el país adversario; tres, la creación de una red de medios propios ajena a los medios de comunicación tradicionales para comunicarse e interactuar de manera directa con las audiencias potenciales y, por último, el uso automatizado de redes sociales para que ese mensaje tenga una gran magnitud y llegue a más audiencias. Vamos a ver diversos ejemplos de este proceso paso a paso.

Empezaremos con el análisis de las vulnerabilidades y por un caso extremo que genere consenso. En esta comparecencia me gustaría mantenerme en un nivel técnico y no entrar en temas demasiado polémicos, por lo que vamos a ver casos muy concretos que todos podemos comprender de manera muy nítida. Vamos a empezar con el caso extremo del Estado Islámico en el asunto de los análisis de vulnerabilidades. Como he dicho, las guerras de desinformación pueden partir tanto de grupos subnacionales como de países extranjeros, de Estados nación. Esta metodología a la que he hecho

cve: DSCG-12-CM-131

referencia ha sido utilizada tanto por grupos subnacionales como por naciones Estado con el mismo objetivo, que es debilitar Estados nación consolidados en torno a democracias liberales.

Como he dicho, vamos a empezar con el análisis de las vulnerabilidades. ¿Qué hizo el Estado Islámico en su campaña de desinformación desde el año 2014 hasta el año 2018? Como ustedes bien saben, sería difícil de cuantificarlo, pero podemos decir que el 50 % de los recursos que este grupo terrorista ha utilizado en su particular guerra contra los Estados nación, Siria e Irak, ha sido precisamente una campaña de comunicación o de desinformación. En el año 2015, un informe de Naciones Unidas reflejó perfectamente que los lugares donde mayores necesidades humanitarias se estaban produciendo, concretamente en Irak, era precisamente en las regiones sunníes, en las regiones de Nínive y Al Anbar, donde mayores carestías de servicios públicos se estaban produciendo. El informe del Banco Mundial del año 2014 también advirtió que los lugares donde más se estaba sintiendo la crisis del precio del petróleo había sido precisamente en las zonas donde después surge el ISIS, es decir, las mismas zonas sunníes de Nínive y Al Anbar. ¿Cuál es la narrativa? El Estado Islámico detectó perfectamente estas vulnerabilidades que se estaban produciendo en las regiones sunníes de Irak y lanzó toda una campaña de comunicación —este es un análisis de las principales narrativas del Estado Islámico de esta dinámica desde el año 2014 a 2018—, y podemos ver cómo el 25 % de sus comunicaciones son mensajes positivos de gobernanza. Es decir, el Estado Islámico detectó estas vulnerabilidades de los Estados nación y generó toda una narrativa destinada a posicionarse con una alternativa a los Estados nación.

Aquí tenemos imágenes del Estado Islámico generando una policía y seguridad, generando educación, generando sanidad pública para toda la población, generando medidas contra la pobreza y a favor de la inclusión social. Es decir, el Estado Islámico se posicionó en torno a unas vulnerabilidades que detectó en su rival. Estas vulnerabilidades, en este caso de Irak y Siria, consistían en una falta de servicios públicos en una parte de la población, pero estas vulnerabilidades pueden estar en Europa; por ejemplo, en Italia con la crisis migratoria que se ha vivido en los últimos años; también en Francia, con la crisis de los chalecos amarillos o en España pueden ser los conflictos producidos sobre temas identitarios o de cohesión política de algunas regiones. Son vulnerabilidades que grupos subnacionales u otros Estados detectan en Estados que consideraban adversarios, y tratan de potenciarlas.

¿Qué ocurre después de que un grupo subnacional o un Estado adversario hayan detectado las vulnerabilidades en un país que quiere erosionar? Se produce lo que se denomina la creación de unas narrativas destinadas a fomentar precisamente esas vulnerabilidades o, hablando en lenguaje más coloquial, echar gasolina al fuego, a las hogueras. Esto es importante destacarlo, porque cuando hablamos de guerras de desinformación hay que tener claro que estas guerras de desinformación no crean problemas nuevos, sino que lo que van haciendo es alimentar problemas ya existentes. Está más que comprobado que las campañas de desinformación están produciendo grandes problemas de gobernanza, pero están basadas en problemas ya preexistentes; es, como he dicho anteriormente, la metáfora de echar gasolina a incendios que ya están provocados. Un ejemplo muy claro de esta creación de narrativas son las conclusiones del informe Müller, en la Cámara de Representantes de Estados Unidos, donde se están haciendo públicos los mensajes supuestamente pagados por el Gobierno de Rusia en Facebook en la campaña electoral del año 2016. Está probado y esta es una de las conclusiones que actualmente se están publicando. Por ejemplo, los autores de estos anuncios pagados en Facebook, durante la campaña electoral de Estados Unidos hablaban de que las mujeres musulmanas apoyaban a Hillary Clinton o que la LGTB apoyaba a Bernie Sanders. Pero resulta que la misma persona, el mismo individuo o la misma empresa que estaba pagando estas campañas era el mismo que pagaba estas otras campañas, en las que, por ejemplo, vinculaba a la comunidad LGTB con los terroristas del ISIS o en las que decían de Satán: sí elijo a Clinton, yo gano. Jesús, no con mi ayuda. Es decir, la misma persona que estaba haciendo campañas a favor de la comunidad musulmana y de las mujeres y de la comunidad LGTB estaba favoreciendo campañas que decían exactamente lo contrario. Estas personas, esta institución o este país, que estaban pagando estas campañas, habían detectado unos puntos de fractura en la opinión pública de Estados Unidos —como el asunto de la incursión de la comunidad LGTB, el tema de la integración de otras comunidades culturales— y crearon una serie de narrativas para polarizar más aún ese debate. Es un ejemplo muy claro de la operación de estas narrativas.

Hay un ejemplo muy claro de esta misma semana, concretamente, de hace un par de días, que también podría ser, dentro de la creación de estas narrativas para fomentar la crispación social o para aumentar las vulnerabilidades detectadas en una sociedad, la crisis de los chalecos amarillos en Francia. Aquí vemos una cuenta, que después analizaremos con más detalle, en la red social de Twitter que es la

cve: DSCG-12-CM-131

más activa difundiendo mensajes a favor de los chalecos amarillos, pero también hemos visto que difunde noticias que son directamente *fake news,* noticias falsas que lo que hacen es alentar una narrativa a favor o que aumenta la tensión sobre los chalecos amarillos. Esta cuenta, por ejemplo, está diciendo que hay una milicia secreta enviada por la Unión Europea para apoyar al dictador Macron contra los chalecos amarillos. Hay una foto en la que se ve a los que probablemente sean policías de paisano, pero que esta cuenta identifica como una milicia secreta enviada por la Unión Europea. Otra cuenta también muy activa en la crisis de los chalecos amarillos apoya el mismo mensaje diciendo que el dictador Macron manda mercenarios de la Unión Europea, que hablan en diferentes idiomas, para matar inocentes en la crisis de los chalecos amarillos. Es decir, el fenómeno de las *fake news* los podemos incluir dentro de toda una campaña por introducir de manera maliciosa una serie de narrativas que fomentan o echan gasolina a crisis políticas ya existentes. Esta misma cuenta que, insisto, es la cuenta más activa dentro de la comunidad de los chalecos amarillos, difunde imágenes de la masacre del pueblo francés entre las que incluye, por ejemplo, la imagen de una manifestante herida el 1 de octubre en Barcelona, es decir, noticias falsas.

Volviendo al tema de Cataluña, un ejemplo muy claro de noticias falsas es cuando un medio extranjero publicó que había tanques en las calles de Barcelona. No quiero hablar de la crisis de Cataluña, pero creo que todos podemos estar de acuerdo en que no hubo tanques en las calles de Barcelona; sin embargo, de manera deliberada, se intentó ampliar las consecuencias o la magnitud de una crisis política ya existente en España diciendo que había tanques en las calles de Barcelona, cuando eso no ocurrió, afortunadamente.

¿Cómo se transmiten estas narrativas? Volviendo un poco al orden de la comparecencia, cuando un país extranjero o un grupo adversario detecta las vulnerabilidades preexistentes en un país crea unas narrativas que fomentan estas vulnerabilidades. ¿Cómo se transmiten esas narrativas a la opinión pública? Creando una red de medios propios. Es decir, estas estrategias de desinformación son conscientes de las crisis de credibilidad que tienen los medios de comunicación tradicionales. De hecho, es muy interesante ver cómo algunos de estos agentes disruptores dedican esfuerzos a aumentar esta crisis de credibilidad de los medios. Esto es una vez más una imagen, del 28 de diciembre, de la cuenta más activa a favor de los chalecos amarillos, en la cual acusan a los medios tradicionales de Francia, a las cadenas de televisión tradicionales de ese país, de estar asesinando a la verdad. Es decir, inciden en la idea de que los medios de comunicación tradicionales ya no sirven para transmitir la verdad, sino que son los mayores enemigos de la verdad: se insiste en fomentar esa crisis de credibilidad de los medios. Es muy curioso porque su imagen coincide con una imagen que hizo pública el Estado Islámico en el año 2015, en la cual pedía a los ciudadanos que dejasen de consumir medios de comunicación tradicionales. Incluso mostraba una imagen de los ciudadanos pisoteando receptores de televisión por cable, y les pedía que dejasen de consumir *traditional media,* medios de comunicación tradicionales y que solo consumiesen los canales propios del Estado Islámico. Existe ese punto en común en estos agentes disruptores.

¿Cómo funcionan estos nuevos medios que se han posicionado como medios alternativos para difundir los mensajes propios de la desinformación? Como les he dicho, este es un análisis de la pasada campaña electoral en Italia, en la cual uno de los debates más polarizados fue precisamente el que estaba a favor de la inmigración y en contra de la inmigración, y dentro de la comunidad que estaba en contra de la inmigración detectamos una página web que se hacía llamar Vox intentando pasar desapercibida. —No tiene nada que ver con el partido político de España; por favor, que nadie saque conclusiones erróneas porque no hay ninguna mala intención en esto. De hecho, esta imagen estaba sacada antes de que apareciese este partido político—. El nombre de Vox viene porque esta página web, que fue una de las más activas y de las más compartidas dentro de la comunidad antiinmigratoria en Italia, tomó este nombre para hacerse pasar por la página web de Estados Unidos llamada Vox, que es una página web de prestigio y muy reconocida en cuanto a la calidad de las noticias. Lo que intentaba era generar confusión en la audiencia y, por eso, se hacía pasar por un medio de *fact checking,* pero lo que hacía era difundir imágenes y una narrativa muy nociva y contraria a la comunidad inmigrante en Italia. En este medio hay una absoluta falta de transparencia sobre quién está detrás, cuáles son sus accionistas, quién escribe las noticias. Nació justamente unos meses antes de la campaña electoral, es decir, es un medio que tiene todas las características de un medio de desinformación, de crear confusión en mitad del contexto.

