DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2017 | XII LEGISLATURA | Núm. 67 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 10

celebrada el jueves 23 de noviembre de 2017 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

Comparecencias. Por acuerdo de la Comisión Mixta de Seguridad Nacional:

---

cve: DSCG-12-CM-67

Se abre la sesión a las once y cincuenta y cinco minutos de la mañana.

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

— DE LA SEÑORA MILOSEVICH-JUARISTI, INVESTIGADORA PRINCIPAL DEL REAL INSTITUTO ELCANO Y PROFESORA ASOCIADA DE HISTORIA DE RELACIONES INTERNACIONALES DEL INSTITUTO DE EMPRESA (IE UNIVERSITY), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 219/000906 y número de expediente del Senado 715/000293).

El señor **PRESIDENTE:** Señorías, buenos días.

En primer lugar, quiero agradecer a todos los grupos, y especialmente a sus portavoces, la flexibilidad en el manejo horario de esta Comisión. Hoy empezamos con media hora de retraso, pero el celebrarla por la mañana permite a los senadores y diputados que vivan fuera de Madrid tener una agenda más flexible.

Mi agradecimiento también a Mira Milosevich-Juaristi, que es nuestra primera compareciente, que ha aguantado con estoicismo franciscano esta media hora de retraso. Y, sin más, le voy a dar la palabra y después abriremos el turno de los grupos.

Tengan ustedes en cuenta que tenemos una segunda comparecencia, la del general don Carlos Gómez López de Medina. Si queremos tener un horario razonable de comida calculen que deberíamos terminar hacia las dos y media, si es posible; si no, continuaríamos.

Señora Mira Milosevich-Juaristi, gracias por comparecer en esta Comisión, que es una Comisión de nuevo cuño que va organizando su agenda día a día, un poco como la película *Casablanca*, que el guión del día siguiente se escribía la noche anterior. En fin, *Casablanca* terminó relativamente bien y espero que esta Comisión también. **(Risas).** Tiene usted la palabra.

La señora **MILOSEVICH-JUARISTI (**Investigadora principal del Real Instituto Elcano y profesora asociada de Historia de Relaciones Internacionales del Instituto de Empresa, IE University): Buenos días a todos.

En primer lugar, muchísimas gracias por invitarme. Para mí es un honor comparecer ante la Comisión de Seguridad Nacional y compartir con todos ustedes, con sus señorías —una palabra que oigo frecuentemente en la televisión, pero nunca he estado aquí—, los conocimientos que tengo de Rusia y de la guerra de información de Rusia. Y como se ha mencionado la película *Casablanca*, yo espero que esto sea el comienzo de una larga amistad, como acaba la película. **(Risas).**

Dicho esto, tengo entendido que ante esta Comisión van a comparecer otros expertos. Y también tengo entendido que dos análisis publicados por el Real Instituto Elcano han sido repartidos a los miembros de esta Comisión. Uno de ellos es de comienzos de año y es sobre desinformación y el otro, que es sobre el concepto de combinación, está escrito después de la celebración del referéndum ilegal de Cataluña. En primer lugar, simplemente vamos a aclarar dos conceptos, hay que diferenciar entre lo que es un ciberataque y la guerra de información o desinformación, que puede ser una u otra cosa. La guerra de información se practica en las redes sociales y en otros servicios de Internet. Los responsables del Centro Criptológico Nacional ya afirmaron en su declaración que no hubo un ciberataque desde Rusia, precisando que hubo setenta pero que su procedencia es de los delincuentes cibernéticos como Anonymous u otro y que, en cualquier caso, que no se trataba de Rusia. Los mismos responsables subrayaron que retuitear desde perfiles falsos o desinformar no es un ciberataque, aunque puede formar parte de la llamada guerra híbrida. Hemos oído mucho este término y no voy a entrar ahora —aunque luego si alguien me pregunta puedo dar mucho más detalles— en ella, solo haré algunas precisiones. El término de guerra híbrida se ha usado muchísimo, es un concepto que empezó a usarse primero en el vocabulario de la OTAN para describir la lucha contra las fuerzas insurgentes, luego se describió como una guerra de combinación entre las fuerzas convencionales y las irregulares y desde 2014, desde la anexión de Crimea por Rusia, se habla de la guerra híbrida como una de las estrategias de Rusia. Documentos rusos traducen literalmente la palabra híbrida por гибридная война (*gibridnaya voyna)*. Sin embargo, ellos usan otros términos como guerra no lineal, guerra ambigua, guerra especial o la guerra de las redes. Si comparamos lo que los rusos comprenden por guerra no lineal —término que más usan— realmente coincide con dos conceptos que ya están en la estrategia de la Unión Soviética y cuya raíz está en la Rusia prerrevolucionaria. Un concepto se refiere a las medidas activas y el otro es la guerra de

cve: DSCG-12-CM-67

información. Los rusos usan estos dos conceptos, medidas activas y guerra de información, casi como sinónimos y habitualmente los usan conjuntamente, es decir, van juntos y muchas veces se confunden.

Ahora pasaré a hablar de los hechos, de por qué estamos aquí, de por qué hablamos de una posible injerencia de Rusia en Cataluña. Una de las razones —y en esto no voy a entrar ahora en detalle porque creo que la mayoría de ustedes han visto muchas de estas imágenes y de este material en los medios de comunicación y en otros análisis, de hecho los he puesto aquí por si los necesito en las respuestas— son estos tuits creados por Julian Assange. Es la afirmación que se ha hecho desde *El País* y desde la Universidad de George Washington sobre el aumento en las redes sociales de las palabras Cataluña y referéndum catalán, que aumentaron un 2000 % en los últimos días de septiembre. También hay imágenes de la información que ofrecieron RT, la antigua Russia Today, y Sputnik. Ustedes se van a quedar con este *powerpoint,* por lo que podrán verlo detalladamente. En esta presentación no he puesto el análisis que he usado en mi publicación de Elcano sobre la información que se ofreció en las televisiones estatales de Rusia porque está en ruso y creo que no tenemos tiempo para traducirla. En cualquier caso, aquí están las informaciones más llamativas de los mensajes que ha creado Julian Assange, que se han repetido con una velocidad que algunos afirman que en un segundo son sesenta veces, que solo se puede hacer por un *bot*, por un robot, que es imposible que seres humanos en un segundo retuiteen sesenta veces un tuit aunque sea de Julian Assange.

En cualquier caso, hay que decir también —en esto hay que ser justos— que muchas de las imágenes que Sputnik y Russia Today han usado son imágenes que los mismos independentistas ofrecieron a varios medios de comunicación. Otra cosa son los comentarios de diferentes medios de comunicación. Como precisión diré que medios tan respetables como *New York Times*, *The Guardian* o *BBC* —y muchos otros— han publicado varias informaciones erróneas intencionadamente o no, esto hay que subrayarlo: Rusia no es el único país cuyos medios de información han publicado este tipo de información. Donde hay una distinción es que RT y Sputnik reciben alrededor de 311 millones de dólares al año directamente del Gobierno. Son medios de comunicación que funcionan fuera de Rusia o que forman parte —digamos— de la financiación gubernamental de Rusia.

Resumiendo todo esto, resumiendo los mensajes de Twitter retuiteados, analizando los reportajes de RT y los artículos de Sputnik y analizando la información de las televisiones rusas estatales, aquí están los mensajes más importantes. Si hablamos de la desinformación, hay que decir que la desinformación no es solo —*Vamos a contar mentiras tralará*— lanzar mensajes verdaderos, noticias verdaderas o falsas; la desinformación es crear mensajes, tener un propósito de lanzar un mensaje alrededor y apoyándolo obviamente en una noticia. De los mensajes más destacables uno es obviamente el uso de la fuerza por parte de la policía, que siempre se ha presentado como una violencia deliberada y no como una legítima defensa de la seguridad del Estado, y normalmente esta noticia siempre se ha vinculado como una práctica de la época franquista y no de la España democrática.

Otro de los mensajes era que la Unión Europea reconocería la independencia de Cataluña, que la Unión Europea había presionado a España para llevar explícitamente a cabo una acción represiva que impidiera el referéndum porque después del *brexit* no venía bien ninguna independencia más. Se describió esto como la revolución de color; los rusos llaman revolución de color al derrocamiento de los regímenes cleptocráticos en los Estados del espacio postsoviético, en las exrepúblicas soviéticas, donde acusan directamente en primer lugar a los Estados Unidos pero también a la Unión Europea de fomentar el derrocamiento de los Gobiernos de estos Estados y lo definen como revolución de color. Describen lo que ocurre en Cataluña —estos medios— como una revolución de color dentro de la Unión Europea. Hubo muchísima comparación entre Kosovo y Cataluña, entre Crimea y Cataluña, entre la Guerra Civil de la región de Donbáss y la supuesta o posible guerra civil entre España y Cataluña, aquí se ve en *RT* clarísimamente esta intención. Y el mismo presidente Vladimir Putin en el Club de Valdai salió y dijo que él había advertido a Occidente hace tiempo de que el reconocimiento de Kosovo como Estado independiente iba a abrir una caja Pandora y que iba a fomentar independentismo y separatismo en otra parte. Creo que la posición oficial de España coincide con esta valoración y puedo decir que con la mía propia. La cuestión de Kosovo es sin duda alguna un precedente histórico que puede tener consecuencias muy diferentes.

Uso una palabra que en ruso es *сочетание (kombinaciya)*, que significa «combinación», y la pongo entre comillas porque realmente se ha usado mucho en todos los análisis el concepto de desinformación o de *fake news*, pero yo creo que ha habido muy pocos análisis, o por lo menos yo no los conozco, que hayan intentado detectar cómo funciona la desinformación. Aquí pongo un gráfico que se refiere a que hay

cve: DSCG-12-CM-67

una combinación entre varios instrumentos y una coordinación entre ellos. La combinación es la palabra que siempre se utiliza tanto en la doctrina militar como en varios artículos sobre la guerra de información. *Сочетание (kombinaciya),* nunca solo una cosa puede conseguir una desinformación o lanzar un mensaje.

Sabemos que incluso en la Wikipedia hay una entrada sobre brigadas, hay muchas investigaciones sobre la existencia de los *trolls*, de los *bots* y de los *sockpuppets*. Esto es una información y luego volveré a este tema porque no necesariamente haya sido un uso exclusivo por parte de Rusia, existe una cosa que se llama web brigada y se compone de diferentes elementos.

En Rusia existen fábricas y granjas de trolls, la más conocida está en San Petesburgo, y hay un libro publicado sobre qué tipo de gente trabaja allí, cómo se trabaja y cuál es su trabajo. Tenemos los medios de comunicación financiados por el Gobierno de Rusia que son RT y Sputnik, están las redes sociales y Facebook. Luego tenemos dos personajes como Edward Snowden, exiliado en Rusia, y Julian Assange, que está en Londres, como sabéis. Si Julian Assange ha sido pagado por tuitear, esto más podría ser por parte de Cataluña que por parte de Rusia, aunque no tengo pruebas, pero sí que ha salido en la prensa que uno de los ideólogos del separatismo catalán ha estado reunido unas tres o cuatro horas en la embajada de Ecuador en Londres y esto es lo que ha comentado nuestro ministro de Defensa.

Existe la ciberinteligencia y aquí, ¡ojo!, no hablo de ciberataques. La ciberinteligencia es una parte de cualquier servicio de inteligencia que incluso con métodos analíticos puede conseguir información valiosa y significativa para una operación de fuentes abiertas. Hoy en día nuestras vidas están en Internet incluso por nuestra propia voluntad y por una inercia. Luego está la desinformación, que es un concepto que en realidad tiene una larga trayectoria. En la época soviética la desinformación sobre todo servía para persuadir y convencer lo superior que era el socialismo y el comunismo en relación con el capitalismo. Hoy en día la desinformación no tiene este papel y su papel es más confundir y desacreditar a una persona, a una organización o a un grupo de gente y, sobre todo, demostrar que son falsos, hipócritas o que habitualmente son los enemigos de Rusia.

Comprendo que estoy aquí para hablar de quién podría haber hecho esto y por qué lo habría hecho. Esta es la pregunta clave: ¿Quién lo ha hecho y por qué lo ha hecho? Mi hipótesis en el análisis, y que intentaré explicar por qué, es, teniendo en cuenta que la procedencia territorial confirmada por la ministra de Defensa y ministro de Exteriores, también confirmada a mí personalmente por varias personas que trabajan para las consultoras privadas —y tengo entendido que algún diputado había pedido la comparecencia de los actores del campo privado, no solo de las instituciones españolas— que hay indicios de que la procedencia territorial es de Rusia y de Venezuela en el caso de la repetición robótica de los mensajes tuiteados por Julian Assange y por muchos otros rusos, que son perfiles falsos, que son fantasmas. Es un fenómeno que ha existido y del que se ha hablado mucho, pero teniendo en cuenta la procedencia territorial y la complejidad de la combinación y la coordinación de los medios e instrumentos tecnológicos de la guerra de información, yo considero que esto no pudo venir de un individuo patriota, y aquí uso la palabra patriota porque hay una grabación del presidente Putin que ha salido en la Televisión Española en la que dice: Cuando algún *hacker* ve que alguien critica a Rusia y habla mal de Rusia hace su trabajo, pero nosotros nos tenemos nada que ver, y los llamó *hackers* patriotas. María Zajárova, la portavoz del Ministerio de Asuntos Exteriores de Rusia, llamó abiertamente en su Facebook a dos personas que hicieron la broma a nuestra ministra de Defensa combatientes informáticos; dijo que el libro que habían publicado no era un libro de bromas, era un manual de combatientes informáticos. Quiero decir que desde mi punto de vista hay una coordinación y que, en cualquier caso, la complejidad de esta operación requiere de una estrategia planificada y un apoyo de agencias cercanas al Gobierno ruso.