Otro ejemplo, en el que no quiero poner nombres porque es una investigación en curso y todavía no quiero adelantar las conclusiones, es una conversación digital sobre un debate político de gran relevancia

cve: DSCG-12-CM-131

a nivel global, en el cual la comunidad que está siendo hegemónica o la que mayor apoyo está recibiendo en este debate político está basando su narrativa —presente aquí en estos dos nódulos digitales más grandes— en unos medios de comunicación nuevos que han aparecido este año, es decir, que apenas tienen historial, que no tienen transparencia ni credibilidad. Hay una metodología común a la hora de, en este proceso de desinformación, estar basándose en medios de dudosa transparencia y credibilidad.

El siguiente paso, que sería el último en esta campaña de desinformación, sería el uso automatizado de redes sociales, lo que conocemos como *bots,* que vamos a ver es un fenómeno bastante más complejo. Por ejemplo, en el caso del que les estaba hablando de Francia, tenemos esta cuenta digital, que está siendo la más activa dentro de la comunidad de los chalecos amarillos, que está produciendo una media de 752 mensajes por día. Puede haber un consenso general en que es bastante difícil que un ser humano publique 752 mensajes al día sobre un tema en concreto. O es una persona muy obsesionada o es una máquina que sigue las órdenes de un Gobierno, de una institución o de un grupo de personas que tienen una agenda oculta y que, de manera maliciosa, están intentando interferir en el debate con una metodología muy concreta. Quiero ponerles un ejemplo de España, el perfil de Ivan 226622. A veces los robots son muy fáciles de detectar; en este caso con un análisis de *big data* sobre la conversación digital de los chalecos amarillos se puede identificar cuál es el perfil digital más activo y, con un análisis manual, viendo la actividad que tiene y cuándo se creó la cuenta —en este caso en agosto de 2018— se ve que no tiene un comportamiento humano. Pero cada vez es más complicado detectar estas cuentas de comportamiento no humano. Aquí se puede ver el caso de Ivan 226622, que es una persona que tiene rostro; he editado la imagen, pero aquí se le ve compartiendo una cena con cuatro mujeres en un restaurante asiático. Dice que le gusta la tecnología, los negocios y las noticias, y pone una cara sonriente. Lleva en esta red social desde noviembre de 2012 y tiene 1200 seguidores. Podríamos pensar que este perfil es de una persona real o que tiene las características de una persona real. Tenía —porque esta cuenta fue eliminada— un comportamiento bastante humano a la hora de colgar mensajes. Esa cuenta fue una de las más activas en el debate electoral sobre el 1 de octubre en Cataluña en el año 2017. Y precisamente la detectamos por el interés que de repente empezó a tener sobre Cataluña. Resulta que esta cuenta, Rick888 (el león de Judá), era la más activa, y luego aparecía Bobbit (la vida es un viaje y no un destino), y todos ellos aparentaban un aspecto humano. Sin embargo, un análisis más en detalle, fijándose, por ejemplo, en las fotos más compartidas por estas cuentas, permite ver que estaban compartiendo a la vez el mismo contenido; tenían un aspecto humano, parecía que estaban gestionadas por una persona real, pero estaban compartiendo constantemente el mismo contenido. De hecho, aquí hay un ejemplo muy claro: el 4 octubre, a las 9:40 las tres cuentas a la vez dijeron que Kosovo era más serbio que Cataluña español y que por qué la OTAN no estaba bombardeando Madrid. Las tres estaban constantemente diciendo los mismos mensajes. Hay indicios para pensar que estas cuentas, que eran de las más activas y que movían el contenido de un medio extranjero sobre este tema, a pesar de que aparentaban ser humanas eran controladas por una tercera persona o por una institución que tenía un afán de generar desinformación y confusión en torno a un debate polémico o a una crisis política que tenía un país tercero. Este patrón, en el caso del análisis de la conversación digital en Cataluña, se repitió de manera constante. Esta también era una de las cuentas más activas, un *fake* como de Jeremmy Corbyn, y que estaba posteando los mismos mensajes. Si se fijan aquí en las fotos y videos más compartidos, verán que estaba compartiendo el mismo contenido que una cuenta que aparentaba ser de la derecha alternativa en Estados Unidos y, sin embargo, de repente durante esos días solamente hablaba de Cataluña y estaba compartiendo los mismos contenidos. Es decir, fue un patrón seguido de manera constante durante ese caso.

En este otro caso vemos un ejemplo de un grupo subnacional en el caso del Estado Islámico. Se comprueba cómo cada vez que este grupo inicia una campaña de comunicación utiliza de manera masiva *bots*. Este es un análisis hecho también por la empresa Alto Analytics, en la que se puede ver cómo cada vez que el Estado Islámico empieza una campaña, utiliza una serie de *bots* o de robots automatizados para que esta campaña tenga mayor magnitud. Este fenómeno es muy recurrente. Como les he dicho, en el caso de Italia se ve claramente cómo la comunidad antiinmigración tenía 18000 usuarios y generaron 470000 comentarios. En el caso de la comunidad a favor de la inmigración tenemos un comportamiento mucho más natural y orgánico, es decir, había 35000 usuarios que generaron 198000 comentarios. La comunidad antiinmigración, con muchos menos usuarios, creó muchísimos más comentarios, con lo cual, este es un indicador que puede demostrar cierta automatización o una intención maliciosa por aumentar el impacto de esta comunidad antiinmigración en Italia. El caso que les pongo

cve: DSCG-12-CM-131

ahora es de otra investigación en curso, por eso no quiero poner ni el país ni las personas afectadas porque creo que es prudente que nos fijemos más en el fenómeno que en el caso concreto. Se trata de una investigación en curso en la que se está viendo el mismo fenómeno. Esta comunidad está siendo hegemónica en esta conversación digital, y con 50 000 autores está generando casi 6 millones de comentarios, cuando, por ejemplo, otras comunidades que tienen 138 000 autores apenas generan 2 millones de comentarios. En esta comunidad verde vemos un comportamiento orgánico o natural, porque hay trece interacciones por autor, que sería un comportamiento humano, mientras en la comunidad azul, que está siendo hegemónica en la conversación digital, hay 117 reacciones por autor, por lo que hay indicios en este comportamiento de que puede haber una automatización maliciosa. Hay otro caso de conversación política de envergadura global en el que observamos el mismo fenómeno. La comunidad hegemónica, en este caso la amarilla, que es la que he puesto antes que además está utilizando dos medios de reciente creación, tiene un comportamiento automatizado en redes sociales o unos niveles de automatización mayor que otro tipo de comunidades que tienen un comportamiento más orgánico.

Recapitulando, la metodología de la disrupción o las campañas de desinformación son un fenómeno mucho más complejo que el de las noticias falsas. Muestro en lo que consisten: analizar las vulnerabilidades de un rival, crear esas narrativas que lo fomenten, crear una red de medios propios y hacer un uso automatizado o malicioso de las redes sociales. Esta es la primera exposición que me gustaría plantearles y que es fruto de la investigación que estoy realizando en torno a diversas campañas políticas en distintos lugares del mundo.

Una vez propuesta mi hipótesis y explicadas mis conclusiones, quedo a la espera de compartir con ustedes sus impresiones y de fomentar un diálogo o de responder a las preguntas que ustedes consideren.

Muchas gracias.

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

Damos comienzo al turno de intervenciones. Les recuerdo a ustedes los compromisos de tiempo que tiene nuestro compareciente y, por tanto, les ruego la máxima brevedad.

Por el Grupo Parlamentario Mixto, el senador Yanguas.

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

Quiero agradecerle al señor Lesaca sus amplias explicaciones y también su disponibilidad de estar hoy aquí a través de videoconferencia. Se nota su labor de docente, porque el discurso ha sido bien elaborado e incluso me atrevería a decir brillante. Además, creo que donde está usted son las seis de la mañana, por lo que redoblo el agradecimiento por la disponibilidad de estar hoy con nosotros y abrirnos los ojos en una cuestión importante, como es la guerra de la desinformación.

El ponente ha abordado este tema de actualidad: la desinformación, y sobre esto el anterior compareciente —no sé si ha podido verlo—, el general Sanz Roldán, ya nos ha dicho que la inteligencia artificial podría ayudar a evitar la desinformación porque evitaría muchas *fake news*. Usted también ha señalado que esto es mucho más que noticias falsas, que es una auténtica guerra de la desinformación. Le querría preguntar si usted está de acuerdo en que la inteligencia artificial nos va a ayudar a luchar contra esta guerra de la desinformación.

Para no alargarme, quiero enviar al ponente, enviarte, un gran abrazo de mi parte y de Carlos Salvador, diputado de Unión del Pueblo Navarro, porque por tu condición de navarro —aunque no lo has dicho— nos conocemos desde hace muchos años y te deseamos que sigas cosechando muchos éxitos.

Muchas gracias, buenos días y enhorabuena por este excelente trabajo que nos has expuesto.

El señor **PRESIDENTE:** Muchas gracias.

Señor Xuclà.

El señor **XUCLÀ I COSTA:** Muchas gracias, señor presidente.

Muchas gracias, profesor Lesaca. Soy Jordi Xuclà, diputado del Partit Demòcrata Català. Gracias por su exposición en la que pinta un panorama muy complejo. Cierto es que no hubo tanques en Barcelona el día 1 de octubre. Como ha citado las fuentes de otros ejemplos, es bueno que se cite que en este caso fue *Russia Today,* pero no quiero gastar los minutos de mi intervención en este ámbito, porque lo que se produjo, el día 1 de octubre de 2017, en Barcelona fue una represión policial, que fue un grave error político y de manejo de la gestión de la crisis.

Dicho esto, usted nos ha planteado científicamente la existencia de burbujas de información que producen una grave polarización. Desde el punto de vista de la lucha contra las mentiras —se pueden

cve: DSCG-12-CM-131

denominar *fake news*—, ¿cómo deben reaccionar la comunidad de inteligencia, la política y la sociedad? ¿Multiplicando o chequeando la verdad y la mentira, cuando usted mismo nos ha planteado la existencia de páginas de verdad que eran falsas? Es difícil; le planteo el problema, no le planteo la solución. ¿Cómo reaccionamos, multiplicamos?

Hace muy pocos meses en España se produjo un incremento —nada que decir, votaron los ciudadanos— de un partido político que está en el Parlamento andaluz, que se llama Vox, que creció en días a través de los *whatsapp* reenviados a través de noticias exageradas o basadas en mentiras, que impactaron especialmente en personas mayores. Me gustaría saber si usted tiene datos sobre el impacto de las noticias falsas entre la población joven y entre determinados segmentos de buena gente mayor que se lo cree todo y lo reenvía absolutamente todo.

Me gustaría preguntarle si cree que se puede producir una fatiga por saturación. A veces la gente abandona Twitter o las redes sociales, porque es muy *cool* y muy minoritario, pero me gustaría saber si es también puede producirse una fatiga por saturación. Perdón porque aquí no hemos venido hablar de libros, pero me gustaría que me dijera si el contenido de *21 lecciones para el siglo XXI,* del profesor Hariri, es algo fiable o es una perspectiva a medio plazo.

Para terminar —yo soy un abogado de provincias, que no sé mucho de ingeniería—, hablando de los chalecos amarillos y de la página web que genera más de 700 tuits al día, ¿una máquina fabrica los tuits o hay una orientación y unos algoritmos que cruzan mensajes? ¿Estamos hablando de personas o de máquinas que generan los mensajes de cada uno de los tuits?

Muchas gracias.

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

Señor Legarda.

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

Me sumo a las felicitaciones de los portavoces que me han precedido en el uso de la palabra. Dado del tiempo del que disponemos, seré muy breve. Nos ha expuesto el diagnóstico de un problema, pero me gustaría preguntarle, y que nos contestara aunque fuera de manera sumaria, cuál sería el tratamiento ante esta situación, y si la inteligencia artificial puede ser un problema. Me gustaría que nos dijera qué otras alternativas tendríamos en este momento frente a este diagnóstico disruptivo en las sociedades democrático-liberales.

Muchas gracias.

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

Senadora Angustia.

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

Buenos días, señor Lesaca. Gracias por su exposición, y sobre todo por la disponibilidad con el tiempo limitado con el que contaba y las horas que son. Dada la limitación que tenemos y la propia que tendrá el compareciente para responder con comodidad a las cuestiones, propondría, si el señor presidente y el señor Lesaca me lo permiten, que pudiésemos trasladar por escrito todas las cuestiones que traíamos preparadas, y el señor Lesaca pueda responderlas. Lo digo por una razón: yo traía un gran bloque sobre gestión institucional de la ciberseguridad para saber si el modelo que seguimos con diferentes organismos es estable en este momento y responde a las nuevas necesidades a las que tenemos que responder, si la propia configuración de nuestras estructuras nos facilita responder para que nuestra protección sea efectiva o no; traía un segundo gran bloque sobre libertad de expresión y desinformación, queriendo saber la opinión del señor Lesaca sobre si él considera que nuestra seguridad está amenazada por la desinformación, y muy en concreto en el marco de las redes sociales por las *fake news,* pero tenía muchas más preguntas; y un tercer gran bloque en el que queríamos conocer su opinión sobre el real decreto-ley que traspone la Directiva NIS; queremos saber si cree que son efectivas las medidas que se han puesto en marcha ya, en el primer trimestre de vida, si los protocolos de petición de notificación a las empresas de los ataques e incidentes que puedan surgir son suficientes para la prevención, y sobre todo si a través de esta normativa hemos conseguido generar un plus de seguridad en el marco social en torno a nuestra protección de ciberseguridad. Reitero si es posible la propuesta de trasladar por escrito al compareciente estas tres páginas, y agradecerle de nuevo su precisión y sobre todo lo pedagógico de la exposición que acaba de hacer.

Muchas gracias.

cve: DSCG-12-CM-131

El señor **PRESIDENTE:** Gracias, señora Angustia.

Señor Lesaca, si está de acuerdo con esta propuesta le haríamos llegar esto por escrito, naturalmente esperando que conteste en aquellas cuestiones que sean de su competencia académica, porque hay algunas que dudosamente entran en su campo de investigación.

¿Está de acuerdo en que las remitamos por escrito y usted nos envía las contestaciones por escrito?

El señor **LESACA ESQUIROZ** (doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia): Sí, sí, no hay problema.

El señor **PRESIDENTE:** Gracias. Así lo haremos.

Damos paso ahora al señor Luena.

El señor **LUENA LÓPEZ:** Gracias, presidente.

Profesor Lesaca —iré rápido, porque sabemos que no tiene tiempo—, si estamos en guerra habrá que ganarla, y desde ese punto de vista, ¿qué herramientas concretas tiene la ciberseguridad de los Estados nación, de las democracias liberales a las que usted ha aludido para ganar esa guerra, y en concreto cómo ve en las diferentes facetas a España para librar esa guerra, y qué riesgos tiene España como Estado nación y democracia liberal en otros Estados para afrontar y ganar esa guerra. Ha hecho alusión a muchos temas concretos, pero le pregunto, por ejemplo, qué nos puede usted decir de la injerencia rusa, de la Federación Rusa como Estado en determinados asuntos públicos de España. Segundo, qué grado de conciencia pública e institucional cree usted que hay en este país sobre la penetración de ese riesgo, del peligro para las democracias de la desinformación masiva. Tercero —el diputado Xuclà ha aludido al profesor Harari—, ¿puede ser que esta sea la primera vez en que la humanidad crea un fenómeno tecnológico que puede acabar dominando a la propia humanidad?

Gracias.

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

Señor Romero.

El señor **ROMERO SANTOLARIA:** Muy brevemente.

Bienvenido, señor Lesaca. Le agradezco su brillante intervención y también su interesante conferencia, por la que quiero felicitarle.

En primer lugar, le agradezco, en nombre del Partido Popular, su participación en esta Comisión, máxime reconociendo el esfuerzo que ha realizado para hacer posible esta comparecencia, a través de videoconferencia. De sus palabras deduzco —espero no estar equivocado— que tenemos una excesiva dependencia de las redes sociales, y haciendo analogía de su libro creo que hemos convertido las redes sociales en nuestra arma de seducción masiva.

Ha hablado usted en su conferencia de ruptura de ese contrato social, de la desconfianza en las instituciones y de una confianza débil ante los medios de comunicación, que son cuestiones preocupantes; ha hablado de desinformación como arma de guerra, pero ha habido una frase que ha lanzado usted y que me ha preocupado, y es la siguiente: manipular lo que los ciudadanos ven y oyen para liderar la opinión pública, todo ello con el objetivo de crear confusión. Creo que eso es dramático. A ese respecto, siendo coincidente con otros compañeros, por ser breve, le preguntaría qué podemos hacer frente a esta cuestión desde las instituciones públicas.

Haré referencia también a una intervención suya en un desayuno, creo que el año pasado. Usted hizo al auditorio una pregunta que no sé si la podremos responder nosotros, y me gustaría que usted, si tiene datos al respecto, lo pudiera hacer. La pregunta era: ¿sabemos quién toca el tambor de las sociedades actuales?

Muchas gracias.

El señor **PRESIDENTE:** Ahora doy la palabra al señor Lesaca para que conteste lo que pueda contestar en esta intervención oral, dejando para un momento posterior las contestaciones a las preguntas que le formulemos por escrito.

El señor **LESACA ESQUIROZ** (doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia): Señor presidente, ¿de cuánto tiempo dispongo?

cve: DSCG-12-CM-131

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

El señor **LESACA ESQUIROZ** (doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia): De acuerdo.

En primer lugar, muchas gracias a todos por sus planteamientos. Han hecho las preguntas pertinentes y les agradezco su comprensión y su amabilidad en la exposición de las mismas. Un saludo, por supuesto, al senador Patxi Yanguas y a Carlos Salvador, es un placer verles, aunque sea por videoconferencia.

Voy a agrupar, si no tienen inconveniente, las respuestas por áreas temáticas. Me han preguntado por el tema de la inteligencia artificial, de cómo se pueden detectar estas campañas y si sabemos quién toca el tambor. Actualmente existen *softwares* de análisis de *big data* y hay que partir de la premisa de que todas estas campañas de desinformación se producen en fuentes públicas y abiertas, es decir, no estamos hablando de campañas que se producen en redes ocultas o en la Internet profunda, sino que son fuentes públicas y abiertas, y aunque probablemente los ciudadanos no sean conscientes, son mensajes públicos; es decir, cuando una persona se expresa en Facebook automáticamente pierde su control sobre los mensajes que pone en Facebook, en Twitter o en cualquier otra plataforma. Los mensajes se convierten en mensajes públicos que pueden ser monitoreados de manera legal. Cuando hablamos de monitorización de redes sociales no estamos hablando de herramientas de espionaje, sino que estamos hablando de monitorización de redes sociales públicas abiertas, que es una cosa absolutamente legal y legítima, y de hecho prácticamente la mayoría de grandes empresas de España, de Europa o de otros países utilizan de manera recurrente *softwares* de *big data* para leer los comentarios de redes sociales de la opinión pública, y detectar cuáles son los gustos sobre consumo, sobre moda y sobre diferentes asuntos, y en función de eso las empresas toman decisiones comerciales. De la misma manera los *softwares* que utilizo para mi investigación, en este caso la empresa española que he citado tiene la capacidad para analizar grandes volúmenes de conversaciones digitales; es decir, todo lo que los ciudadanos publican en redes abiertas se puede monitorear, y en función de esto se pueden detectar las anomalías que he expuesto en esta comparecencia, con lo cual sí que es posible detectar las anomalías que se producen en una conversación digital. ¿A qué me refiero con anomalías? Pues al uso automatizado de redes sociales, a la aparición de medios nuevos o desconocidos que de repente tienen gran influencia en conversaciones. Todo esto se puede detectar hoy en día.

¿Qué no se puede detectar o qué no se puede probar científicamente? De momento hay dos lagunas en el mundo académico, y son dos grandes lagunas —lo quiero reconocer— en el ámbito de la desinformación, que son: probar la atribución y probar la causalidad. Es decir, yo puedo probar, como ha dicho el señor Xuclà, que hay unas páginas de un país extranjero que tiene mucho interés en la crisis política de Cataluña de octubre, pero no puedo probar que el Gobierno de ese país esté involucrado en esa acción. Es decir, puedo probar que hay una serie de indicadores que demuestran que agentes de ese país tuvieron mucho interés en un tema de otro país, pero no puedo probar que hay una conexión directa con un Gobierno como autor directo de esa acción. ¿Qué no se puede probar tampoco, que es el gran debate en Estados Unidos, por ejemplo? La causalidad. Es decir, se puede probar que un país extranjero intentó de manera maliciosa pagar una serie de anuncios en una campaña electoral extranjera, pero no se puede probar si eso realmente influyó en la toma de voto de los ciudadanos. Es decir, se puede probar la intención, pero no se puede probar de momento si eso realmente influyó en las campañas. Pero, bueno, sí que existen hoy en día herramientas suficientes para detectar que en una campaña electoral o en un proceso político complejo se están produciendo una serie de injerencias de manera maliciosa.

¿Qué se puede hacer? Desde luego, la primera medida es respetar siempre. Creo que es un tema complejo en el sentido de que estamos legislando sobre libertad de expresión y sobre asuntos que de momento muchos de ellos no están tipificados como delitos. Es decir, publicar una noticia falsa de momento no es un delito, podrá ser una mala práctica, pero no es un delito; utilizar un robot para generar mensajes es una mala práctica, pero no es un delito. Con lo cual yo creo que lo que se puede hacer es institucionalizar la monitorización de ese tipo de campañas para detectar la mala praxis o los intentos maliciosos por alterar una conversación digital.