¿Cuáles son mis argumentos? Esto es una hipótesis, es la deducción de un análisis que hago. Mis argumentos son los siguientes —y luego puedo entrar en detalle, estaré encantada de responder a sus preguntas—. En primer lugar, he mencionado que hay varios medios de comunicación y otra gente que ha transmitido información errónea, intencionadamente o no, sobre el referéndum ilegal de Cataluña, pero de todos estos actores ninguno de ellos ni ningún país tiene el concepto de la guerra de información como parte de la doctrina militar, que es un documento público que está en inglés y en ruso, no en español. La doctrina militar de Rusia de 2014 incluye por primera vez el concepto de la guerra de información en un documento oficial. Hay otro concepto, el de la disuasión estratégica. Los occidentales identifican el concepto de disuasión estratégica con la guerra híbrida, pero en el caso de los rusos es una combinación de métodos militares —explícitamente se define así— y no militares en disuadir al enemigo de Rusia. Cuando hablo de métodos militares están incluidos los nucleares, y cuando hablo de métodos no militares

cve: DSCG-12-CM-67

me refiero —según dice la explicación— a métodos políticos, económicos, de información, culturales, etcétera. Hay varios artículos sobre la guerra no lineal del general Valeri Guerasimov, que es el jefe del Estado Mayor. Guerasimov afirma que lo que era guerra convencional en el campo de batalla en tierra, mar y aire simplemente ahora tiene una nueva dimensión, que es la dimensión de información, y que se combina con esta convencional batalla. Otros argumentos son la historia, evolución y perfeccionamiento del concepto de la guerra de información desde el año 2000 pero sobre todo desde 2011, desde las manifestaciones antigubernamentales contra el Kremlin después del supuesto fraude electoral y la culminación de esta estrategia se ha demostrado en la anexión de Crimea y posteriormente la combinación de métodos militares y de información en la guerra de Siria y en la guerra del sureste de Ucrania, en la región de Donbáss.

También he tenido en cuenta los hechos previos de la guerra de información en las campañas de las elecciones presidenciales en los Estados Unidos, en la campaña del *brexit*, en las elecciones en Francia y Alemania, que siguen su curso de investigación. Mi artículo es una hipótesis, es una deducción y una conclusión basadas en los hechos del comportamiento anterior y de los documentos oficiales que incluyen la guerra de información en la doctrina militar, documentos oficiales sobre este concepto.

Creo que varios expertos en ciber —puro ciber, no en desinformacion sino en lo que se refiere a los ciberataques— han subrayado que no existen pruebas materiales ni huellas informáticas de que fueran ordenadas por el presidente Vladimir Putin o por miembros concretos de su gabinete. Hay muchas declaraciones recientes —también del ministro Serguéi Shoigu— sobre la guerra de la información y su importancia. La naturaleza misma de la guerra de información no deja o borra este tipo de huellas y hay constancia de que existe Internet Research Agency —IRA— en San Petersburgo, que es una de las fábricas de *trolls* más importantes, cuyo propietario es Yevgeny Prigozhin, que es uno de los mejores amigos del presidente Putin. Lo que se ha demostrado hasta ahora es que la comisión de ese tipo de operaciones normalmente se externaliza, es decir, el sistema informático y el ciberespacio posibilitan la externalización de este tipo de operaciones porque buscan varios terminales y varios actores.

En cualquier caso, yo sigo sosteniendo que la complejidad de lo ocurrido refleja una coordinación y, desde mi punto de vista, creo que hay una estrategia detrás de ello. ¿Por qué? ¿Cuáles son los objetivos de Rusia en eso? En esto estoy de acuerdo con las declaraciones oficiales de varios representantes de Rusia que creen que Rusia apoya la integridad territorial de España; el objetivo de Rusia no es la independencia de Cataluña pero sí que creo que España, como miembro de la Unión Europea y de la Alianza Atlántica, es un instrumento, es una oportunidad para debilitar a la Unión Europea y para desacreditar tanto la democracia española, como las instituciones europeas y el orden democrático que tienen todos los miembros de la Unión Europea y de la OTAN. Otro de los objetivos —y este siempre está presente— es distraer la atención de los ciudadanos rusos de los problemas internos y, si se fijan en los mensajes de RT y de Sputnik, Rusia describe lo terrible que es el sistema democrático en España y pide libertades en España, las mismas que nunca ha permitido en Rusia misma. Para no ir más allá basta observar el caso de Chechenia para ver cómo se ahoga un movimiento independentista, un movimiento de soberanía que pretendía crear un nuevo Estado. ¿Cuáles son los motivos? ¿Cuál es el *drive*, el motor que impulsa a Rusia para hacer eso? En todos estos documentos oficiales, en algunos más que otros explícitamente —sobre todo en los artículos personales de Gerasimov y en documentos oficiales— se habla de influir no de destruir. Hay un oficial ruso que dijo que en la Primera y en la Segunda Guerra Mundial era mucho más costoso matar a un hombre que influir en él. Hoy en día no hace falta matar a la gente si se puede influir en ella. Es una de las declaraciones que se hace. La influencia —no la destrucción— es el motivo principal y, bueno, todo el mundo quiere ejercer la influencia, no es solo algo ruso. Los motivos son más bien domésticos.

El modelo de la democracia liberal se presenta como un modelo fracasado y sin credibilidad para dar lecciones morales a Moscú. Detrás de ello existe la convicción de Rusia —lo he explicado resumidamente, pero bien en mi análisis— de que esto ha empezado en Estados Unidos y su objetivo es dar a probar de la propia medicina a los países occidentales. Se trata de la comprensión que desde el punto de vista de Rusia ellos tienen que devolver. La doctrina militar, que incluye el concepto de la guerra de información, clarísimamente refleja lo siguiente. Primero, que los rusos creen que se trata de medidas defensivas —defensivas— y no ofensivas. Y segundo, teniendo en cuenta que se introduce en un documento de doctrina militar, desde mi punto de vista refleja que Rusia considera que está en una plena guerra de información. Quiero decir que lo convierte y lo militariza; lo convierte en un concepto de la doctrina militar.

cve: DSCG-12-CM-67

¿Qué podemos hacer? Es imposible que los países occidentales, los países de la Unión Europea, de la OTAN, respondan con total éxito a la desinformación de los instrumentos y tácticas empleados por Moscú, por Venezuela o por quien sea. Los Gobiernos occidentales no pueden restringir de manera efectiva los flujos de información y además no lo pretenden. Una de las características de la democracia occidental es la libre expresión; otra cosa es encontrar un equilibrio, que en ello estamos. Nuestro propósito no es prohibir Facebook —que ahora mismo está prohibido en Rusia y en China—, pero hay países que limitan muchísimo el uso de las redes sociales porque las consideran peligrosas para su seguridad nacional.

La guerra de información no es una guerra convencional, la guerra de información no es una guerra de conflicto físico, sino una guerra de influencias, en el sentido de crear un ambiente favorable para futuras acciones rusas, de apoyar a fuerzas hostiles que existen en los países occidentales o a actores exteriores o simplemente para crear simpatías entre la población. En este sentido —con esto concluyo—, la batalla que tenemos que librar, y no solo con Rusia —lo he explicado en mi primer análisis, donde solo hablo de desinformación—, es que el límite de la influencia rusa es nuestra solidez, nuestra calidad democrática, nuestras convicciones liberales. Porque como dijo Stanilav Levchenko, que fue jefe de la KGB en los años setenta en la Cuenca del Pacífico: Busca tus vulnerabilidades y encontrarás la KGB. Hoy en día podríamos decir que nuestra defensa no es hacer más propaganda con Rusia, no es atacar a Rusia ni mucho menos, sino buscar nuestras vulnerabilidades y mejorar nuestras democracias y así blindarlas ante la desinformación y las falsas noticias.

Muchas gracias. Quizá me he excedido un pelín.

El señor **PRESIDENTE:** Muchas gracias, señora Milosevich.

Vamos a abrir ahora el turno de intervenciones, empezando por el Grupo Mixto. Tiene la palabra el señor Yanguas.

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

Quiero agradecer en primer lugar a la señora Milosevich su exposición y los informes que nos facilitaron en la pasada sesión, porque nos aclaran —por lo menos a mí me aclaran— conceptos que son complicados y difíciles de entender en la realidad en la que nos movemos algunos políticos. Ha dicho usted que la desinformación no es solo lanzar noticias falsas, sino crear mensajes. Yo creo que esa es una de las claves de lo que usted nos ha dicho aquí, porque es muy difícil encontrar la verdad y desmontar esas falsedades en un segundo, y llegar hasta el final y deshacer esos mensajes falsos es muy complicado. Además las personas nos apuntamos rápidamente a esos mensajes falsos y a retuitear y a compartir. Yo creo que a eso nos apuntamos todos rápidamente.

Usted ha hecho referencia hoy a alguno de los informes, y en el de la combinación nos decía —hoy también nos lo ha dicho— que los medios de comunicación rusos y alguno español informaron de que estaba el Gobierno de Rusia detrás de esta combinación, de estas noticias falsas, aunque también hoy nos ha dicho algo más que yo no leí en el informe, y es que no hay pruebas de que nadie del Gobierno ruso, ni el presidente ni ningún ministro o alto cargo ruso estuviera detrás, pero sí se ve una estrategia, además de lo que nos ha explicado usted. Me parece que esa estrategia está clara. Aunque no haya pruebas —usted lleva tiempo estudiando esto—, ¿cuál es la opinión que le merece? ¿Está el Gobierno ruso detrás o no? Aunque no haya pruebas quiero su opinión, si nos la puede dar —aunque la ponga ante un pequeño o un gran brete—, si cree que hay Gobiernos detrás de estos ataques a la credibilidad de España o del Gobierno de España, cómo se han hecho las cosas.

Esa era la pregunta clave que le quería hacer hoy de lo que he leído y lo que le he escuchado y volver a agradecerle lo que nos ha dicho. Me ha dado la sensación de que esta película continuará, que tendrá una segunda, tercera, cuarta y quinta parte. Es la sensación que me ha dado, que la solución no es fácil —no la tiene usted ni creo que la tengamos nadie— pero que este tema continuará. Esa es la sensación que me ha dado y le agradezco de nuevo su comparecencia hoy aquí.

El señor **PRESIDENTE:** Tiene ahora la palabra el señor Salvador, del Grupo Ciudadanos.

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

Doña Mira Milosevich, en primer lugar le agradezco, como han hecho anteriormente, tanto la presentación de los informes como lo que ha sido su exposición. Yo creo que estamos ante un tema que por primera vez probablemente se esté tocando en estas Cortes Generales y en esta Comisión de

cve: DSCG-12-CM-67

Seguridad Nacional. Por tanto, nos gustaría opinar al hilo de su intervención, a la vez que le hacemos algunas preguntas en relación con ello, en primer lugar porque entendemos que en este momento estamos ante conceptos… **(Rumores).** Presidente, hay mucho lío.

El señor **PRESIDENTE:** Silencio.

El señor **SALVADOR GARCÍA:** Tiene más autoridad que Ana Pastor, con una palabra basta.

En primer lugar, estamos ante momentos distintos, momentos en los que, por ejemplo, conceptos como la inteligencia económica ya se contemplan tanto en defensa como en seguridad nacional, así como lo que está usted planteando ahora mismo sobre la maquinaria de desinformación en un momento determinado con la intención de hacer una intromisión, una injerencia, y alterar unos resultados naturales en un país. Es verdad que todo esto forma parte de las propias bondades que tienen la red, nuestro mundo globalizado y la capacidad para comunicar, donde las personas se informan a través de la red, a su vez se convierten en prescriptores y comunican, y a partir de ahí lo suelen hacer normalmente por fuentes creíbles, pero también, si se inunda de contenidos, es difícil para la gente poder evaluar lo que es correcto y lo que no es tan correcto, e incluso al final, cuando una persona coge una información que da por verosímil y la divulga entre sus círculos cercanos, es como si coparticipara esa información y la blanqueara un poco haciéndola más accesible y más creíble a las personas a partir de esa comunicación.