¿Qué más se puede hacer? Desde mi punto de vista es fundamental el tema de la *wordness* o de la denuncia pública. Creo que es muy importante denunciar a aquellos medios que no están siguiendo unas buenas prácticas o que no tienen la transparencia necesaria; creo que es importante advertir a los ciudadanos de la importancia de consumir bien. De la misma forma que hemos estado muchos años advirtiendo a los ciudadanos de la importancia de que fumar mata, de que consumir comida basura

cve: DSCG-12-CM-131

produce problemas de salud, es importante enseñar a los ciudadanos a consumir bien medios de comunicación, a informarse bien de diferentes fuentes, de fuentes plurales, no permitir que los ciudadanos se informen mediante unos algoritmos y sean los algoritmos los que si yo pienso de manera A, cada vez que enciendo el ordenador solo voy a recibir mensajes que van a reforzar mi manera de pensar A, y eso es perjudicial. Es decir, los ciudadanos tienen que ser conscientes de que de manera proactiva tienen que buscar noticias en diferentes medios para formarse una opinión pública, y creo que eso precisa de campañas de concienciación.

De igual manera creo que es importante establecer un diálogo con las empresas o regularlo de manera directa. En este asunto las plataformas digitales tienen una gran responsabilidad con el tema de los famosos algoritmos. Muchas veces las decisiones sobre cómo nos informamos no las toman ya ni siquiera personas, sino que son algoritmos, robots, *softwares* los que deciden de qué manera nos estamos informando, y yo creo que es importante abrir esos debates. La creación de estas cámaras de opinión que están generando las plataformas no es sano para una democracia.

Comentaba el señor Xuclà el impacto de noticias falsas. Es muy difícil medir el impacto de las noticias falsas, es la gran carencia del área de la academia. Hay que desarrollar metodologías para ver de qué manera están impactando. Hemos dicho que podemos probar el dolo, la mala intención, pero todavía es muy difícil probar hasta qué punto o qué consecuencias tiene, si realmente eso ha sido influyente o no en una campaña electoral.

El tema de los mensajes, si los producen ordenadores o si los producen personas, bueno los ordenadores funcionan en función de las claves o de las instrucciones que les da una persona, con lo cual, por ejemplo, este caso que les he puesto de los chalecos amarillos, es una máquina la que está generando todo este tipo de contenido, pero la máquina lo genera en función de las órdenes que le ha dado una persona, que en este caso digamos que consistía en generar mensajes o interactuar con todo tipo de contenido a favor de una determinada posición política que le está haciendo daño a un país, con lo cual, sí, son robots pero siempre los robots reciben órdenes de personas.

Me han preguntado sobre si tenemos una excesiva referencia a redes sociales. Esta es una pequeña impresión subjetiva, pero yo creo que precisamente este es el debate. Hay una comparación, no recuerdo ahora mismo al autor, aunque desde luego no me voy a atribuir yo esta conclusión, pero he leído ya en varios lugares que de la misma manera que el Estado nación no se entiende sin la creación de la imprenta digital, que fue lo que permitió aglutinar el conocimiento, la razón y en función de eso se funda el concepto de Estado nación, las redes sociales si no se regulan y si no hay unas campañas para enseñar a los ciudadanos a usarlas de manera inteligente pueden acabar con el propio Estado nación, puesto que evidentemente muchos de estos mensajes, como estamos viendo, no están basados en la racionalidad o en la objetividad, sino que están basados en fomentar o apelar a las pasiones más primarias que podemos tener los seres humanos. Entonces creo que es importante que haya una reflexión sobre el uso de estas herramientas sociales. En primer lugar, es importante legislar e intentar regular este campo, pero por otra parte creo que es muy importante, como les he dicho, el tema de la educación y del uso racional, por ejemplo, para evitar los mensajes de odio, para evitar incluso las apelaciones personales. Creo que hay toda una cultura detrás del uso de estas plataformas que no está favoreciendo la mayor de las calidades democráticas.

¿Cómo se debe regular todo esto? Yo creo que ese es el trabajo de instituciones como el Congreso de los Diputados, de los *policymakers,* de las instituciones, y creo que es importante empezar a tomar cartas en el asunto. Por tanto, en el ámbito —por resumir un poco las respuestas— de la detección existen herramientas que permiten detectar las campañas maliciosas, existe capacidad legislativa para regular por ejemplo el uso del anonimato en redes sociales, que creo que es una auténtica lacra, la creación de algoritmos que solo favorecen el reforzamiento de ideas muchas de ellas profundamente negativas, y la creación de medios que no tienen ningún tipo de trazabilidad. Voy a poner otro ejemplo alimentario: de la misma forma que estamos exigiendo a los alimentos que haya una trazabilidad en el origen, desde de qué se alimenta la vaca, en qué granja está consumiendo, hasta que llega al plato del usuario, creo que es importante también exigir, tanto a determinados medios de comunicación como a determinadas plataformas, de qué manera están proyectando la información, cuáles son las fuentes que utilizan, cuál es el proceso de comprobación de los datos. Creo que esto es bastante importante, porque al final de lo que se alimenta la opinión pública es de la manera en que sale la opinión pública. Y luego está el tema de educar para, desde la más temprana infancia, hacer un buen uso de estas herramientas de la comunicación, porque lo que está en juego no es simplemente la calidad democrática, sino probablemente

cve: DSCG-12-CM-131

lo que está en juego es la propia supervivencia de los Estados nación y de las democracias liberales, y eso ya son palabras mayores. No sé si lo que puede venir después de un Estado nación es algo mejor o peor, pero desde luego genera inquietud.

Espero haber respondido a gran parte de las preguntas, aunque lo he hecho de manera bastante resumida; en cualquier caso, como le he dicho al presidente, tiene mi correo electrónico y estaré encantado de responder de manera más pausada y detenida a cuestiones más concretas por correo electrónico.

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

Haremos uso de esa posibilidad que usted nos ofrece de ampliar nuestros interrogantes vía *email* y le agradezco de antemano sus respuestas; y ya no de antemano, sino actualmente, su intervención en este momento. Así que muchísimas gracias y buen día.

El señor **LESACA ESQUIROZ** (doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia): Muchas gracias a todos; ha sido un placer. **(Pausa).**

— DE LA SEÑORA SUBSECRETARIA DEL MINISTERIO DEL INTERIOR (GOICOECHEA ARANGUREN), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/002362 y número de expediente del Senado 713/001148).

El señor **PRESIDENTE:** Vamos a continuar, señorías, porque ahora sí que vamos contrarreloj.

Bienvenida, y yo pediría a la subsecretaria que en diez minutos nos haga sus reflexiones, y estoy seguro de que cumplirá con este ruego. Señora subsecretaria, suya es la palabra.

La señora **SUBSECRETARIA DEL MINISTERIO DEL INTERIOR** (Goicoechea Aranguren): Muchísimas gracias, presidente.

Señorías, diputados, senadores, voy a hacer todo lo posible por entrar dentro de ese periodo de tiempo que se me ha dado, pero es cierto que habíamos pensado que la intervención inicial iba a ser un poquito más larga. Espero no alargarme demasiado y procuraré seguir estas notas que traigo, porque es verdad que es mucho lo que se hace desde el ámbito del Ministerio del Interior, y en concreto desde la subsecretaría, en materia de procesos electorales, y me gustaría que pudiera quedar reflejado. Aunque también soy consciente plenamente de que han escuchado a tantos expertos en esta materia que posiblemente nada de lo que yo diga va a poder ser sorprendente en este momento. Lo que espero es que pueda aportar algo desde un ámbito que no es estrictamente el informático; nosotros no somos los competentes directos del departamento en materia informática, pero sí es cierto que asumimos la responsabilidad en materia de procesos electorales, y eso supone también asumir la responsabilidad de coordinación de los distintos órganos que, dentro del ámbito del propio departamento ministerial y de otros departamentos, tienen competencias y recursos para asumir las responsabilidades en materia de seguridad informática, de ciberseguridad, que es lo que aquí nos trae.

Desde luego las nuevas tecnologías han irrumpido en nuestra vida y lo han hecho, tanto en nuestro ámbito privado como también en nuestro ámbito público. Eso, además de muchas más capacidades de gestión y de actuación y la facilidad para hacerlo de la que disponemos todos en este momento, supone también un incremento de los riesgos. Y de ello tenemos que ser plenamente conscientes. Hablaba con el secretario de esta Comisión de tiempos anteriores. Estuve durante unos años en el ámbito de las tecnologías de la información —en la Secretaría General de Administración Digital— y de verdad que, como le decía a él, sin conocimiento directo, lo que sí pude hacer durante ese tiempo fue asomarme a la realidad que supone la capacidad infinita que tiene la informática de transformación de nuestros procesos, de nuestra capacidad de gestión, pero también pude ver los riesgos que esto supone para nuestra actuación privada y pública. De modo que desde que llegamos al ministerio una de las preocupaciones lógicas que hubo que asumir, dentro del ámbito de la subsecretaría, era la de los riesgos que podían suponer los ataques cibernéticos para los procesos electorales, que forman parte de las competencias de mi subsecretaría. En nuestro país desde luego no es una preocupación nueva y no es nuevo tampoco el escenario al que nos estamos enfrentando.

Yo formo parte de la Administración como funcionaria, y soy consciente de que lo que tenemos es un procedimiento continuo de trabajo entre los distintos equipos, y cuando llegamos al departamento nos encontramos con que ya en los años 2015 y 2016 se había visto que había habido distintos tipos de amenazas cibernéticas en los procesos electorales que se habían desarrollado, y así lo puso de manifiesto

cve: DSCG-12-CM-131

el CNI, concretamente el Centro Criptológico Nacional, detectando vulnerabilidades que nos fueron comunicadas y que dieron lugar a continuar ese proceso de reflexión y de adopción de medidas, que ya en el ámbito de la Dirección General de Política Interior sus técnicos estaban abordando. De hecho las medidas que se han ido adoptando y que quiero transmitirles —voy a ver si consigo hacerlo con brevedad— comenzaron ya desde la misma configuración de un acuerdo marco; un acuerdo marco que es la decisión administrativa que se tomó, el recurso administrativo para facilitar la disponibilidad para el Gobierno, para las estructuras de gestión del Ministerio del Interior, de la capacidad de contratar en el menor tiempo posible el contrato más importante de un proceso electoral, que es el contrato de difusión del escrutinio provisional de resultados. Esa decisión, adoptar un acuerdo marco que pretendía durante cuatro años de vigencia que se pudiera, con absoluta rapidez y seguridad, contratar a la empresa que fuera a gestionar esos procesos electorales, desde el momento que se concibió ya se hizo sabiendo que el tema cibernético, el tema de seguridad informática tenía que ser uno de los componentes fundamentales, y se tuvo en cuenta desde un primer momento. Luego me referiré a él dentro del contexto general desde el que estamos abordando el tema de la ciberseguridad.

Nuestra responsabilidad como Ministerio del Interior es garantizar que las elecciones transcurran con absoluta transparencia, con objetividad, con seguridad; debemos ser garantes de ese procedimiento absolutamente democrático y garantizar el ejercicio del derecho al voto de todos los ciudadanos. Afrontamos tres elecciones en un día; eso es algo que ocurre cada veinte años, cada veinte años se produce esa concurrencia y sabemos que es un reto importante, pero ese es un reto que queremos abordar como Gobierno poniendo en juego todas las capacidades que tiene la Administración del Estado. Han pasado ya distintos responsables por aquí. El Estado tiene distintos órganos competentes y con una experiencia y unas capacidades muy importantes para dar garantías también en materia de ciberseguridad al desarrollo de esos procesos electorales. Esa experiencia acumulada es la que hemos llevado al diseño de una supraestructura, de una estructura con la que pretendemos establecer un modelo de gobernanza para que el proceso electoral transcurra con plenas garantías de seguridad.

Cuando hablamos de seguridad —lo hago yo como subsecretaria del Ministerio del Interior— tenemos que ser conscientes de que hablamos también lógicamente de seguridad física y no solo de seguridad en información y ciberseguridad. Lo digo por dar un contexto general en materia de seguridad, dado que nos corresponde al mismo departamento ministerial. Por lo que se refiere a la seguridad física, somos todos conscientes. Dentro del ámbito de responsabilidad de la Secretaría de Estado de Seguridad nos corresponde el funcionamiento de fuerzas y cuerpos de seguridad, en colaboración con los responsables de los cuerpos de seguridad de las comunidades autónomas y de las entidades locales. Pero también garantizaremos la seguridad con toda la infraestructura material que desde la Dirección General de Política Interior hay que poner en marcha, en colaboración con delegaciones y subdelegaciones del Gobierno, para el desarrollo de todo este proceso. Estamos hablando de tres comicios que van a suponer la elaboración y puesta a disposición de —a mí es que el número me impresiona desde que llegué aquí— mil millones de papeletas, y de todas las urnas y de todas las cabinas que hay que poner en marcha. Lo haremos. Y vamos a abordar además la seguridad en información y ciberseguridad.

Las actuaciones que vamos a llevar adelante, como decía antes, van a ser actuaciones coordinadas con todos los órganos competentes en la Administración del Estado. Lo que hemos venido haciendo —y en cierto modo estamos haciéndolo todavía— es preparar esas tres elecciones, y trabajar todos los órganos en la configuración de esa estructura que una todos los recursos posibles de seguridad de la Administración, dotándonos de un modelo de gobernanza y un protocolo de actuación que nos permita ser eficientes. Lo que hacemos es, tomando la experiencia de los procesos anteriores, intentar establecer un sistema —y estoy convencida de que lo vamos a conseguir— en el cual seamos plenamente garantes de que cualquier riesgo que pueda suscitarse en materia de ciberseguridad sea detectado precozmente, y una capacidad inmediata de actuación, y de actuación ejecutiva, para garantizar que los comicios se celebren con absoluta normalidad. Para ello contamos, desde la Dirección General de Política Interior, con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad, el CNPIC —también del departamento de Interior—, la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, y la Subdirección General de Calidad de los Servicios e Información, desde el ámbito de nuestro departamento ministerial.

¿Qué papel ha jugado y está jugando la Dirección General de Política Interior que depende de la subsecretaría? Ese papel está siendo fundamental desde el momento en que se concibió ese acuerdo marco al que me he referido antes. El acuerdo marco para el contrato de difusión del escrutinio provisional

cve: DSCG-12-CM-131

ha pretendido incorporar todas las sugerencias en materia de seguridad que el CNI y el CCN nos han facilitado después de la evaluación, después de la auditoría realizada de los procesos electorales anteriores, especialmente 2015 y 2016. Por primera vez en un acuerdo de este tipo se ha incorporado ya desde los pliegos de contratación todos los requerimientos de seguridad que estos órganos especializados que antes he citado han considerado imprescindibles para la seguridad. Lo que hemos hecho ha sido asumir en primera persona desde la subsecretaría, desde la Dirección General de Política Interior, cuáles son esas prescripciones de seguridad, no dejando que sean únicamente las empresas, la empresa que resulte adjudicataria del contrato, la que asuma el diseño de seguridad y la que asuma también cuáles tienen que ser esos estándares de seguridad. Se han establecido ya en el pliego de contratación. Se ha hecho algo más y eso es muy importante. Lo que se ha incluido también en ese contrato marco es la necesidad de realización de una auditoría de seguridad por aquellas empresas que se presentaron a ese acuerdo marco. Esto significa que sobre aquellas empresas que se presentaron —y fueron una UTE y una empresa— se realizó esa auditoría de seguridad con carácter previo a la adjudicación del contrato. Por tanto, se trata de intentar garantizar desde un primer momento que respondan a los estándares de seguridad que se consideran imprescindibles para que un proceso en este momento —en el que, como digo, la informática nos ofrece muchísimas posibilidades, pero también nos abre una enorme ventana de riesgo— se pueda desarrollar con la mayor seguridad posible. Estas auditorías se han realizado con fase previa a la adjudicación y, obviamente, sobre esos sistemas y aplicaciones piloto que ofrecían estas empresas como su aportación para la realización del contrato en caso de que les fuera adjudicado. La implementación y desarrollo de los sistemas y aplicaciones reales adaptados al proceso electoral concreto está exigiendo, porque ya ha sido adjudicado, de la empresa adjudicataria la realización de todo un diseño, implantación e implementación de un modelo de seguridad. Ese trabajo se está haciendo ya en colaboración con el Ministerio del Interior y con los órganos del Ministerio del Interior que antes he citado. Por tanto, hay un trabajo desde el primer momento de colaboración que hasta ahora no se ha venido realizando de esta manera, pero insisto en que la experiencia adquirida nos aconseja que así se haga y así lo estamos haciendo. En este momento, la empresa que ha resultado adjudicataria del contrato de difusión de resultados provisionales, una UTE conformada por Scytl y Vector, un contrato que se firmó el pasado 31 de enero, se ha puesto ya en marcha con trabajos técnicos para poder asumir las labores del día 26 de mayo con absoluta seguridad. Desde el pasado 11 de febrero estamos ya llevando a cabo reuniones conjuntas con los órganos técnicos del ministerio y con el asesoramiento del CCN y del CNI para poder llevar a cabo los procesos electorales con la mayor seguridad posible.

Por lo que se refiere a las actuaciones por parte del Centro Nacional de Protección de Infraestructuras y Ciberseguridad, del CNPIC, se va a llevar a cabo la puesta en marcha de un dispositivo extraordinario de ciberseguridad. El gabinete, centrado en los próximos comicios, va a poner en marcha ese dispositivo que tendrá que llevar a cabo una especial vigilancia efectiva y un seguimiento proactivo de las diversas acciones y hechos que pudieran ocurrir en el ámbito cibernético para proceder a la difusión de la información entre los distintos actores que participan en la difusión de la información de estos procesos electorales, las juntas electorales y las comunidades autónomas que participan también en este proceso, así como las delegaciones y subdelegaciones del Gobierno que materialmente colaboran en su realización. El dispositivo extraordinario que se propone se basa, en primer lugar, en la obtención y análisis de información de diversas fuentes. Esto persigue la elaboración de informes coordinados, periódicos y sistemáticos para desplegar medidas preventivas o reactivas en su caso en el menor tiempo posible y con la mayor eficacia que sea posible. En segundo lugar, se pretende también apoyar a la Junta Electoral Central y a los otros actores que tienen parte en este proceso. Asimismo, se pretende un enlace eficaz con el ministerio fiscal y con la junta electoral ante el conocimiento de cualquier incidente que será puesto en su conocimiento para actuar con la mayor diligencia posible. Por último, una información constante sobre los ataques que se puedan estar produciendo para la elaboración de manuales, guías de procedimiento y también para una adecuada respuesta a los mismos. Este dispositivo prevé la recopilación de información procedente de las distintas fuentes para que, con los protocolos de los que nos estamos dotando, estamos trabajando con ello, llegue la información a quienes tienen que tomar la decisión en el menor tiempo posible, y que la información sea especializada para cada órgano para que no se produzca lo que en ocasiones suele ocurrir, que llegue un exceso de información duplicando esa información, con lo cual se retrasa la capacidad de análisis y, por tanto, de toma de decisión o que se generen ámbitos en los que no se produzca esa información y, por tanto, no se pueda tener la respuesta que sea imprescindible. Este dispositivo que se ha propuesto se ha hecho lógicamente en colaboración con las Fuerzas y Cuerpos de

cve: DSCG-12-CM-131

Seguridad del Estado, con la Subdirección General de Sistemas de Información y Comunicaciones, el Instituto Nacional de Ciberseguridad, el Incibe, el Centro Criptológico Nacional y el Mando Conjunto de Ciberdefensa del Ministerio de Defensa. Insisto mucho en ello porque, como en otros ámbitos de gestión de la subsecretaría, consideramos que lo que hay que hacer es sumar todas las capacidades de todos los elementos que tienen conocimiento, capacidad de información y capacidad de respuesta hacia lo que pueda producirse. Nosotros nos guiamos por la máxima de que hay que sumar capacidades y de que tenemos que trabajar en absoluta colaboración y en líneas transversales de funcionamiento.

En cuanto a la seguridad de la información, lo que hemos hecho también es poner en marcha algo que hasta ahora no teníamos, que es la aprobación de una política de seguridad de la información que se aprobará en breve. Esta política de seguridad de la información en el ámbito de seguridad lógicamente está alineada con el esquema nacional de seguridad en el ámbito de la Administración electrónica. Nuestra propuesta es garantizar que los sistemas de información que integran el servicio de difusión de resultados provisionales en procesos electorales cuenten con los más elevados niveles de confidencialidad, disponibilidad e integridad, debido principalmente al grado de criticidad de la información y la grave repercusión que puede tener para la ciudadanía en caso de que se produzca algún ataque. Esta política desarrolla una estructura organizativa en la que participan los órganos superiores y directivos a los que me estoy refiriendo constantemente.