Estamos hablando de criterios básicos de comunicación. Al final hay unos objetivos; esos objetivos se convierten en una serie de mensajes; esos mensajes se llevan a una estrategia de comunicación; esa estrategia de comunicación se convierte en contenidos; se aumenta el valor de los contenidos para que los utilicen prescriptores que ya tienen un tirón fuerte y son *influencers* en el ámbito de la red y, a partir de ahí, se utilizan todos los medios disponibles para poder divulgar masivamente todo ese tipo de información. Eso no es malo en sí, lo que es malo es cuando no se utiliza para dar una información de parte, correcta y a las claras, como un posicionamiento que alguien plantea frente a un tema. En este caso, como Gobierno de España y como país tenemos la obligación de informar al conjunto de los ciudadanos de las cosas que entendemos. Por ejemplo, en la cuestión a la que se ha hecho referencia —la crisis catalana— entendemos que hay que hacer una campaña de información para llegar al mayor número posible de gente. Pero la diferencia está en que tiene que ser información veraz, lo más objetiva posible y, sobre todo, que se pueda constatar o demostrar con datos. Todos sabemos que en Internet lo que predomina en este momento es el ruido, el lío; es muy fácil desinformar y, sobre todo si, como hemos visto, se hace masivamente y con una información que se consume muy rápido y por personas que no están todo el día pendientes de qué información les van a dar y de analizarla, sino que la van consumiendo conforme va entrando. Por tanto, es un fenómeno muy global.

Al hilo de su intervención, y lo hemos visto en su informe, yo le quería preguntar —lo ha hecho el interviniente anterior— si usted seguiría manteniendo que el Gobierno ruso ha podido dar cobertura a estos *hackers,* patriotas o como queramos llamarlos; si exactamente sucede lo mismo con el Gobierno de Venezuela, lo que en este sentido sería un poco denunciable. Hemos visto también las presiones del Gobierno ruso diciendo que esto pude enrarecer las relaciones y por eso creo que diplomáticamente, a partir de ahora, el Gobierno de España y los organismos que dependen de él, probablemente, hagan una comunicación diplomática de algo que en el fondo nos tiene que preocupar y que tiene que llegar incluso —no me refiero a este asunto en concreto sino a este tipo de actitudes— a Naciones Unidas. Porque en este momento estamos hablando de que cualquier cuestión que se pueda dirimir en cualquier país —véase el *brexit*, véanse las elecciones en Estados Unidos, véase el asunto catalán o cualesquiera elecciones, o simplemente la interpretación de un atentado— está sujeta a ver qué país es capaz de construir la maquinaria más grande de desinformación, y sonriendo y silbando, como si no tuviera nada que ver, poder cambiar los resultados y el curso de la historia.

Creo que es un asunto muy importante sobre el que no tenemos que frivolizar en absoluto como país; tenemos que elevarlo a otro tipo de organizaciones, y si se constata que hay países en los que existen grupos organizados que están actuando, se les trate como ciberdelincuentes y también se pueda actuar. Lo mínimo que se le puede exigir al país que tiene los *hackers* y que tiene a las personas que están utilizando estos *bots* es que actúe contra ellos. Que pueda decir que es verdad que están en su territorio pero que como país los está combatiendo, los está criminalizando y va a intentar impedir esto. Entendemos que no vale con ser actores pasivos y decir que esto es libertad de expresión y nosotros no tenemos nada que ver. Si se detecta dónde están esos ordenadores, dónde están esos *bots,* dónde están esas personas, la comunidad internacional tiene también que legislar e intentar que se actúe contra ellos. Porque si en

cve: DSCG-12-CM-67

ese caso no se hace, ya se podría decir que el país es cómplice y que, probablemente, está coparticipando de esta intervención.

Para terminar, quiero pedirle su valoración personal de acuerdo a sus estudios y si, desde su óptica, cree que la incidencia real de estas campañas pueden cambiar el curso de acontecimientos. Todos podemos tener nuestra opinión pero me gustaría conocer la suya, si cree que se consiguen esos objetivos, cómo se tendría que actuar frente a esto y si coincide con los planteamientos que he puesto encima de la mesa de que tendría que ser algo tratado a nivel de los Estados, del *fair play* y de las relaciones, en vez de ocultarlo y decir: esta vez lo has hecho tu, mañana lo hago yo.

Le doy las gracias por su comparecencia y estaré atento a sus respuestas.

El señor **PRESIDENTE:** Antes de la próxima sesión, les recomiendo el capítulo de un libro de César Molinas, *La crisis existencial de Europa*, que presentamos el otro día Joaquín Almunia y yo. Tiene una tesis muy parecida a la suya: comparar el ciberespacio con la mar y aplicar a los *hackers* las mismas reglas que se aplicaban a los piratas desde el punto de vista del derecho internacional.

El señor Mayoral tiene la palabra.

El señor **MAYORAL PERALES:** Muy buenos días.

La verdad es que no puedo estar tan contento como el resto de los portavoces de los otros grupos porque estamos muy sorprendidos por los informes que se han facilitado a esta Cámara. En primer lugar, nos gustaría, en una Comisión como esta, que es parlamentaria, que nos dijera si estamos en guerra con Rusia. Esa es la primera pregunta que se tiene que aclarar porque nos parece que eso tiene una trascendencia no menor. Supongo que usted sabe que existen tropas españolas desplegadas en los países bálticos en estos momentos. Como comprenderá, las afirmaciones que contienen los informes que usted facilita a esta Comisión son de extremada gravedad para la seguridad nacional de nuestro país, y más viniendo de un instituto como el suyo.

Su instituto tiene historial respecto a los conflictos armados; no es nuevo. Querría mencionar a algunas personas relevantes que forman parte del instituto al que usted pertenece, como son Felipe González, José María Aznar, María Dolores de Cospedal, Íñigo Méndez de Vigo, y gente de la sociedad civil, en concreto del sector financiero, como Francisco González, Jordi Gual Solé, Ana Patricia Botín y otras personas. Supongo que usted también sabe que su instituto fue uno de los *lobbies* más importantes que dieron respaldo a la intervención militar ilegal en Irak por España y que además sirvió para intoxicar al conjunto de la opinión pública mundial en cuanto a la posible existencia de armas de destrucción masiva y a la posibilidad de que el Gobierno de Irak las utilizase. Le pregunto: ¿Tienen la misma fiabilidad estos informes que aquellos en los cuales ustedes afirmaban no solo que existían armas de destrucción masiva en Irak, sino también que Irak las pudiese utilizar contra Occidente?

No sé si usted sabe que España se constituye en un Estado social y democrático de derecho que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político. El pluralismo político es un elemento fundamental en la articulación de la democracia. Y eso, cuando se tiene una responsabilidad a la hora de realizar un informe como el que usted realiza para traerlo a esta Cámara, hay que tenerlo en cuenta, máxime cuando —no sé si usted lo sabe— en esta Cámara hay un informe que acredita la utilización del Ministerio del Interior contra la disidencia política. No sé si conoce esos informes —pero se los recomiendo— en los que se pone de manifiesto que se han utilizado recursos del Estado para perseguir a los disidentes políticos y, entre otras cosas, para intoxicar y desinformar contra aquellos que opinaban de forma diferente al Gobierno. Se lo digo porque desgraciadamente hemos visto que en su informe usted no tiene ningún decoro en decir que el Partido Podemos puede estar recibiendo financiación del Kremlin, como otros partidos populistas, aunque será difícil obtener pruebas de ello, ya que se trataría de una financiación opaca. Yo no sé si usted entiende la gravedad que tienen sus afirmaciones, no sé si calibra que usted en estos momentos está haciendo parte de una doctrina de la seguridad nacional, nosotros entendemos que esto forma parte de una estrategia de intoxicación inaceptable en un Estado democrático cuando no se aporta ni una sola prueba; ni una sola prueba. Es una descalificación y un ataque al pluralismo político y a la democracia en nuestro país, máxime cuando nos encontramos en una Comisión de Seguridad Nacional. Ya dijimos al principio que nos preocupaba mucho que existiese una Comisión que se llamase Comisión de Seguridad Nacional porque nos recordaba demasiado a una cosa que seguro que usted conoce, que es la doctrina de la seguridad nacional, por la cual desaparecieron personas, se persiguió a disidentes políticos y se puso por encima de

cve: DSCG-12-CM-67

los intereses y de las libertades de las personas los intereses de las grandes corporaciones internacionales. Supongo que la conocerá.

No deja de sorprendernos encontrarnos con informes como este con afirmaciones tan duras como la diferencia entre la política y la guerra. La diferencia entre la política y la guerra es que en una se mata y en la otra se influye; no es que cuando se influye se haga la guerra. ¿Qué quiere que le diga? Prefiero que pueda haber libertad de información como uno de los pilares esenciales de la democracia en España y en el mundo. La libertad de información es uno de los elementos clave para que podamos disfrutar de democracia y para que podamos tener diversas informaciones. Hemos visto que usted ha traído muchísimas informaciones de algunos medios de comunicación, pero le han faltado otros. Le ha faltado un análisis del tráfico del resto de los medios de comunicación en relación con Cataluña para que nos haga una comparativa. ¿Solamente aparecieron en las portadas de los medios de comunicación de Rusia los hechos ocurridos en Cataluña? ¿Solamente fue puesta en cuestión por los medios de comunicación rusos la actuación en Cataluña frente a la consulta del 1 de octubre? Creo que es obvio que no, pero si usted tiene otra opinión, le pido que me la explique. Lo que nosotros hemos visto es que las principales portadas de los medios de comunicación internacionales no aceptaban que en un Estado democrático se arremetiera contra la población, porque el principio de mínima intervención penal hubiera hecho innecesaria una intervención de esas características y la utilización de la violencia contra la población desarmada. No es algo que se nos haya ocurrido en nuestro país, sino que es un valor democrático de preservación de bienes jurídicos protegidos en el momento en el que se tienen que producir intervenciones proporcionadas. Eso es lo que supuso el escándalo mundial; no fue un escándalo en Rusia, sino que fue un escándalo mundial. Le digo que estamos muy preocupados por estos informes que vienen de un instituto que es real, cuya presidencia de honor la ostenta el rey de España. Estamos muy preocupados porque entendemos que pueden formar parte de una estrategia de intoxicación y desinformación. Entendemos que algunas de las afirmaciones que contienen estos informes son un ataque al pluralismo político, que es un valor fundamental en nuestra democracia.

Muchas gracias.

El señor **PRESIDENTE:** En primer lugar, los informes del Real Instituto Elcano son públicos, están en la web y se repartieron no por iniciativa del Instituto Elcano, sino por iniciativa mía. Me parecía que, teniendo una compareciente como la que hemos tenido hoy, era aconsejable que tuviesen documentación previa para que sus señorías pudiesen formular sus propias tesis, como el señor Mayoral ha hecho.

En segundo lugar, la compareciente debe responder de los informes de los que es autora. Si mis datos son correctos, ella forma parte de la plantilla fija del Real Instituto Elcano desde 2016. No creo que esté en condiciones de responder sobre la filosofía del Elcano desde sus primeros tiempos, sobre su composición o sobre informes cuya autoría no corresponden a la señora Milosevich.

En tercer lugar, es perfectamente admisible en cualquier comparecencia parlamentaria que los diputados y los senadores que intervengan hagan las preguntas que consideren a la compareciente que tiene la bondad de estar con nosotros o maticen o critiquen las bases sobre las que se ha hecho, cosa que ha hecho el señor Mayoral. De la exposición del señor Mayoral, entiendo que no hay ninguna pregunta concreta sobre el tema de Rusia y de Cataluña, salvo algunas observaciones marginales que nada tienen que ver con la señora Milosevich. **(El señor Mayoral Perales: Presidente, usted está haciendo una valoración que no corresponde al presidente de una Comisión. Está haciendo una valoración política. Quiero elevar una protesta, porque usted está haciendo una valoración política de mi intervención. No forma parte de sus funciones como presidente).**

Perdóneme, estoy yo en uso de la palabra y no usted, y los debates los dirijo yo. Ya comprenderá que la señora Milosevich no tiene que responder sobre las cargas policiales del 1 de octubre. No es su función ni es su competencia. Me parece que eso es una evidencia. Por tanto, lo que estoy intentando es reconducir el debate al objeto de esta Comisión. No estoy criticando para nada la intervención del señor diputado. **(El señor Mayoral Perales: Lo está haciendo, señor presidente).**

¿Quiere usted decirme algo? Ahora sí que le doy la palabra. ¿Cuál es la valoración que yo he hecho?

El señor **MAYORAL PERALES:** Usted está haciendo una valoración política…

El señor **PRESIDENTE:** Dígame en qué he hecho una valoración.

El señor **MAYORAL PERALES:** Consta en el *Diario de Sesiones*.

cve: DSCG-12-CM-67

El señor **PRESIDENTE:** Pero dígame en qué he hecho una valoración, por si tengo que rectificar.

El señor **MAYORAL PERALES:** No voy a repetir lo que consta en el *Diario de Sesiones*, pero usted se está extralimitando en el ejercicio de la Presidencia haciendo una valoración política de nuestro grupo, prevaliéndose de su posición de presidente de esta Comisión y quiero elevar una protesta para que figure en el *Diario de Sesiones*.