Voy a señalarles ahora, señorías, si me lo permiten, algo en relación con la Unión Europea y cuál es el papel que jugamos y que juega la Unión Europea en todo este proceso. Desde Bruselas se está poniendo especial énfasis en esta cuestión con ocasión de la celebración de las elecciones al Parlamento de 2019, conscientes como son de los ataques que han sufrido distintos procesos electorales en los tiempos pasados. Ese interés de la Comisión Europea se puso especialmente de manifiesto el pasado 12 de septiembre 2018 mediante una recomendación, la de creación de una red nacional en materia de elecciones. Pues bien, sobre ello era sobre lo que estábamos trabajando y precisamente esa recomendación incide en lo que hasta ahora les he venido comentando, en la necesidad de coordinación y en el desarrollo de ese protocolo común de trabajo y en ese modelo de gobernanza coordinado en el que hemos estado trabajando con los distintos órganos de la Administración del Estado. Todo ello se ha plasmado en la configuración de una red nacional que hemos comunicado a la Reper hace escasamente veinticuatro o cuarenta y ocho horas en la que participan los órganos que antes he citado y que conformará en un futuro esa red europea. Además, hemos aprovechado incluso esa recomendación europea para hacer extensiva esta red nacional a los otros procesos electorales a los que nos enfrentamos también en este país próximamente. Es una red en la que lógicamente cada órgano antes citado participa obviamente dentro de su ámbito competencial y que tiene, como no podía ser de otra forma, al ministro del Interior como punto de contacto con la Unión Europea. En esa red participan también, además de los órganos mencionados, el Instituto Nacional de Estadística y participará la Agencia Española de Protección de Datos, así como lógicamente la Junta Electoral Central. Participamos y buscamos el funcionamiento y las garantías en cuatro bloques. El primero de ellos, garantizar que el proceso electoral se lleva a cabo con transparencia y objetividad, acorde con el principio de igualdad, respetando las reglas de juego previstas en el procedimiento electoral. En este bloque va a participar además de la Subsecretaría del Ministerio del Interior a través de la Dirección General de Política Interior, el Instituto Nacional de Estadística, que es el organismo responsable de la conformación del censo electoral. El segundo bloque fundamental es proteger el correcto uso de los datos personales frente a ataques para la utilización indebida, para lo que contamos, lógicamente, con la Agencia Española de Protección de Datos. El tercer bloque de actuación que queda recogido dentro de esta red nacional persigue establecer procedimientos frente al riesgo que representan los ciberataques para los sistemas informáticos de las elecciones, las campañas, los partidos políticos y los candidatos a las administraciones públicas, velando por la seguridad de todos los aspectos informáticos del proceso electoral a través de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad y del CNPIC. El cuarto bloque es, lógicamente, combatir la desinformación en línea y las informaciones falsas, a través de la Secretaría de Estado de Comunicación y del Departamento de Seguridad Nacional, ambos de la Presidencia del Gobierno.

Por último, la Administración electoral, encabezada por la junta electoral —tal y como recoge la Ley Orgánica 5/1985— garantizará la transparencia y la objetividad del proceso electoral y del principio de igualdad. Este dispositivo tiene por objeto llevar a cabo una vigilancia efectiva y un seguimiento proactivo de las diversas acciones y hechos que pudieran ocurrir en el ámbito cibernético para proceder a la difusión de la información a los actores que se consideren especialmente involucrados, en caso de que algo pueda

cve: DSCG-12-CM-131

ocurrir. Nuestra posición, la del Ministerio del Interior, es activar de manera inmediata la red nacional —a la que he hecho antes referencia— dejando claro que apostamos por que tenga un carácter de permanencia. Lo que estamos viendo en este momento en el ministerio, lo que se está configurando, es una red que queremos, creemos y confiamos en que realmente va a actuar como garante de un proceso electoral y, por tanto, creemos también que sería conveniente que esta red se mantuviera con carácter permanente, de tal forma que la activación en caso de procedimientos electorales fuera inmediata y con una capacidad de respuesta también inmediata.

Señorías, vivimos en un momento —y no quiero repetirme más— en que la democracia nos obliga a estar alerta, prevenidos frente a los ataques que puedan desplegar los distintos enemigos que la democracia tiene, pero también vivimos en un momento en el que tenemos muchas capacidades para actuar y esas son las que creemos que estamos poniendo en juego en esta red de alerta, en esta red de actuación inmediata a través del Ministerio del Interior, pero con la colaboración de los distintos departamentos ministeriales competentes. Para ello creo que vamos a aportar, y digo el creo con una cierta modestia, pero no quiero hacerlo sin tampoco aportar la enorme seguridad que da hablar aquí con el respaldo de todos los órganos que he citado. No se trata únicamente de la subsecretaría, no se trata, obviamente, de una reflexión personal; se trata de un equipo, el de política interior, que ha puesto de manifiesto ya su enorme capacidad de respuesta a los retos que los distintos procesos electorales han supuesto, pero también de todos los órganos y sus responsables —que han pasado por aquí— que nos dan como estructura de Estado una enorme capacidad de respuesta y también una enorme capacidad de colaboración desde el principio de lealtad institucional con las comunidades autónomas que tienen que abordar también procesos de una enorme responsabilidad el 26 de mayo. Por ello, es una satisfacción y un honor poder venir aquí sabiendo que lo que tenemos detrás es una estructura con una enorme capacidad de actuación; una capacidad que viene además demostrada por la capacidad técnica de todo el personal, absolutamente profesional, que está desempeñando sus funciones en esos órganos, y también, quiero decirlo, de una empresa que ha resultado adjudicataria después de sufrir un sistema de auditoría por parte de uno de los órganos más exigentes que podemos tener en este país, que es el CCN. Por tanto, creo que podemos aportar en este momento un enorme valor de capacidad de respuesta para dar solidez a uno de los procesos más importantes que vive una democracia, que es el de procesos electorales.

Sin más, termino mi intervención y quedo a disposición de todos ustedes para lo que consideren oportuno. Muchísimas gracias.

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

Vamos a empezar el turno. Como he anunciado anteriormente, señor Xuclà, tres minutos. Procure concentrar dos intervenciones en una.

El señor **XUCLÀ I COSTA:** Muchas gracias, señor presidente. Incluso no agotaré los tres minutos.

Señora subsecretaria, gracias por su comparecencia. Me voy a centrar en la parte de su intervención más directamente vinculada con los trabajos de esta Comisión mixta Congreso-Senado. Usted nos ha trasladado a esta Comisión mixta que en el pasado ya se han producido ataques cibernéticos durante procesos electorales en España. Me gustaría que nos ilustrara y profundizara sobre este particular que ha trasladado a esta Comisión.

Muchas gracias, señor presidente.

El señor **PRESIDENTE:** El señor Salvador no está. Señora Angustia.

La señora **ANGUSTIA GÓMEZ:** Gracias, presidente. Buenos días, señora subsecretaria.

Voy a empezar por una cuestión que no es, evidentemente, de estricta competencia de su subsecretaría en el Ministerio del Interior y, por lo tanto, no está referido específicamente a ella, pero sí, como muy bien decía, porque muchas de las cuestiones son trabajos interministeriales y sí dependen de la coordinación y también supondrán un reto de coordinación en el que se debería ver implicada su responsabilidad. A lo largo del último año se han visto aquí enfrentados dos modelos en torno a cómo se gestiona la desinformación, en torno a cómo se gestionan las noticias falsas. Sobre todo, cobra especial importancia las bases que pongamos a ese modelo cuando hablamos de procesos electorales, por una cuestión que usted señalaba, porque posiblemente sea uno de los máximos exponentes de nuestros procesos democráticos. Había un plan elevado y propuesto desde el Ministerio de Defensa

cve: DSCG-12-CM-131

durante el Gobierno del Partido Popular que planteaba una censura previa a todas las noticias, un sellado oficial que realizase el Gobierno y que, por lo tanto, implicaba también la eliminación del anonimato, que creemos que es un derecho fundamental que debía de estar contemplado. Existía otro modelo, no diferente sino directamente enfrentado, que es el que planteábamos desde nuestra oposición. Se trataba no solo de que todas las políticas de protección y de regulación del ciberespacio que afectasen a los poderes públicos debiesen estar basados en las materias de derechos fundamentales, del derecho internacional y de la Unión Europea, sino de no utilizar nunca como pretexto para recortar la libertad de expresión este tipo de ataques o de afectaciones a la seguridad y, en último plano, precisamente a lo que usted se refería, que los poderes públicos trabajasen de forma coordinada. ¿Cuáles son las medidas, dentro de este gran proyecto, que están encaminadas en ese marco de trabajo interrelacionado a garantizar que las campañas de desinformación, que las *fake news,* no afectan tampoco a nuestros procesos electorales, en un momento en el que además —se comentaba durante la primera comparecencia— algunos de ellos están incluso judicializados? Por lo tanto, ¿cómo vamos a garantizar que no afecten a lo nuestro?

Me ha quedado clarísimo durante la exposición el programa, los pasos que se están siguiendo y cuáles son, además, los puntos fuertes que se intentaban compensar con respecto al camino que veníamos haciendo. Pero me ha generado dudas: ¿Existe la posibilidad de tener un proceso totalmente telematizado? ¿Existe la posibilidad de implantar ese sistema? ¿Es seguro? ¿No lo es? Sobre la base de esas posibles carencias o problemas que pudiese tener un proceso totalmente telematizado, ¿se está valorando el empezar a caminar hacía el? Paso a formularle la última pregunta y termino, presidente —la capacidad de síntesis no la he tenido a lo largo de toda esta Comisión y hoy era difícil que me viniese de golpe—. Hablamos de contratar empresa privada, hablamos de generar mayores mecanismos —y esto nos alegra— durante las auditorías en un sistema con mayor capacidad de intervención o de ratificación por parte de la Administración publica de ellos, pero ¿no sería mejor, tal vez, pensar en un organismo totalmente publico, independiente, que estructurase todo el proceso, que auditase, que procediese a la recopilación de datos, de escrutinio y a la posterior emisión de estos resultados? ¿No sería mejor tener una gestión totalmente pública a través de un organismo independiente que fuese entonces un poder totalmente independiente de los demás?

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias.

Señor Salvador. No hay relación de causalidad pero sí de coincidencia; en su ausencia hemos respetado —salvo en el último turno— muy bien los límites de tiempo.

El señor **SALVADOR GARCÍA:** No, no se preocupe, además voy a ser excesivamente rápido. En este caso porque creo que la labor del Gobierno en este sentido es una labor acertada, que tiene que garantizar, precisamente, la limpieza de nuestro sistema electoral. Usted ha dicho que se están adoptando las medidas necesarias. Lo que le quiero preguntar es que cuando ha dicho mil millones de papeletas, ¿a cuántas elecciones se refería?, ¿a una o a varias? Eso simplemente como anécdota.

En Andalucía hemos tenido elecciones recientemente y en esas elecciones —lo digo porque yo soy un defensor a ultranza de la parte digital y de cómo tenemos que acometerla— la ausencia de papeletas en colegios de Sanlúcar evitó que todos los andaluces pudiéramos seguir el recuento electoral en los medios de comunicación, como normalmente se ha hecho siempre en España. Tuvimos que enterarnos de golpe prácticamente de cuál había sido el resultado automáticamente. Por tanto, quiero decir que a veces en el sistema trabajamos muy bien una parte y, sin embargo, otra se nos escapa. Esto era simplemente como anécdota.

En relación con las campañas de desinformación, aunque pueda formar parte de su departamento… **(El señor presidente hace signos negativos).** Estoy viendo al presidente negar con la cabeza. Lo digo por lo que había parecido de la intervención anterior, pero yo precisamente lo que le iba a decir es que las campañas de desinformación no creo que formen parte de su cometido. Lo que sí tiene que ser es garantizar la limpieza de un proceso electoral, que no tenga interferencias y que se garantice en libertad. Hay otros ámbitos que son los que considero que tienen que desarrollar esa otra función.

Muchas gracias.

El señor **PRESIDENTE:** Lo que le estaba diciendo con la cabeza es que la competencia de la subsecretaria del Interior no coincide con la competencia que la senadora Angustia pretende que tenga.

cve: DSCG-12-CM-131

(La señora Angustia Gómez: Yo en ningún momento le atribuí la competencia). No es nada feo atribuir competencias excesivas.

Señor Raffo.

El señor **RAFFO CAMARILLO:** Muchas gracias, presidente.

Gracias también, lógicamente, a la señora Goicoechea por su presencia y por el esfuerzo que ha tenido que realizar para prepararse la intervención, que quiero adelantar que creo que ha estado muy bien estructurada, organizada y explicada, sin necesidad de muchas presentaciones que, en algunas ocasiones, no sabe uno si facilitan o dificultan seguir una intervención. Esa felicitación me gustaría también trasladarla a los profesionales que trabajan directamente en esto.

Voy a ser muy rápido. Una primera parte tiene que ver con esta felicitación porque hay algunas preguntas que iba a hacer y que ya no tengo que hacerlas. Veo que está muy bien enfocado y bastante bien controlado todo el proceso con el que se lleva a cabo el sistema de alerta, protección y respuesta ante posibles amenazas y, en el caso de que las hubiera, cómo resolverlas. Esto es un paso adelante importantísimo que se da fruto de la profesionalidad, la experiencia, la formación y la capacitación de los profesionales de la Administración pública. En este aspecto solo tengo una duda, que imagino que será sencilla de responder: Quién está exactamente al frente del sistema de alerta y protección de los sistemas informáticos y todo el procedimiento que tiene que ver con lo telemático en todos los procesos electorales. Me gustaría saber si van a seguir prácticamente ya con este formato.

La segunda parte es que me gustaría que ampliara un poco la información relacionada con la existencia de relaciones con otros países de la Unión Europea, si hay grupos de trabajo tanto de ámbito político como técnico que tengan que ver con todos estos procedimientos de alerta, protección y reacción contra ataques cibernéticos a procesos electorales. También hablaría aquí de la desinformación y me explico. La Unión Europea es un territorio que tiene una debilidad en cuanto a cohesión territorial ya que hay un número no desdeñable de países que, a su vez, tienen territorios que pueden generar ciertos problemas y ciertas tensiones. Aquí lo importante no son solo las elecciones generales de cada país, sino también las de ámbito local, regional, autonómico o federal, como queramos llamarlo. La pregunta va dirigida a lo siguiente: ¿existe una perspectiva de que, desde la Unión Europea, se genere una red de grupos de trabajo o de colaboración para garantizar unas elecciones limpias, independientemente del ámbito territorial en el que se celebren, teniendo en cuenta la posibilidad de las injerencias y de los ataques que pueden modificar los resultados electorales?

Muchas gracias.

El señor **PRESIDENTE:** Señora Cabezas.

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

Buenos días, señoría, y muchísimas gracias por su intervención, subsecretaria.

Me ha quedado bastante claro que los procesos electorales de los que ha hablado —ha mencionado tres, puede ser que sean cuatro, vaya preparándose— van a ser claros, transparentes, va a haber seguridad y, sobre todo, va a intentar que no existan esos posibles ataques. Mi intervención va a ir dirigida a otra gran preocupación que tenemos la mayoría de los españoles, que es la ciberseguridad de cualquier vecino y, sobre todo, por lo que está ocurriendo últimamente en España; vamos a hablar de nosotros, los españoles. Como usted bien ha dicho, es verdad que las nuevas tecnologías llegaron muy pronto y rápidamente, pero aquí ha sido al revés, primero nos han puesto un móvil o una *tablet* en la mano y, después, han querido formarnos. Debería haber sido al contrario, primero formarnos y, después, poder acceder a las nuevas tecnologías. Hay grandes peligros en el ciberespacio, peligros importantes a los que nos estamos enfrentando y, por desgracia, están saliendo datos en las noticias que son bastante escalofriantes, como el ciberacoso que están sufriendo los escolares en un 75 %. Hay grandes problemas a los que nos enfrentamos. Me gustaría saber qué está haciendo la subsecretaría que usted dirige. **(El señor vicepresidente, Jiménez Tortosa, ocupa la Presidencia).** Todo lo que está aconteciendo en el ciberespacio es muy importante, ya que es un mundo todavía bastante desconocido y, además, es usado cada vez con más continuidad por los menores. Creemos que todavía no hay la formación suficiente para utilizar muchas de las tecnologías que están a disposición de cualquiera, de ahí que se estén cometiendo muchos delitos y creo que todavía no se está trabajando lo suficiente como para evitarlos.

Yo pertenezco al medio rural, soy de la provincia de Córdoba, concretamente del pueblo Fuente Obejuna, donde la dispersión es muy importante, por lo que me gustaría saber si hay algún plan o proyecto

cve: DSCG-12-CM-131

en su ministerio para trabajar en esa brecha que tenemos tan importante, porque no llega la formación ni la información a muchos vecinos —padres, madres, personas mayores— para que puedan saber exactamente a qué se enfrentan con una mala práctica del ciberespacio. Me gustaría saber si desde su ministerio se está haciendo algo. También mi grupo parlamentario quisiera conocer qué acciones se están realizando desde el Ministerio del Interior para adquirir talento especializado tanto en actividades operativas de lucha contra el cibercrimen como para su propia protección. Esto es muy importante para nosotros. Asimismo, también son muy importantes los últimos datos sobre los *hackers* que se están dando desde el Ministerio de Hacienda y el de Justicia para denunciar la falta de seguridad que existe. También nos gustaría que nos contestara sobre esa intranquilidad que han generado las últimas noticias.

En alguna ocasión ya he dicho que ha habido proyectos en otros países con voluntarios para ciberseguridad. Me gustaría saber si su ministerio se ha planteado esa posibilidad en beneficio de todos nosotros. Algunos de los proyectos que se han llevado a cabo en otros países han dado muy buen resultado. A mi grupo parlamentario también le gustaría conocer, además del actor principal en la lucha contra el cibercrimen que es el Ministerio del Interior, posibles objetivos del mismo. ¿Considera que su ministerio dispone de los recursos necesarios tanto económicos como de talento para autoprotegerse? También sería importante que me evaluara la permanente competencia entre diversas unidades organizativas de su ministerio para adquirir el escaso talento disponible en esta materia. Asimismo, nos gustaría que nos dijera, desde que usted está en el ministerio, cuáles son los avances que se han hecho o los protocolos de actuación para bajar ese índice tan alto de cibercrimen. Todos sabemos que hoy los delincuentes han cambiado de sitio, ahora mismo no hace falta atracar un banco con pistola, se atraca con un móvil desde cualquier parte del mundo. Es verdad que son muchos peligros…

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Señora Cabezas, por favor, vaya concluyendo.

La señora **CABEZAS REGAÑO:** Voy terminando, presidente.

Es verdad que son muchos los peligros que hay ahora en el ciberespacio, pero nos gustaría que, en nombre de su ministerio —ante lo que todos conocemos y ante la intervención que en muy pocos minutos le he hecho—, nos transmitiera un poco de tranquilidad al medio rural en el sentido de que están trabajando para que esa información o posible formación llegue a cada rincón de España.

Muchas gracias.

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

Le damos nuevamente la palabra a la compareciente para que conteste aquello que considere oportuno y con brevedad, si es posible.

La **SEÑORA SUBSECRETARIA DEL MINISTERIO DEL INTERIOR** (Goicoechea Aranguren): Muchísimas gracias, presidente.

En aras de la brevedad —y espero no defraudarles, señorías, lo lamentaría mucho—, es cierto que algunas de las cuestiones que se han planteado me exceden, no son propiamente de mi ámbito de competencia, si bien son de sumo interés y algunas de ellas de enorme interés para nuestro ministerio, que está actuando activamente pero me temo que quizá no sea estrictamente el foro ni yo la persona más autorizada para entrar en ello porque soy la subsecretaría del ministerio y mis competencias en este momento, y por lo que me han traído aquí, a esta Comisión, son las relativas a los procesos electorales, a la garantía y seguridad de esos procesos electorales en concreto. Por ello digo que lamento no estar en condiciones de contestar a todo aquello que se me está preguntando, pero espero poder avanzar algunas cosas sobre lo que sí se ha dicho.

Para comenzar, agradezco muchísimo esas felicitaciones hacia el equipo, como yo también he mencionado anteriormente. Soy funcionaría y llevo treinta años en la Administración, por tanto, la Administración es mi empresa y soy consciente de que uno de los grandísimos valores que aporta la Administración a la sociedad española es la calidad de sus técnicos y de sus profesionales. Es lo que yo me he encontrado cuando he llegado a la subsecretaría del Ministerio del Interior, un magnífico equipo de profesionales, que es lo que también hay en el resto de esas unidades que he venido citando. No quiero aburrir ni con siglas ni con órganos, pero creo que sí es importante esa cita porque esa cita nos da la idea de lo que es ese conjunto de profesionales, ese conjunto de responsables que abordan en este concreto momento estas tareas de procesos electorales para dotarlos de garantía, para dotarlos de seguridad porque lo que tenemos claro los funcionarios públicos es que tenemos que servir a estas ciudadanas, a

cve: DSCG-12-CM-131

estos ciudadanos, que son los que nos ponen donde estamos y que son los que nos pagan y que, por tanto, son los que tienen todo el derecho a recibir el mejor servicio posible. De modo que agradezco las felicitaciones y por supuesto las haré extensivas a quienes se las merecen, que son esos profesionales que forman equipo con nosotros.

He hablado antes de ataques y no sé si he mencionado esta palabra, pero yo he estado seis años en la Secretaría General de Administración Digital y quiero decir que la palabra ataque dentro del ámbito de la seguridad digital es una palabra que se utiliza muy a menudo. Hay algo que no nos podemos negar y es que todos los servicios resultan vulnerables y que siempre, sea por aficionados, por chavales, por *hackers,* por mayores intereses, por empresas o incluso por Estados, puede haber un interés de llegar a determinados tipos de estructuras por muchos motivos. A mí una de las cosas que me sorprendió, incluso en esos momentos en la secretaría general, es que muchas veces se hace por prurito personal, por competencia entre distintos colegas, etcétera. Quiero decir que los ataques se producen, los ataques están ahí, pero la envergadura de esos ataques y la capacidad de llegar más o menos dentro de nuestros propios sistemas, la capacidad de llegar a tocar estructuras sensibles, es obviamente lo que varía. Para defendernos de todo esto, este país cuenta con una red sumamente segura de detección de esos ataques, con capacidad, además, de hacer diseños preventivos que nos hagan francamente fuertes hacia esa posibilidad y que nos dé una capacidad de actuación en el caso de que se produzcan.