El señor **PRESIDENTE:** Que figure en el *Diario de Sesiones.*
Muchas gracias por su intervención, señor Mayoral.
Tiene ahora la palabra el representante del Grupo Parlamentario Socialista, señor Hernando.

El señor **HERNANDO VERA:** Gracias, señor presidente.
Gracias, señora Milosevich. Quiero agradecerle especialmente su comparecencia. Sabemos que tenía un viaje pendiente a Alemania y que precisamente lo ha retrasado por estar hoy aquí ilustrando a esta Comisión y, desde luego, mi grupo se lo agradece. También le informo de que, efectivamente, España es un Estado social y democrático de derecho gracias a la Constitución de 1978 y a un pacto constitucional de entonces, sobre la base del cual, en desarrollo del cual y gracias al Reglamento de esta Cámara usted puede venir aquí a expresarse con toda la libertad y a decir lo que estime conveniente sin que ningún grupo de esta Cámara pueda condicionar sus manifestaciones aunque no le gusten. Por tanto, bienvenida a expresarse con toda libertad en el Congreso de los Diputados, que representa a toda la ciudadanía española.
El otro día hubo un compareciente que vino del centro para la seguridad nacional, y nos dijo que para determinar ciertas campañas de desinformación, información, ciberataques, etcétera, había que tener una aproximación holística, una aproximación integral. Y creo que lo que usted ha hecho hoy es una aproximación intelectual y académica a la autoría de lo que parece evidente que es toda una campaña; una aproximación desde la academia y desde un instituto de estudios. Por tanto, bienvenida sea esa otra vertiente de la aproximación al problema que usted ha tratado, que nos parece fundamental. A usted le van a decir —o ya le han dicho— que por qué hay que cuestionar lo que dice RT, Russia Today o Sputnik y no lo que dice el *New York Times*, *El País* o la BBC, porque, por qué no iba a ser cierto lo que dice el señor Julian Assange de que España es una república bananera y no la denuncia que hace *El País*, la BBC o el *New York Times* acerca de la campaña de Rusia. Pues mire, cada uno con sus medios, cada uno que estime si Russia Today o Sputnik son los medios que informan objetivamente de la situación que se ha vivido en Cataluña o si son estos medios tan vilipendiados de las democracias liberales, como son algunos de los que he mencionado y de los que usted ha mencionado. Por cierto, estos medios también han publicado informaciones que no nos han gustado, pero estamos seguros de que nadie se las ha dictado desde ningún sitio.
Usted nos ha dicho que el crecimiento del 2000 % de los mensajes a través de las redes sociales durante el proceso de Cataluña, llamémoslo así, provienen de Rusia, de hackers rusos o del territorio ruso. Nos ha dicho que Rusia tiene estas prácticas integradas en su estrategia de inteligencia. Nos ha dicho que los medios que retuitean a estos hackers y a estos bots son medios financiados por la Administración rusa, son públicos: aproximadamente 320 millones de euros. Nos ha dicho que las políticas y procedimientos que se han utilizado en Cataluña son similares a las prácticas y procedimientos que se han utilizado con ocasión del brexit, de las elecciones alemanas o de las elecciones norteamericanas. Por cierto, el Senado y el Congreso de los Estados Unidos tienen abierta una Comisión de investigación a este respecto y el objetivo es Rusia. El otro día se lo preguntaban, ni más ni menos, que al fiscal general de Estados Unidos, el señor Sessions. Nos han dicho que los robots y los hackers están instalados en territorio ruso, incluso ha nombrado la ciudad en la que están instalados; nos ha dicho que cuentan con personas como el señor Snowden, que está refugiado en Rusia desde hace años —yo me quedo con el Snowden que dibujaba Oliver Stone, y no con el actual con cierto síndrome de Estocolmo—. Nos ha dicho que los argumentos que se utilizan por estos medios y que son retuiteados algorítmicamente a quien benefician es a Rusia y a sus argumentos respecto a repúblicas caucásicas, respecto a Chechenia, respecto a Ucrania. Nos ha dicho todo esto, y ahora usted concluye que el Gobierno ruso lo mismo tiene algo que ver con esto. ¡Qué atrevimiento, qué osadía, señora Milosevich!, pero voy a estar de acuerdo con usted. Porque cuando anda como un pato, vuela como un pato, nada como un pato, y dice cua cua, suele ser un pato y no un oso hormiguero. Esa es la cuestión. Seguramente lo que no podemos hacer —y usted es experta y yo no— es quedarnos callados. Está bien que usted esté aquí porque usted puede decir

cve: DSCG-12-CM-67

cosas que no pueden decir las autoridades españolas por razones que todos conocemos. Pero está bien que usted lo diga y, desde luego, en mi caso coincido con usted absolutamente.

Usted dice en uno de sus documentos: No es suficiente con contar la verdad. No, no es suficiente con contar la verdad. Ante la campaña de desinformación, no es suficiente con contar la verdad, porque las mentiras estas son mentiras que nos perjudican, que nos han perjudicado, que han perjudicado a nuestra imagen internacional, y que han perjudicado la lectura que mucha gente de buena voluntad ha hecho gracias a la información que se ha difundido a través de estos medios.

Por lo tanto, no sé si lo que hay que hacer es lo que está haciendo el Gobierno de los Estados Unidos, que no me gusta, que es impedir que Google, impedir que Twitter, retuiteen información de Russia Today o de Sputnik. Seguramente en las democracias liberales estas cosas no nos gustan; ellos sí pueden hacerlas, no pasa nada, pero nosotros esto no podemos hacerlo, no debemos hacerlo. En todo caso, lo que creo que no debemos hacer es quedarnos callados. Por eso, mi grupo le da la bienvenida a esta Comisión y le agradece que hoy esté aquí diciendo lo que ha dicho.

Gracias.

El señor **PRESIDENTE:** La señora Milosevich está aquí porque así lo decidió por unanimidad la Mesa y portavoces, y habrá tantas comparecencias como la Mesa y portavoces quieran que haya en esta Comisión.

Tiene ahora la palabra la señora Vázquez, por parte del Grupo Popular.

La señora **VÁZQUEZ BLANCO:** Muchísimas gracias, señor presidente.

Quiero darle la bienvenida a la señora Mira Milosevich a esta Comisión. La verdad es que yo desde hace muchos años soy de las personas que leo los informes del Real Instituto Elcano; en muchos coincidiré, en otros no, pero en todo caso son informes muy rigurosos en los que se aprende muchísimo. Soy muy aficionada a los informes sobre terrorismo yihadista —Carola y otros profesionales que trabajan en el Instituto Elcano son unos magníficos profesionales—, a pesar de que hoy aquí algún partido que está detrás de mí no debe de ser consciente de lo que tratamos en esta Comisión. Le quiero explicar que esta no es una Comisión de Defensa, no. Seguridad Nacional tiene que ver con el medio ambiente, con la seguridad marítima, efectivamente con la defensa, pero con muchísimos parámetros, no solo nos dedicamos a la defensa.

Yo, en nombre del Grupo Parlamentario Popular, le pido disculpas por el atrevimiento, la osadía y la sinvergonzonería que han tenido estos señores que se sientan detrás de mí. **(Rumores).** Sí, le pido disculpas; y, sobre todo, le pido disculpas porque esta es una Comisión en la que, a propuesta del Grupo Parlamentario Popular, ya hace meses se está hablando de ciberdefensa y de crear esta ponencia de estudio, a pesar de que hoy no le ha interesado a algún grupo saber más sobre este tema.

El Grupo Parlamentario Popular es de los que cree que el mundo avanza, que la tecnología avanza, y avanza para bien y para mal. Hemos visto cómo, efectivamente, la huella digital es muy difícil de apreciar. Detrás de un perfil falso se puede esconder cualquiera, y se puede retuitear desde cualquier parte del mundo —como hoy usted nos ha dicho—, y se puede retuitear sesenta veces en un segundo. Es decir, esto es algo que se nos escapa del concepto normal de Internet. Hoy hemos escuchado cómo, efectivamente, un 2000 % procedía de Rusia… **(Rumores).** Señor presidente, le pido amparo para que no me molesten.

El señor **PRESIDENTE:** Tiene usted mi amparo.

La señora **VÁZQUEZ BLANCO:** Yo les estuve escuchando a ellos con toda la atención. Creo que el Grupo Podemos hoy no está contento…

El señor **PRESIDENTE: E**stoy seguro de que lo van a hacer con la misma cortesía que usted ha demostrado.

La señora **VÁZQUEZ BLANCO:** Muchas gracias, señor presidente.

Nosotros recibimos ciberataques, efectivamente, a nuestras empresas y particulares en España —se ha incrementado por seis en los últimos tres años—, y ahora, a raíz de este referéndum ilegal de Cataluña, hemos recibido no ciberataques, lo que usted hablaba de una desinformación, de una guerra híbrida intencionada para, de alguna manera, atacar las democracias liberales de Europa. Esto ha pasado con el *brexit*, ha pasado con las elecciones americanas, con las francesas, y nosotros lo estamos viviendo ahora.

cve: DSCG-12-CM-67

De hecho, la Comisión Europea dice que a partir de enero pondrá en marcha un equipo multidisciplinar para ver cómo se puede combatir este tipo de ataques y guerras híbridas que está sufriendo Europa. Que vaya con esto mi primera pregunta, para que me haga una valoración de si el trabajo que se va a hacer en esta Comisión es el oportuno. Nosotros, a diferencia de otros países, no podemos prohibir las redes sociales, tenemos que convivir con ellas, pero —como decíamos— nos tenemos que defender, nos tenemos que defender de lo que podemos llamar ciberguerras. Como usted ha dicho, ya no hay campos de batalla, ahora es en el ciberespacio donde se producen las ciberguerras y es donde todos los países democráticos tenemos que saber combatirlas. Son campañas de manipulación, de información en redes. Hemos visto como un señor desde la embajada de Ecuador remetía 40 000 tuits u otro desde la embajada de Rusia remetía también cerca de 100 000 tuits. Estamos hablando de una web-brigada de *trolls*, de *hackers*, de *bots*, de *sockpuppets*, es decir, de un ejército virtual para desestabilizar países, sí. Aquí ha dicho la ministra de Defensa que el 55 % de los mensajes vinieron de territorio ruso y un 30 % de Venezuela. Me gustaría preguntarle —porque seguramente al Grupo Podemos también le interesa— si lo de Venezuela tenía algo que ver con el Gobierno. Por cierto, a lo mejor en el futuro necesitaríamos tener algún informe sobre qué papel jugaron Venezuela y los retuits, ese 30 % de retuits que se hicieron desde territorio venezolano, en la crisis que hubo con Cataluña y el referéndum ilegal. Me gustaría tener alguna información al respecto. Me extraña que Venezuela esté mandando mensajes para desestabilizar España, la verdad, me extraña muchísimo. Por eso necesitaría que nos ampliase la información que tenga sobre Venezuela.

Entiendo que al Grupo Podemos no le guste su informe. No lo dijo la señora Mira Milosevich, lo dijo *The Economist* el 15 de febrero de 2014, cuando expuso que Podemos podía estar recibiendo financiación de Rusia. No lo dijo la señora ponente que está hoy aquí, lo dijo *The Economist*. Así que, señor Mayoral, a quien tiene usted que demandar, si no la recibe, es al periódico y al periodista y, mientras, tiene que escuchar a los demás, no le queda otro remedio. Ustedes, lo que no les gusta, lo censuran, como hacen en los países que defienden, Venezuela, Irán. **(El señor Mayoral Perales: Nosotros no hemos metido en la cárcel a nadie. Aquí se mete a la gente en la cárcel por opinar).** Todo lo que no les gusta, ustedes lo censuran.

Aparte de Venezuela, me gustaría hacerle otra pregunta. ¿Qué puede aconsejar usted al Gobierno de España y a los ciudadanos españoles?, porque creo que tenemos que tener conciencia de lo que es verdad y de lo que es mentira. Hubo imágenes ese día que muchos llegamos a creernos. Hay gente que ha puesto en cuestión esa carga policial, incluso se ha puesto en cuestión a profesionales. Por tanto, ¿qué podemos hacer los ciudadanos españoles y el Gobierno para mitigar estos ataques que podemos sufrir? ¿Qué nos puede aconsejar de cara al 21 de diciembre? Lo que ha pasado el 1 de octubre puede volver a repetirse, por tanto, ¿qué cree que podemos hacer como ciudadanos, como Gobierno y como democracia liberal para no volver caer en las mentiras de esa ciberguerra que hemos sufrido durante estos últimos meses?

El otro día recibimos aquí al director del Incibe y dijo que en el futuro se necesitarían unos 6000 puestos de trabajo más en ciberdefensa. ¿Qué valoración le merece crear equipos de voluntarios, de gente con talento que colabore con los Estados en ciberdefensa? Me refiero a una especie de ciberreserva, de reservistas, gente que puede poner sus aptitudes a disposición de la ciudadanía. En un ciberataque masivo recibido en Reino Unido fue un joven el que solucionó el problema, por eso le pregunto qué opinión le merece.