Lo que tenemos son vulnerabilidades y las tenemos porque es inevitable. Cualquier sistema, por sumamente robusto que sea, las tiene, y me imagino que quienes han pasado por aquí lo han dicho. Lo que quiero decir es que cuanto más se sabe más conscientes somos de lo que no sabemos; cuanto más fuerte somos, también más conscientes tenemos que ser de cuáles son nuestras debilidades y, en este caso, por la responsabilidad que a mí me toca como subsecretaria de Interior, lo que me enorgullece y me tranquiliza es saber que tenemos a nuestro lado a precisamente esas organizaciones dotadas de esos profesionales con absoluta capacitación técnica para dar la mejor respuesta posible en el menor tiempo posible.

Es cierto que se detectaron vulnerabilidades en los procesos anteriores. Algunas de las vulnerabilidades hacían referencia precisamente a la empresa que había asumido el reto de llevar a cabo el proceso de difusión de escrutinio y, como decía antes, eso entra dentro de esta lógica; entra dentro de la lógica inapelable de lo que es la evolución de los sistemas informáticos. Los informáticos hacen siempre procesos de auditoría después de cualquier proceso, que es una auditoría que todos tenemos que hacer desde la humildad de lo que es una crítica positiva; lo que intentas es analizar cuáles han sido los posibles fallos que se han producido y, una vez detectados, intentar corregirlos. ¿Qué es lo que detectamos y por eso lo he destacado? Lo que se detectó es que, efectivamente, dentro de los sistemas de la empresa había determinadas vulnerabilidades, lo que dio lugar a que en el acuerdo marco convocado para después poder contratar a las empresas que en su momento resultaran adjudicatarias, en el propio acuerdo, en el propio pliego de esa contratación se incluyeran muchas prescripciones de carácter técnico-informático que previamente no se habían tenido en consideración porque en un proceso electoral, quizá de no hace tantos años, parecía que la seguridad era otra cosa. Cuando se hablaba de seguridad, se estaba hablando que otro tipo de seguridad; cuando se hablaba de cuál era la infraestructura que había que poner en marcha para el proceso electoral, todos estamos pensando, por ejemplo, en esas mesas —no sé si son 36000, y miro a la directora de Política Interior porque seguro que con el número quizá no acierte del todo— en ese procedimiento que tienes que poner en marcha, en esas urnas, que son muchas. En definitiva, hay que hacer mucho trabajo previo, mucho trabajo ese día y mucho trabajo a continuación porque todavía seguimos teniendo un escrutinio en papel. Entonces, se hablaba de esa seguridad; ahora, cuando hablamos de infraestructuras, cuando hablamos de seguridad, estamos hablando de otra cosa, por eso vamos adaptándonos a lo que vaya surgiendo.

¿Quiénes están detrás de todo este proceso? Están los órganos de antes he citado y, obviamente, está el Ministerio del Interior como responsable último de los procesos electorales y está, asimismo, el CNPIC de la Secretaría de Estado de Seguridad y también —y ha intervenido anteriormente el responsable del CNI— están con la máxima confidencialidad y discreción todas esas infraestructuras con las que cuenta nuestro Estado para garantizar nuestra seguridad, que, obviamente —y quiero resaltarlo porque se ha preguntado por ello— están en absoluta colaboración con todos los sistemas internacionales, en el mundo europeo y no europeo, velando por la seguridad.

A veces, quizá no a veces, siempre, conseguir que las cosas parezcan fáciles una vez que se han conseguido exige un esfuerzo y un trabajo enorme; desde ustedes, señorías, que tienen que dotarnos de

cve: DSCG-12-CM-131

esa legislación que nos tiene que dar esa cobertura, a la Administración, lo que se hace de manera más pública y transparente, y a otras redes, que tienen una dosis lógica de confidencialidad, todo ello exige un esfuerzo nacional y un esfuerzo internacional. Por suerte, España se suma a todo un colectivo de países, a todo un mundo en el que la informática nos ha hecho pequeños; aquella aldea global de la que se hablaba hace unos años en otro contexto hay que traerla también al mundo de la ciberseguridad. En realidad, somos todos uno y entre todos conseguimos esa protección.

Yo antes mencionaba que este sistema de alerta, del que anteriormente he trazado sus grandes líneas y que acabamos de comunicar a Reper, no deja de ser un sistema que se va a enlazar dentro del sistema europeo; formamos parte del sistema europeo, trabajamos con Europa con la que tenemos grupos de trabajo y no solamente para estas infraestructuras, no solamente para dotarnos de seguridad, sino también para reflexionar sobre qué modelo de escrutinio es el idóneo, hacia dónde nos pueden llevar estas tecnologías, qué necesidades y, algo que creo que se ha mencionado en esta sala anteriormente, qué medidas hay que ir incorporando en lo sucesivo en nuestras leyes. Quizá a nuestra ley orgánica no le vendría mal darle un barniz y dejar algo dicho en ella sobre materia de seguridad informática porque en el momento en el que se hizo la ley la realidad en la que estábamos era otra y hay un proceso constante de adaptación de la normativa, lógicamente, a la realidad.

En cuanto a los procesos telemáticos, cuando llegué aquí, mi jefa anterior me dijo: tienes que conseguir que las elecciones sean informáticas y que se lleve a cabo todo el proceso y, de esta manera, apoyarnos en medios telemáticos. Es un objetivo y, como tal, hay que reflexionar sobre ello y hay que trabajar porque, obviamente, hay que utilizar todas las herramientas disponibles. Ahora mismo todavía no es una realidad y no lo es tampoco en otros países de nuestro contexto. Si hablamos, por ejemplo, de Europa, Alemania, por ejemplo, lo declaró inconstitucional; Dinamarca, lo intentó y lo retiró, y nosotros tenemos un sistema en este momento en el que la informática juega un papel fundamental pero, ¿por qué no decirlo?, juega un papel fundamental en el escrutinio provisional. Nosotros somos un país absolutamente señero —cuánto nos cuesta en ocasiones reconocer nuestras propias capacidades y lo que de verdad entre todos aportamos a lo largo de los años— en esa información y se da, además, una magnífica información porque nosotros tenemos un sistema de escrutinio definitivo que se basa en el papel, que es el que al final nos da la seguridad absoluta. Lo que se ha venido contrastando es que entre ese escrutinio provisional y el escrutinio definitivo hay pocas diferencias. Eso habla muy mucho de nuestra capacidad y de la capacidad de esos profesionales de los que antes hablábamos. Aun así, en esas infraestructuras que tenemos que poner en juego se han mencionado antes algunos errores. Me temo que sí, que algunos se cometerán. Quizás cuando vivamos esa noche electoral que me temo que será larga porque tenemos tres procesos, con lo cual tendremos un escrutinio que lleva su tiempo a las mesas realizarlo, transmitirlo y volcarlo en información, es posible que nos pase algo, como señalaba su señoría con el caso de esas papeletas que faltaron en Sanlúcar. Además, en este caso, tenemos procesos que son responsabilidad del Estado y otros que son responsabilidad de las comunidades autónomas. Tenemos mucho en juego ese día 26, y yo me temo que estaré ahí tirando de mi gente porque nos tocará dar esa información. Pero estamos poniendo todo de nuestra parte para que esos pequeños errores y deficiencias no se produzcan. De todas formas, teniendo en cuenta que son más de seis mil municipios y que vamos a poner en juego elecciones municipales, al Parlamento Europeo y a las comunidades autónomas, que tengamos algún fallo creo que es comprensible. Espero que sus señorías y espero que también nuestros ciudadanos puedan entender que en un momento dado puedan faltar papeletas en un determinado colegio electoral, pero procuraremos que no ocurra, y ahí están nuestras delegaciones y subdelegaciones de Gobierno luchando por que eso sea así. Y cuando antes hablaba de mil millones de papeletas estaba hablando solamente del proceso de las elecciones al Parlamento Europeo, solamente de eso. O sea que imagínense las infraestructuras y todas las capacidades que hay que poner en juego en este sistema.

No sé si me estoy dejando algo sin contestar. Como decía la señora Cabezas, lo que se está planteando es un tema apasionante. Además, por mi anterior trayectoria administrativa, me resulta de un interés extremo, pero, como decía antes, es un tema en el que tenemos una Secretaría de Estado de Seguridad y en el que tenemos otros órganos de la Administración, como el Incibe, que juega ahí un papel fundamental. Creo que todos somos conscientes de que este es un proceso que nos va empujando. En materia de informática se habla de las generaciones que sí han nacido con la informática y las que no, de los que son nativos o de los que no son nativos. Yo no sé dónde estoy, creo que por mi edad no me toca nativa. No, no soy nativa, pero me gusta muchísimo el tema informático, y en él vas adquiriendo las capacidades a veces como buenamente puedes, con un ejercicio, lógicamente, de intentar aprender

cve: DSCG-12-CM-131

desde la humildad algo que nos está llegando con una velocidad enorme. Las instituciones públicas tenemos una obligación y un reto enorme, que es el de ayudar a nuestra ciudadanía, y también lo tiene la sociedad civil. Este es un proceso en el que tenemos que estar entre todos, y entre todos intentar conseguir que las herramientas tecnológicas que nos dan unas ventanas de oportunidad magníficas lo sean dentro de la más absoluta seguridad y que sean realmente constructivas para, entre todos, alcanzar esa sociedad mejor, que es lo que todos queremos.

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Muchas gracias, doña Isabel Goicoechea Aranguren por su apasionada comparecencia. Con su brillante capacidad de comunicación, creo que nos ha convencido de que estamos en muy buenas manos. Si cada veinte años se produce esta coincidencia de elecciones, dentro de poco tendremos la prueba para comprobar que estamos en muy buenas manos y las elecciones se van a celebrar perfectamente. Y esperamos que ese superdomingo no aumente.

Muchas gracias.

Se levanta la sesión.

Eran las dos y quince minutos de la tarde.

CORRECCIÓN DE ERROR:

En el *Diario de Sesiones* número 126, correspondiente a la Comisión Mixta de Seguridad Nacional, sesión número 25, extraordinaria, celebrada el miércoles 23 de enero en el Palacio del Congreso de los Diputados, en la página 48, cuando dice: «El señor Hernando Fraile», debe decir: «El señor Hernando Vera».

cve: DSCG-12-CM-131