Para finalizar, le doy de nuevo la bienvenida. El presidente decía al principio que no nos parecemos a la universidad. Le pido disculpas, porque hoy hemos sido peor que el patio del colegio. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señora Vázquez.

Tiene la palabra la señora Milosevich, luego habrá, como es tradición, un segundo turno de tres minutos. Por tanto, vayan preparando sus preguntas haciendo gala de la continencia verbal que caracteriza a los miembros de esta Comisión.

Señora Milosevich.

La señora **MILOSEVICH-JUARISTI** (Investigadora principal del Real Instituto Elcano y profesora asociada de Historia de Relaciones Internacionales del Instituto de Empresa, IE University): Muchas gracias, procuraré ser breve, concreta y concisa en las respuestas para que nos dé tiempo y así lleguen ustedes a comer.

cve: DSCG-12-CM-67

Agradezco al presidente de la Comisión todas las precisiones que ha hecho sobre el Instituto Elcano, solo añadiré una refiriéndome a su instituto. El instituto no es mío, soy miembro —y con mucha honra, porque respeto mucho la institución— del Instituto Elcano, sin embargo el Instituto Elcano no es responsable cien por cien de lo que yo escriba. Como puede reflejar la página web del Instituto Elcano, hay informes muy diferentes que reflejan opiniones personales, análisis personales; justamente uno de los objetivos del Instituto Elcano es ofrecer variedad de opiniones para crear un debate público y llegar al mayor número de lectores y al mayor público en España.

Dicho esto, sobre las preguntas que se me han hecho, muchísimas gracias por los comentarios. Yo dije que pensaba que esto era una universidad simplemente por responder directamente a cada pregunta, pero sobre todo porque yo entiendo aquí mi presencia en el sentido de lo que yo soy. Soy una doctora en Estudios Europeos, soy autora de un libro sobre Rusia y de varios libros más; es decir, vengo del mundo académico, no tengo ciberpruebas y mi análisis es un análisis académico con —creo yo— bastante y suficiente conocimiento sobre Rusia. Yo he emigrado de un país donde no se podía hablar y he venido a uno democrático para hablar, y me honra mucho estar en el Congreso de los Diputados de España. Soy española ahora, pero quiero decir que una de las razones de emigrar fue justamente porque no quería vivir en un ambiente donde no se podía hablar abiertamente. Pero vamos a las preguntas.

Aquí hay una pregunta clave que ha aparecido en dos ocasiones, que suponía que se iba a plantear y que he intentado explicar: ¿Hay pruebas directas de que es el Gobierno ruso? Yo no tengo pruebas directas de que sea el Gobierno ruso. Pero, como he intentado explicar, la complejidad, la combinación y la coordinación —porque ocurren en un mismo espacio de tiempo— necesitan un actor gubernamental o que esté cerca del Gobierno para coordinarlas. Yo no puedo decir que esto fuese ordenado por el Gobierno ruso, no lo puedo decir porque no tengo pruebas de ello, pero tengo elementos y argumentos de los que lo deduzco e intento probar mi hipótesis de que se trata de un apoyo oficial. Es cierto que las ciberbrigadas, incluso la que existe en San Petersburgo, las puede alquilar cualquier persona. Son ejércitos virtuales que están a disposición de quien los paga, de quien los alquila, de quien los exige, pero también es curioso que esté en San Petersburgo, y es uno de los conocidos, por no hablar de los que están en Siberia o en lugares más remotos.

Dicho esto, respecto a la pregunta sobre la estrategia para luchar contra la ciberdelincuencia y el comentario del presidente de esta Comisión, que realmente se les debe tratar como a piratas, sin duda alguna hay una necesidad de legislar a nivel, primero, de la Unión Europea y, luego, a nivel internacional. Esto no lo tenemos; no lo tenemos porque es un fenómeno relativamente nuevo para Occidente. Para Rusia no es un fenómeno nuevo. Yo les puedo hablar desde los revolucionarios que inspiraron a Lenin; el mismo Lenin dijo que las palabras y la información son como bombas porque tienen un poder. En este sentido, es necesaria la legislación, y yo creo que España, como país de la Unión Europea, tiene que contribuir primero en la Unión Europea y luego, obviamente, también como miembro de la Alianza Atlántica. El pasado 6 de diciembre de 2016 la Unión Europea y la OTAN habían firmado ya un acuerdo de colaboración. Teniendo en cuenta que se trata de un fenómeno relativamente nuevo, los occidentales todavía no están completamente preparados para ello. Luego, creo que hay mucha confusión entre lo que se considera ciberataques y lo que se considera desinformación al usar ciberespacio. Las redes sociales e internet son dos cosas diferentes y son dos cosas que se deben abordar y legislar. La ciberseguridad es más fácil de legislar porque se puede percibir con más facilitad.

En cuanto a las campañas de desinformación y de influencia política, existen desde que existen las campañas políticas y desde que existe el hombre, otra cosa es cuando un país las usa como un instrumento. Por tanto, apoyo absolutamente la idea de una legislación no solo en España, sino una coordinada con la Unión Europea.

Agradezco a la portavoz del Grupo Popular la aclaración de que lo que yo cito aquí es un artículo de *The Economist*. Marine Le Pen del Frente Nacional en Francia ha dicho que efectivamente ha recibido financiación del Kremlin, de Vladimir Putin; lo ha dicho abiertamente, no es ningún secreto en Francia, y hubo prácticas en otros países de ello. En cuanto a que el partido político Podemos, como dice el artículo de *The Economist*, pueda ser uno de los receptores, el mismo *The Economist* dice que es difícil probarlo, pero yo tengo entendido que respecto de la financiación del Grupo Podemos se ha hablado en la Cámara y hay varias causas. **(El señor Mayoral Perales: ¡Archivadas!).** En eso no entro ni estoy aquí para hablar de ello, sino de mi informe, aunque agradezco la cita de *The Economist*.

Usted preguntó si España está en guerra con Rusia y si somos conscientes de que hay efectivos españoles en el Báltico. Pues sí, claro que hay efectivos, porque España es un país que pertenece a

cve: DSCG-12-CM-67

la OTAN, a la Alianza Atlántica. Después de la anexión de Crimea y después del apoyo militar, económico y político de Rusia a los prorrebeldes rusos en Donbáss, la OTAN ha empezado a cambiar su estrategia y, efectivamente, la participación de España corresponde al hecho de que es miembro de la Alianza Atlántica. Por tanto, creo que España hace bien al demostrar su solidaridad con otros miembros de la Alianza Atlántica. Esto no se cuestiona.

Usted también preguntó si mi informe era fiable. No voy a comentar si los otros informes de El Cano son fiables. En esto no entro. Mi informe es fiable. Esta pregunta sinceramente me recuerda a lo que comenta Margarita Simonova al decir que no hay una verdad objetiva y que su trabajo es ofrecer un punto de vista alternativo. Yo no intento ofrecer ningún punto de vista alternativo; yo soy una experta en Rusia, he trabajado muchos años en ello y mi análisis se basa en mi conocimiento de historia, de las prácticas y, en este caso, de los documentos oficiales de Rusia.

Señoría, usted también ha mencionado que yo no hago diferencia entre política y guerra. Léase el concepto de disuasión estratégica del documento oficial ruso y verá que los mismos rusos dicen que la línea entre la guerra y la paz se esfuma en este concepto. Lo cito en este caso. La Federación Rusa lo llama guerra de información, *информация война (informatsionnaya voyna)*. Usa la palabra guerra y lo pone en su doctrina militar. Por tanto, creo que yo aquí no he inventado nada.

Agradezco especialmente el apoyo al señor Hernando y la comparación con el pato —aquí puede ser incluso más divertido de lo que uno espera—. Agradezco su apoyo y sobre todo agradezco la valoración que me hace como analista y como persona que viene del mundo académico. De todo lo que ha dicho quiero centrarme especialmente en lo que ha sacado del informe, que no es suficiente contar la verdad. Con este informe yo no he intentado ofrecer una visión alternativa, yo he intentado llamar la atención de un fenómeno que está ocurriendo y que no ha ocurrido en octubre con el referéndum de Cataluña. Es un fenómeno sobre el que yo escribí primero en enero, un fenómeno que está ocurriendo en todos los países occidentales. Es también un fenómeno que no es solo practicado por Rusia, esto está claro, pero aquí estamos para hablar de Rusia, yo hablo de Rusia porque yo sé de Rusia. Otros lo usan de otra forma; la misma campaña del presidente Trump se basó mucho en el uso de las redes sociales. También es cierto que el 40 % de los estadounidenses exclusivamente se informan a través de redes sociales. Quiero decir que hay oportunidades que se aprovechan. Cuando digo que no es suficiente contar la verdad, quiero decir que hay una estrategia detrás de ello. Tenemos que contar la verdad y contrastarla, pero en la vida política y en la vida pública de los países democráticos continuamente se dice algo y se desmiente, es normal, lo que no se ve es que hay una estrategia de influir negativamente. Existen los conceptos de soft power y hard power. El poder blando es el poder de influir pacíficamente, nadie lo niega, pero influir en términos negativos y desacreditar es una estrategia, no es una negligencia ni un deseo de influir.

Respecto a las preguntas de la portavoz del Grupo Parlamentario Popular, tengo que decir que no puedo hablar de las injerencias del territorio de Venezuela porque no soy experta en Venezuela, pero no me sorprenden, además era muy esperable que Nicolás Maduro preguntara inmediatamente quién es España para hablar de lo que hace Venezuela, etcétera. Quiero decir que este comentario era esperable y que la injerencia de Venezuela no me sorprende, pero no la puedo argumentar porque no tengo información.

¿Qué puedo aconsejar yo? A mi hijo le aconsejo que estudie la carrera de «ciberoficio» **(Risas),** creo que es el futuro, pero él quiere estudiar medicina. En fin, perdonen estos comentarios personales, pero solo quería subrayar la importancia que va a tener esto en el futuro. Creo que la guerra convencional no se va a librar, bueno, tiene mucha menos probabilidad que las guerras de ciberespacio. Las guerras futuras son las guerras del ciberespacio, y es una dimensión que asusta porque no la podemos controlar, no podemos usar el concepto de disuasión clásico. Podemos protegernos, pero disuadir a alguien para que no lo haga es difícil en el ciberespacio; en el conflicto convencional sí es posible. ¿Qué puedo aconsejar? En primer lugar, distinguir entre la ciberseguridad y la desinformación. Por lo que he leído y lo que se ha explicado, creo que vamos bastante bien con la ciberseguridad, no hay que confundirlo. La OTAN distingue entre *strategic communication* y ciberseguridad, pero los rusos no hacen esta distinción. Los rusos usan ciberespacio y tienen su *strategic communication*, tienen sus mensajes. Quiero decir que allí hay una brecha en la percepción de las posibles amenazas. Nos falta trabajar, nos falta crear una estrategia, pero esta tiene clarísimamente que basarse en esta distinción entre ciberseguridad, ciberataques y desinformación, y no solo respecto a Rusia. Y creo que en el mundo en que vivimos, el no poder distinguir verdad y mentira es uno de los objetivos de estas campañas, crear caos y crear esta duda sobre lo que es verdad y lo que es mentira y con esta duda poner a tu adversario en la posición de la

cve: DSCG-12-CM-67

apatía y quitarle la capacidad de tomar decisiones por no tener los suficientes elementos para decidir y para ponerlas en práctica.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señora Milosevich.

Empezamos la segunda ronda de intervenciones. Señor Yanguas.

El señor **YANGUAS FERNÁNDEZ:** Simplemente quiero agradecerle de nuevo sus explicaciones a la señora Milosevich.

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

Señor Salvador.

El señor **SALVADOR GARCÍA:** Yo sí quiero aprovechar este turno, porque me he sentido ofendido por las palabras de la persona que ha intervenido después de mí; me refiero al señor Mayoral. No quiero que usted se lleve la impresión de que en esta Cámara al compareciente, que viene a hablar con absoluta libertad y que además lo hace basándose en un informe que ha firmado y por el que da la cara —por tanto no lo hace desde la desinformación sino desde su información— se le amedrenta y se le intenta asustar porque, poco más o menos, puede haber cometido un delito en su comparecencia. Por tanto, quiero transmitirle seguridad y decirle que precisamente el grupo político que ha intervenido es el grupo político que cada vez que utiliza la palabra democracia lo hace precisamente para asociarla a Irán, a Venezuela, a Rusia y a todos los independentistas que intentan romper este país. Para ellos eso es la democracia y el nuevo orden mundial. También quiero que usted sepa que ese partido —aunque me imagino que como persona informada que es lo sabe— es un partido que en el Pacto de Estado antiyihadista, en el que están todas las fuerzas políticas, está de observador, porque parece ser que no reúne las garantías suficientes; me imagino que será con los yihadistas, porque, si no, no entiendo por qué está de observador. **(El señor Mayoral Perales: Eso es una irresponsabilidad, lo que acaba de decir es una irresponsabilidad. Le pido que lo retire. Pido que retire usted lo que acaba de decir. Es una irresponsabilidad lo que acaba usted de hacer en esta Comisión. Le pido que lo retire).**

El señor **PRESIDENTE:** Señor Mayoral, le daré la palabra en el acto. **(El señor Mayoral Perales: Es usted un irresponsable).**

El señor **SALVADOR GARCÍA:** Perdón. Yo a usted le he respetado… **(El señor Mayoral Perales: Usted no me ha respetado con lo que acaba de decir, ni a mis votantes, ni a esta Comisión, ni al Congreso).**

El señor **PRESIDENTE:** Señor Mayoral, le voy a dar la palabra y la tendrá usted tres minutos, pero no está en este momento en el uso de la palabra.

El señor **SALVADOR GARCÍA:** Por supuesto, y yo le escucharé callado, con absoluta atención, pero le repito lo que he dicho por si acaso es que no me ha entendido bien, aunque me parece que a usted también, como en Internet, le interesa más el ruido que el contenido. He dicho que ustedes están de observadores en el Pacto antiyihadista que han firmado todos los partidos, porque a lo mejor no se dan las condiciones adecuadas de cara a las garantías de los yihadistas. Es un condicional y así lo he dicho. Y usted no es nadie para intentar amedrentar en una Comisión a la persona que comparece. A usted le respetamos su turno de palabra y su intervención, pero en el mío digo lo que quiero y, evidentemente, consta en el *Diario de Sesiones*. No tengo que decirle al presidente que lo haga constar porque lo estoy haciendo dentro de mi intervención. Y entendía que lo que teníamos que decir era preceptivo, porque lo que aquí en este momento estamos analizando —y en eso me hubiera gustado también escuchar al señor Mayoral y no le he oído en ningún momento— son los hechos objetivos que traían esta comparecencia a colación. No le he visto hablar de que realmente ha habido una intromisión organizada en Cataluña, no le he oído hablar de dónde procedían esos ataques, no le he oído hablar de qué instrumentos se estaban utilizando; lo que le he oído y le he visto hacer ha sido intentar verter una cortina de humo para intentar despistar y convertir a los informantes en desinformantes, para tapar a los que realmente nos están desinformando a todos. Por tanto, señor Mayoral, usted lo tiene muy fácil; todo lo que yo he dicho consta en el *Diario de Sesiones*.

cve: DSCG-12-CM-67

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

Voy a dar la palabra al señor Mayoral inmediatamente. Me ha pedido el representante del Grupo Podemos en la Mesa que haya una Mesa informal e inmediatamente la haremos. Me gustaría que recondujésemos el clima de esta Comisión Mixta, que ya tiene bastantes complejidades, para dedicarnos en cada una de las sesiones a los temas que son objeto de la comparecencia y que fueron aprobados por unanimidad por todos los miembros.

Señor Mayoral, ahora sí tiene la palabra.

El señor **MAYORAL PERALES:** En primer lugar, estoy muy sorprendido por la irresponsabilidad de algunos de los portavoces que me han precedido en el uso de la palabra. Me parece excepcionalmente irresponsable que se ponga en cuestión la unidad de las fuerzas democráticas de este país en la lucha contra el terrorismo yihadista. Es una irresponsabilidad que no se merece nuestro pueblo. Y si alguien quiere saber por qué nosotros no firmamos, es porque se han introducido normas en el ordenamiento jurídico cuya aplicación ha tenido consecuencias contrarias a los principios básicos del Estado de derecho, algo que no compartimos con el Grupo Ciudadanos. A Ciudadanos le pareció bien que ingresaran en prisión provisional durante un mes unas personas por hacer una obra de títeres en carnaval. A nosotros no nos parece bien y creemos que ataca los principios más básicos de la democracia.

En nuestro país tenemos experiencia acerca de noticias falsas en las redes. Las inauguró el PP, en concreto el señor Alejandro de Pedro. Y esto no lo decimos nosotros, sino los jueces en la trama Púnica, cuyos componentes son los que han intentado manipular las redes.

Hacer afirmaciones gruesas contra fuerzas políticas democráticas y a continuación decir «no tengo pruebas, pero lo reitero» no es una actitud responsable en una comparecencia en el Congreso de los Diputados. Creo que le falta alguna información sobre mi grupo. Ha dicho que tenemos causas sobre financiación, y debo decirle que se han archivado catorce, que fueron promovidas por una organización —Manos Limpias— calificada por los jueces como organización criminal. Sus miembros acabaron en prisión y parece que tienen nexos con las cloacas. Se lo digo para que tenga información, para que sepa que en esta Cámara el único partido que se encuentra investigado por financiación ilegal es el PP. Son datos que le pueden venir bien de cara a las afirmaciones que pueda seguir haciendo en esta Comisión.

A veces, cuando escuchamos algunas cosas, nos da la impresión de que se confunde la libertad de información con la necesidad de implementar una doctrina de la seguridad nacional que ponga en peligro la posibilidad de que las redes sean un espacio de libertad donde las personas se puedan expresar y en la que alguien se pueda atribuir la posibilidad de decir cuáles son los medios de comunicación que pueden funcionar y cuáles no. Esas son derivas peligrosas, porque la doctrina de la seguridad nacional ha tenido esas derivas. La doctrina de la seguridad nacional ha perseguido y criminalizado al disidente.

Yo no voy a decir a la portavoz del grupo parlamentario que es una sinvergüenza, como ha hecho en su exposición, porque esta Comisión no se lo merece, pero sí es irresponsable. Es irresponsable en relación con muchas de las afirmaciones que se están vertiendo en la Comisión. Simplemente voy a pedir un poquito de responsabilidad y le voy a reiterar una sola pregunta que he hecho al principio: ¿Usted considera que España está en guerra con Rusia? Es una pregunta muy sencilla. Usted lo afirma veladamente en su informe y me gustaría conocer su opinión al respecto. Además, le he puesto un ejemplo muy claro. Le he dicho que en estos momentos hay desplegadas tropas españolas en los países bálticos, frontera con Rusia. ¿Existe o no, según su manera de entender, una guerra con Rusia? A esta Comisión le interesa.

Por otra parte, ya que es experta en los países del Este, me ha extrañado mucho que, hablando de Cataluña, no se haya referido a cuál es la opinión de los letones acerca de la cuestión catalana. Me sorprende. Entiendo que es miembro de la OTAN y no de la Unión Europea, pero ha tenido un papel y creo que en su día nacional no ha pasado inadvertida la bandera independentista, creo.

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

Señor Hernando.

El señor **HERNANDO VERA:** Voy a intervenir brevísimamente, señor presidente.

Señora Milosevich, si alguien pretende que ante una campaña de las características de la que hemos estado viendo en el proceso de Cataluña, en el *brexit* o en las elecciones de Estados Unidos se le pregunte al Gobierno de Rusia si tiene algo que ver y que el Gobierno de Rusia lo afirme está un poquito descaminado. Recuerdo que durante la Guerra Fría el representante de la KGB en las instituciones y en

cve: DSCG-12-CM-67

las embajadas solía ser el agregado cultural. Nadie reconocía que era el representante de la KGB. Es un poco infantil pensar que se le va a preguntar al Gobierno de Rusia si tiene algo que ver con esto y que el Gobierno de Rusia va a decir sí y va a levantar las manos. Por tanto usted ha hecho una aproximación académica, como experta y conocedora de Rusia y de la política rusa en la historia y en la actualidad, y eso es con lo que nos quedamos, y ese es un testimonio muy importante para esta Comisión.

Usted ha asistido a un ejemplo de un debate parlamentario en una democracia deliberativa, de Rawls y de Habermas, y hay otros modelos: la del pueblo confrontativo, la del maniqueísmo, la de Laclau… pero esta es esta y esto está bien. O sea, que ha tenido usted un buen ejemplo.

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

Señora Vázquez.

La señora **VÁZQUEZ BLANCO:** Muchas gracias, señor presidente.

Quiero finalizar agradeciendo la respuesta a las preguntas. Efectivamente en esta Comisión hasta ahora había un clima maravilloso, hasta que intervino el señor Mayoral. No sé si es esa la excepción. Ya veo la importancia que ha dado a los ataques desde Rusia con la Operación Cataluña que se ha delicado a hablar de la financiación del Partido Popular y de la financiación de su partido así como de la falta de libertad de los periodistas. Me viene a la cabeza el líder de Podemos, que decía que había que azotar a una periodista hasta que sangrase. Yo creo que por ahí va el tema de la libertad de expresión para los periodistas. En todo caso a nosotros sí que nos preocupan las campañas de desinformación desde Rusia, desde Venezuela y desde cualquier otro país, que vayan contra España, porque yo creo que hoy aquí, excepto el Grupo de Podemos, todos estamos preocupados por lo que ha sucedido durante los meses de septiembre y octubre en la Operación Cataluña precisamente porque intentan desestabilizar a nuestro país, pero es normal, porque este partido que está aquí detrás, según un amigo del señor Pablo Iglesias en el Senado, dice que Irán y Venezuela financiaban precisamente a este partido para desestabilizar España. Es normal que hoy se venga a esta Comisión y no preocupe al Grupo de Podemos el ataque desde Rusia o desde otros países a la integridad y a la democracia en nuestro país. A nosotros sí que nos preocupa, y por eso queremos comisiones como esta, señor presidente, en las que vengan comparecientes de nivel como el que tenemos hoy aquí, que ya les gustaría a muchos parlamentos poder escuchar a la señora Mira Milosevic.

Quiero agradecer al señor presiente y al señor letrado la celeridad con la que se están produciendo estas comparecencias, porque fue el jueves pasado cuando el Grupo Socialista la solicitó, y hoy está compareciendo aquí. Eso es algo inaudito en este Parlamento, así que he de felicitar al presidente y al letrado.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señora portavoz.

Señora Milosevich, tiene la palabra para concluir su comparecencia.

La señora **MILOSEVICH-JUARISTI** (Investigadora principal del Real Instituto Elcano y profesora asociada de Historia de Relaciones Internacionales del Instituto de Empresa, IE University): Concluyo muy brevemente. Quiero dar las gracias a todos los portavoces. Solo hubo una pregunta concreta, si estamos en guerra con Rusia. Desde mi punto de vista y mi valoración, no hay un peligro inminente de que se produzca un conflicto convencional en la frontera entre los países bálticos y Rusia. Las tropas que están allí forman parte del acuerdo del Consejo entre Rusia y la OTAN firmado en 2002. Quiero decir que las fuerzas rotativas que están desplegadas en el llamado flanco oriental no violan los acuerdos firmados con Rusia. Y solo una información más. Incluso el concepto estratégico de la OTAN de 2010, que considera a Rusia como socio estratégico, todavía es válido en la OTAN, cuando obviamente, con la anexión de Crimea, Rusia ha demostrado que no es exactamente un socio estratégico. ¿Está España en guerra con Rusia? Rusia está en guerra de información con España y con el resto de los países europeos.

Muchas gracias a todos. Muchas gracias por vuestra atención, y reitero que ha sido un honor para mí comparecer ante esta Comisión.

Muchas gracias. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señora Milosevich.

Ha sido un honor para todos nosotros oírla. Seguiremos escuchando a todos los expertos que los distintos grupos quieran traernos, para tener, eso sí, visiones alternativas y diferentes. **(Pausa).**

cve: DSCG-12-CM-67

— DEL GENERAL DE DIVISIÓN, JEFE DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD (GÓMEZ LÓPEZ DE MEDINA), PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. (Número de expediente del Congreso de los Diputados 212/001048 y número de expediente del Senado 713/000522).

El señor **PRESIDENTE:** Señorías, si les parece vamos a continuar con la sesión.

Comparece ahora el general Carlos Gómez López de Medina, jefe del Mando Conjunto de Ciberdefensa, para informar sobre diversas cuestiones relativas a la ciberseguridad en España. El procedimiento será el mismo, una intervención inicial del compareciente; una intervención de los portavoces de los distintos grupos de cinco minutos; una segunda intervención del compareciente y una segunda intervención de los portavoces por tres minutos.

General, tiene usted la palabra.

El señor **GENERAL DE DIVISIÓN, JEFE DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD** (Gómez López de Medina): Muchas gracias, señor presidente. Señorías, muy buenos días.

Muchas gracias por haberme convocado. Es para mí un honor estar aquí ante ustedes, y nuevamente muchas gracias porque me van a dar la oportunidad de informarles sobre qué hacemos, cuál es nuestra misión, cuáles son nuestros cometidos y cómo colaboramos en la mejora de la ciberseguridad de España. Incluso muchas gracias, presidente, por haberme permitido estar presente y oír a la señora Milosevich.

(Apoya su intervención con un *powerpoint).* Este es un breve esquema de lo que pretendo hacer, una pequeña introducción para entrar en materia, ponernos en el contexto que yo considero que es apropiado. Aunque sea muy rápidamente no quiero dejar de comentar lo que son los elementos fundamentales para nuestra unidad, contenido en ambas estrategias, en la de seguridad nacional y en la de ciberseguridad nacional. Y finalmente me centraré en lo que es mi unidad.

Les he dejado una definición de lo que es el ciberespacio, pero la verdad es que hay muchas. He escogido la que creo que puede ser más formal para nosotros, que es la que aparece en la Estrategia de Ciberseguridad Nacional. En casi todas se menciona el hecho de que Internet está en el ciberespacio, y esto me parece muy significativo para resaltar que si bien para nosotros, Fuerzas Armadas —y no solo las españolas, sino que me refiero a todas las Fuerzas Armadas occidentales—, Internet es un elemento fundamental del ciberespacio, también nos interesa muchísimo esa otra parte del ciberespacio que no es Internet precisamente.

Les daré algunas ideas sobre la descripción del ciberespacio, probablemente muchas de ellas conocidas para sus señorías: es un espacio artificial, pero real; el efecto puede ser virtual, pero es real, porque está compuesto de cables, de servidores, de equipos electrónicos; es real. Sin tiempo, o es tan pequeño que prácticamente es despreciable; por lo tanto sin distancia, porque da exactamente igual que el ataque provenga de Australia o de Burgos, da prácticamente lo mismo. Sin fronteras, lo cual tiene multitud de connotaciones. Afecta a todas las actividades de la sociedad; estarán sus señorías conmigo en que estamos absolutamente penetrados, el ciberespacio lo inunda todo: desde que llevamos un *smartphone* encima nuestra vida está más en el ciberespacio que en la realidad; nos despierta por la mañana y nos conduce a lo largo de toda la jornada. El entorno legal es muy complejo, un poco derivado de varias de las características que acabo de decir.

Ahora voy a tratar de incidir en algunas características desde el punto de vista operativo, más cercano a nuestro trabajo y a nuestra responsabilidad. Siempre en actividad: he sido un poco radical al decirles que no existe la paz; no quiero decirles que siempre estemos en guerra, no es cierto, pero sí hay una gran diferencia en comparación con los dominios convencionales, con los dominios físicos; siempre hay actividad y siempre hay ataques, de mayor o menor grado, pero siempre los hay. Múltiples actores: esto es tremendamente relevante; en el ciberespacio actúan desde *hacktivistas*, que puede ser una persona aislada, sin más, hasta un grupo de *hacktivistas* organizado: delincuentes, crimen organizado, terroristas y Estados; todos pueden hacer daño, evidentemente unos más que otros, pero todos son relevantes. Sin control de armamentos: para los profesionales de la milicia es muy frecuente hablar de un catálogo, que es el James, donde tienes el listado de todos los armamentos navales, aéreos y terrestres; aquí no hay un James, no hay un control real de armamentos.

Un par de ideas sobre las ciberarmas. La ciberarma normalmente es un arma de un solo uso, que además indirectamente produce una transferencia de tecnología: la víctima que recibe el impacto de esa ciberarma, si es capaz de retenerla, analizarla y hacer ingeniería inversa, si es capaz de mutarla, la puede devolver otra vez al origen o utilizarla en otra dirección, pero en cualquier caso ya se ha revelado el

cve: DSCG-12-CM-67

contenido y el efecto de esa ciberarma, y por eso digo que es de un solo uso habitualmente. Los ataques, haciendo una comparativa con los dominios reales, suelen tener planeamientos y preparaciones muy largos, pero la ejecución es tremendamente corta. Si piensan sus señorías en lo que sucedió en mayo con el incidente WannaCry se darán cuenta de que fue algo que se extendió en horas prácticamente por todo el mundo. Aunque el planeamiento y la preparación fuesen largos, la ejecución suele ser corta; pero no siempre, porque puede que el objetivo no sea dejar fuera de servicio un sistema, sino extraer información de ese sistema. Puede que lo que interese sea que ese elemento, el *malware* desplegado, quede latente durante mucho tiempo y vaya extrayendo información poco a poco. En ese caso la ejecución obviamente no es corta.

Seguimos con algunas características. Es tremendamente sorprendente que sea más fácil, barato, y por tanto eficiente, atacar que defender. Eso nunca sucedía. Normalmente para atacar una posición había que utilizar el triple de recursos utilizado por los defensores. Ahora no es así. Cuando hablamos del ciberespacio defender es mucho más caro que atacar. Además si eso lo unimos con alguna otra característica que voy a comentar a continuación, el atacante tiene poco que perder. Es muy atractivo atacar. Si se tiene la tremenda facilidad de tirar piedras y esconder la mano, y además es fácil y barato, es una mezcla tremendamente atrayente. Es posible alcanzar al adversario en profundidad, mucho más que con el poder aéreo, que fue un salto tremendamente importante a partir de las guerras mundiales. Cualquier instalación, cualquier infraestructura crítica, nosotros mismos con ese *smartphone* que comentaba anteriormente estamos en el ciberespacio, y por tanto al alcance de un posible atacante. Es un tema muy tocado la dificultad de la atribución. Es muy difícil decir quién es el responsable; casi les diría que es imposible de demostrar. ¿Qué sucede si el atacante firma su *malware*, de tal manera que diga que ha sido hecho en tal lugar? Tampoco, porque puede ser un ataque de bandera falsa; ni siquiera de esa forma.

Se ha comentado también en la comparecencia anterior que obviamente por todas esas características es muy utilizado en la guerra híbrida, y por supuesto en periodos de crisis, en los que la actividad en el ciberespacio se dispara. Aumenta mucho sobre situaciones de normalidad, hasta tal punto que constituye un quinto dominio de las operaciones, según la Alianza Atlántica, que aprobó la Cumbre de Varsovia de jefes de Estado y de Gobierno, en julio de 2016.

Daré unas ideas sobre la estrategia, que seguro que es conocida por sus señorías. Solo me interesa pararme en el capítulo 3, donde está la relación de riesgos y amenazas. Son doce, y en tercer lugar aparecen las ciberamenazas, pero lo que resulta interesante es que, con un segundo vistazo a esa lista, observamos —ahora resaltado en negro— que hay más amenazas —no solo las ciberamenazas— donde la utilización del ciberespacio tiene un especial protagonismo: conflictos armados, terrorismo, crimen organizado, espionaje, y por último —¡cómo no!— la vulnerabilidad de las infraestructuras críticas y servicios esenciales. En el capítulo 4 nuestra estrategia nos plantea los ámbitos prioritarios de actuación, y nos dice obviamente que para combatir las ciberamenazas hay que elevar el nivel de ciberseguridad. Como consecuencia, cuando se aprobó la Estrategia de Seguridad Nacional se aprobaron también una serie de estrategias especializadas: seguridad marítima, ciberseguridad y seguridad energética.

Pasamos a centrarnos por unos instantes en la Estrategia de Ciberseguridad Nacional. Aprobada a finales del año 2013 plantea un objetivo global tremendamente amplio y sencillo de tratar, pero muy complicado de lograr. Lo que se pretende es conseguir que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta. Plantea seis objetivos específicos, y a continuación establece ocho líneas de acción que voy a repasar muy rápidamente, porque creo que son muy interesantes. La primera de ellas lo que hace es plantear la necesidad de fomentar las capacidades reales de la ciberseguridad, esa capacidad de nos tiene que permitir proteger los sistemas, detectar, reaccionar y recuperar los sistemas frente a los ciberataques. La segunda línea se centra en las administraciones públicas, en la necesidad de proteger todos los sistemas, especialmente de manera muy concreta aquellos que manejan información clasificada. La tercera se centra en la importancia de las infraestructuras críticas. La cuarta, cómo no, se centra en la importancia del ciberdelito y el ciberterrorismo. La quinta se refiere al sector privado, y le dice: Sector privado, ustedes tienen que invertir entre ciberseguridad, ustedes son víctimas, por supuesto igual que la Administración, que también tiene que invertir en ciberseguridad. La sexta incide en aumentar la capacitación del ciudadano, aumentar las titulaciones y aumentar la inversión en investigación y desarrollo. La séptima, probablemente la más transversal de todas, indica la necesidad imperiosa de aumentar el nivel de ciberseguridad o la cultura de la ciberseguridad de los ciudadanos. Por último, la octava se refiere

cve: DSCG-12-CM-67

al compromiso internacional, tanto a la colaboración en organizaciones multinacionales —concretamente se refiere a la Unión Europea y la OTAN— como en los convenios bilaterales. ¿Por qué? Porque la cooperación es absolutamente fundamental para que entre todos seamos más resistentes a las ciberamenazas. Sus señorías saben que la estructura del sistema de Seguridad Nacional está comandada por el consejo. El consejo tiene varios comités especializados, y uno de ellos es el Consejo Nacional de Ciberseguridad, que tiene esa composición: presidente, dos vicepresidentes y once vocales. Tengo el honor de ser vocal del ministerio de Defensa ante el consejo. La segunda responsabilidad importante del Consejo Nacional de Ciberseguridad es velar por que la estrategia se lleve a la práctica, y se lleve a la práctica correctamente.

Después de haber revisado la estrategia creo que es conveniente tener un listado de quiénes son los actores importantes a nivel nacional cuando hablamos de ciberseguridad: Departamento de Seguridad Nacional, Centro Nacional de Inteligencia, Ministerio de Defensa, Ministerio del Interior y Ministerio de Energía, Turismo y Agenda Digital. Para hacer frente a las necesidades que se encuentra el Ministerio de Defensa el 19 de febrero de 2013 se firmó la creación del Mando Conjunto de Ciberdefensa. Fue la solución que se adoptó para hacer frente a esas necesidades. Es una unidad conjunta ubicada en el Estado Mayor de la Defensa, compuesta por tanto por personal que proviene de los Ejércitos y de la Armada. Alcanzó su capacidad operativa inicial en septiembre de 2013, o sea, hace escasamente cuatro años, y sí me gustaría decir en este punto —porque he tenido la suerte de vivir esos cuatro años en la unidad— que en los comienzos hemos recibido siempre una ayuda muy valiosa por parte de nuestros compañeros en la Administración, que eran más antiguos en cuanto a experiencia, tanto del Centro Criptológico Nacional como del Incibe como del Ministerio del Interior, en su faceta Guardia Civil, Policía Nacional y también Cnpic. Todos estaban ya operativos cuando nosotros nacimos, y todos nos han ayudado a progresar más rápidamente de lo que lo hubiéramos hecho sin su ayuda.

¿Qué misión tenemos? Se recoge en un real decreto. Nuestra misión es el planeamiento de ejecución de las acciones relativas a la ciberdefensa —importante— en las redes y sistemas de información y telecomunicaciones del ministerio. Esa es la primera parte de nuestra misión. Y, ¿por qué es la primera parte de nuestra misión? Pues porque las Fuerzas Armadas occidentales son tremendamente ciberdependientes, más incluso que la sociedad a la que pertenecemos. Los sistemas de armas de hoy en día, tremendamente tecnificados, tremendamente eficaces, basan su funcionamiento en que están interconectados. Sin esa interconexión que se logra a través del ciberespacio retrocedemos muchos años. La segunda parte de nuestra misión es planear y ejecutar también tareas defensivas en otros sistemas que pudiéramos tener encomendados. ¿Y qué es eso? De manera genérica apoyar a todos los otros actores que hemos comentado antes; probablemente más focalizado en lo que podría ser el apoyo en infraestructuras críticas; pero, bueno, es una posibilidad que queda abierta. Otra parte de nuestra misión es contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional. Después lo veremos un poquito más detallado.

Como jefe de la unidad tengo tres dependencias que tienen su significado; en primer lugar, orgánica y operativamente del Jemad, y eso tiene el significado de que, desde la creación de la unidad, se le ha colocado en la estructura orgánica tremendamente arriba, justo al lado del mando operativo de las Fuerzas Armadas. Tengo una dependencia operativa del comandante del mando de operaciones, actuando —como comentaré más tarde— como quinto mando componente, siempre y cuando nos incluyan en algunos de sus planes operativos. De esto se deduce que el Ministerio de Defensa, desde el primer momento, ha tratado de implicar la ciberdefensa con el resto de las operaciones. No podemos ir unos por un lado y otros por otro; todo está mezclado y así debe de ser. Y por último, hay una dependencia funcional del secretario de Estado de Defensa, que es la autoridad de seguridad de la información en el ministerio; y nosotros tenemos una responsabilidad sobre lo que es la seguridad de la información dentro de los sistemas de información.

Sobre la fuerza conjunta quiero comentarles que tenemos una misión permanente; la misión permanente de defender el ciberespacio, responsabilidad del ministerio obviamente. Ahí nos ceñimos; ese es el alcance de nuestra misión permanente. Y dentro de lo que es la estructura de la fuerza conjunta, donde hay un diseño modular de núcleos de fuerza, estamos en el núcleo de fuerza conjunta número uno, que son precisamente aquellos que tienen misión permanente. Esta es la estructura de la fuerza conjunta en su configuración más demandante. Es bastante revelador que exista un mando componente del ciberespacio; o sea, se lleva al último extremo el hecho de que hay que implicarlo en las operaciones y que también hay un nuevo dominio.

cve: DSCG-12-CM-67

¿Qué cometidos tenemos? Quiero precisarles que cuando hablamos de ciberdefensa lo que hacemos es centralizar la dirección, pero tratamos de distribuir la ejecución, para que esta ingente tarea la podamos hacer entre todos. En ese sentido los Ejércitos y la Armada hacen la ejecución de la defensa de sus sistemas, y sobre todo de sus sistemas de armas. Ese esfuerzo se dirige desde el mando conjunto, que también tiene algunas responsabilidades en cuanto a ejecución de defensa en otros aspectos. Somos los responsables de ejercer esa reacción en el ciberespacio, siempre y cuando se cumplan tres condiciones, y es que debe ser de forma oportuna, legítima y proporcionada. Y, por último, pero tremendamente importante, tenemos el cometido de definir, dirigir y coordinar concienciación, formación y adiestramiento. Me detengo brevemente en la importancia de la concienciación. Es probablemente la tarea más eficiente que hacemos porque requiere muy poca inversión y las consecuencias son tremendamente beneficiosas. Un usuario, de cualquier sistema, que esté concienciado de la importancia de lo que está haciendo, de que las ciberamenazas existen, se convierte en la primera línea de defensa del sistema. Es el primer filtro. Sin embargo, un usuario que no está concienciado es el elemento más peligroso del sistema y, si me permiten, solo hay que educarle adecuadamente.

Cuando hablamos de ciberdefensa hablamos de tres capacidades operativas: la defensa en sus modalidades de prevención, de proactividad y de reactividad, en caso de que suceda algo; la explotación, que nos proporciona una cierta alerta temprana, un conocimiento de la situación en general y una inteligencia pero solo a nivel táctico; no somos una agencia de inteligencia, somos una fuerza combatiente en el ciberespacio, que, obviamente, necesita una inteligencia táctica para poder operar. Y, en caso de que fuese necesario, una respuesta siempre y cuando se cumplan las condiciones que comentábamos anteriormente.

Cuando hablamos de cooperación es absolutamente esencial —como he dicho antes y siguiendo una idea de círculos concéntricos—, primero, dentro del ministerio, los ejércitos, mando de operaciones, el Cifas, la Dirección General de Armamento y Material. A continuación, la Administración, tenemos a CCN, Incibe, Policía, Guardia Civil, al Departamento de Seguridad Nacional. Tenemos dos colaboraciones tremendamente importantes, una es con las empresas especializadas en ciberseguridad. Podemos aportar experiencia operativa que, junto con su dedicación, nos puede permitir lograr productos tremendamente interesantes. Segunda, las universidades, de un extraordinario valor cuando hablamos de ciberseguridad; fundamentalmente con dos finalidades, una, la más tradicional, que es la de enseñanza —cómo no—, y otra también muy eficiente que es la de investigación y desarrollo. Piensen que en ciberseguridad lo fundamental son las cabezas, el talento del personal que está detrás de su terminal informático. Aquí no hacen falta grandes infraestructuras para producir barcos ni aviones, no, es muy barato y la universidad tiene, por tanto, una tremenda capacidad para hacer I+D. Por último, la cooperación internacional, la OTAN, tanto el Centro de Excelencia de Ciberdefensa en Estonia como los distintos comités de la OTAN, la Unión Europea, fundamentalmente la Agencia Europea de Defensa, y luego aliados a nivel bilateral con los que en muchos casos tenemos relación.

A modo de resumen —y con esto termino, señor presidente—, no quiero dejar de repasar lo que en mi unidad llamamos el heptálogo, que no decálogo; son solo siete puntos que tratamos de tener siempre en mente. Son siete puntos muy sencillos pero que conviene no olvidar nunca. Todos son bastante radicales pero es que así son más claros. Cualquier sistema TIC puede ser ciberatacado. No le den más vueltas, cualquiera. No estoy diciendo que sea fácil, claro que no, pero es posible. Permítanme darles una cierta esperanza porque cualquier sistema puede ser ciberdefendido, y tampoco hay que olvidarlo. Esa es una realidad. Cuando comento estos dos conceptos tengo que recordar que en muchas ocasiones me he encontrado personas que se debaten entre dos estados que son malos, se debaten entre la incredulidad: esto de las ciberamenazas, ¿realmente hasta qué punto será verdad? Ese es uno de los estados. Otro es la resignación: si te toca, no tiene remedio. Los dos son erróneos, lo que hay que hacer es actuar adecuadamente. Esta no es una tarea imposible, es una tarea de método, es una tarea de persistencia, pero es algo que tiene solución y, por supuesto, para encontrarla hay que tener fe en ella.

Un aspecto eminentemente táctico pero muy útil para todos, creo yo, es que si alguien quiere atacar un sistema tiene que cubrir dos fases, indefectiblemente: primero tiene que llegar al sistema víctima y luego tiene que actuar sobre él; no se puede actuar si no ha llegado a él. Parece una perogrullada pero no lo es. En relación con eso, la primera y mejor protección para un sistema es el aislamiento, y realmente es tremendamente útil, pero tampoco podemos confiarnos en que esa sea la panacea universal. Evidentemente es algo que hay que hacer, pero teniendo además una serie de procedimientos y medidas preventivas porque también el aislamiento se puede superar o evitar.

cve: DSCG-12-CM-67

Otro aspecto que he comentado previamente de otra forma es que en cualquier sistema de información el factor humano es el eslabón más débil, sin ninguna duda. ¿Cómo se resuelve eso? Con concienciación, lo que comentaba anteriormente. Algo ya he dicho al respecto de que, en comparación con los otros dominios, no hay distancia en el ciberespacio porque tanto la distancia como el tiempo realmente están comprimidos. Y, por último —ya lo he comentado—, es muy difícil, con frecuencia imposible, determinar quién es el responsable de un ciberataque; les diría más, es prácticamente imposible demostrarlo. Podemos unir una serie de evidencias y decir: esto es de aquí, esto es de allá, pero demostrarlo es extraordinariamente complicado y, en la mayor parte de los casos, imposible de hacer.

Señor presidente, muchas gracias.

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

Iniciamos el turno de intervenciones. Les ruego que se ciñan a los cinco minutos que tienen atribuidos.

Señor Salvador.

El señor **SALVADOR GARCÍA:** En primer lugar, quiero darle la bienvenida a la Comisión. Aunque nosotros estamos aquí para tomar decisiones y para aportar ideas para toda España, me siento orgulloso de que usted también sea granadino y a mí, como diputado de Ciudadanos por Granada, me agrada enormemente su comparecencia.

Quiero felicitarle también por haber recibido el premio Isaca 2017 en la categoría de Liderazgo inspirador, porque yo creo que si algo se está viendo en toda su intervención, en la intervención anterior, en otras comparecencias y en lo que está instalado en el conjunto de la sociedad, es que estamos en un momento de cambio y una labor muy importante es la concienciación. En este momento creo que ustedes están haciendo una labor muy importante de concienciación también en el propio ejército; si el ejército no es consciente de las amenazas y de la necesidad de protección y de cómo poder actuar, difícilmente en la planificación para sus presupuestos podrá contemplar la importancia y la necesidad de todo esto. Eso lo podríamos extrapolar a todos los ámbitos, también el de las empresas, para que sepan cómo se tienen que proteger ya que están en un mundo donde se multiplican las oportunidades. Por tanto, en relación con lo que ha dicho un compareciente de que se puede intentar aparentar que se criminaliza la red, todo lo contrario; yo he comparado en ocasiones esto con la gran calzada romana o con las cartas de navegación, que sirvieron para desarrollar la humanidad, pero, al mismo tiempo, eso no quitaba que hubiera asaltantes y piratas y que hubiera que tomar medidas. Aquí creo que estamos ante la misma teoría, tenemos que tomar medidas precisamente para que las oportunidades prevalezcan y los malos no terminen dándonos problemas a la gente que nos portamos de forma adecuada.

He visto durante su intervención y también en la intervención de la compareciente anterior que a alguien le sorprendía la palabra guerra. Yo quiero poner de manifiesto —y que incluso usted mismo nos lo pueda decir— que cuando hablamos de que un país está en guerra con otro es una concepción y que si estamos hablando de ciberguerra, de la prevención de la guerra, de guerra híbrida, etcétera, estamos hablando de conceptos en los que parece que no llega la sangre al río, independientemente de que hay aspectos absolutamente importantes para garantizar la seguridad de un país y de que si no se ponen en marcha las prevenciones necesarias, los efectos que se deriven puedan ser absolutamente demoledores.

He visto muchas de las frases que usted ha ido diciendo en conferencias y en distintos ámbitos porque lo he investigado y me parece que es un apóstol imprescindible de toda esta causa. Le voy a preguntar por dos o tres cuestiones. En primer lugar, ustedes surgen en el año 2013 con este nuevo cometido y le quisiera preguntar si desde el momento en que se diseñó como estrategia nacional hasta hoy se han cumplido los objetivos que pudieron tener en ese instante inicial de 2013, sabiendo que era algo que iba a tener una constante evolución y, por tanto, también las respuestas se iban a tener que adaptar y los medios se iban a tener que incrementar. Por tanto, si estos objetivos se han ido plasmando en el tiempo. Por otra parte, qué entiende usted que es todavía mejorable. Porque, independientemente de la voluntad, están los presupuestos, está el señor Montoro y está la facultad para llevar a la práctica esa capacidad para defendernos que usted ha definido muy bien como bastante más cara que la capacidad de atacar. Quiero preguntarle asimismo si considera que en este momento en España nuestra capacidad de respuesta es óptima y podemos estar, no digo tranquilos, pero medianamente satisfechos de que todo va por el buen camino.

Ha dado bastante importancia, aunque no se ha extendido en ello y tampoco hacía falta, a la coordinación entre los distintos actores que actúan para la ciberdefensa o ciberseguridad. Aquí pondría Ejército, Fuerzas y Cuerpos de Seguridad del Estado, el Incibe más el resto de administraciones,

cve: DSCG-12-CM-67

empresas, sociedad civil, las relaciones también con el ámbito internacional, el Poder Legislativo, para adaptar las normas, y también el Poder Ejecutivo, para tener la formación y la capacitación adecuada para ejecutarlas. Decía la compareciente anterior que se puede planificar durante mucho tiempo, se actúa muy rápido. Se ha referido a la falsa bandera y la dificultad que tiene encontrar culpables, pero mientras sea muy fácil atacar y el beneficio pueda ser muy grande, los riesgos sean bastante pequeños y no se vea que hay condenas y que quien la hace, la paga, evidentemente será un acicate para dedicarse a esa profesión de ciberdelincuente porque, además, no deja muertos y no hay violencia física, aunque sí puede arruinar la vida de personas, de entidades o incluso, como hemos comentado, de países.

En relación con todos esos actores, quería preguntarle si usted considera que la adaptación a las respuestas que tenemos que dar en todos ellos va acompasada o si hay unos que están más evolucionados que otros. Lo resumiría en si todos estos organismos y actores tienen el reloj en hora y acometen la amenaza desde la misma perspectiva y sincronizadamente o si cada uno está haciendo la guerra por su cuenta y vamos a salto de mata. Estaré atento a sus respuestas para hacer la segunda intervención.

Muchas gracias.

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

Señor Comorera.

El señor **COMORERA ESTALLERAS:** Muchas gracias, presidente. Muchas gracias, general, por su comparecencia y sus explicaciones. Voy a entrar directamente a hacerle preguntas porque me interesa mucho más lo que nos pueda explicar usted que lo que pueda argumentar yo en este aspecto.

Me gustaría saber qué opinión le merece la reciente normativa NIS en el marco de la defensa nacional. ¿Considera que dicha normativa impulsa la cooperación internacional en la lucha contra el crimen y el ciberterrorismo?

Por otro lado, el CNI, gracias a los expertos del Centro Criptológico Nacional, en un informe que apareció esta misma semana nos informaba de que contabilizaron setenta ataques de *hackers* contra páginas de internet de las administraciones públicas y del Gobierno central en los días en torno a la aprobación del artículo 155. El Centro Criptológico Nacional informó de que el año 2017 terminará con una cifra superior a los 26 700 ciberincidentes en el sector público y empresas estratégicas españolas, es decir, un 26 % más que lo ocurrido en 2016. De ellos, alrededor de 1200 eran considerados muy altos o críticos, lo que, haciendo números, supone gestionar 3,7 ciberincidentes con un nivel de impacto muy alto o crítico. Me gustaría que explicara qué papel desempeña el Mando Conjunto de Ciberdefensa en la defensa y protección ante este tipo de ciberincidentes.

También me interesaría que nos diera su opinión sobre de qué manera considera que se debe abordar, desde el punto de vista de la defensa nacional, la creciente expansión de lo que se llama el Internet de las cosas, y ello en relación con lo que usted ha calificado como aislamiento como mejor medida. Precisamente ayer leía un informe que destacaba que la inteligencia artificial abre nuevas posibilidades al cibercrimen, señalando que las infraestructuras críticas están en el punto de mira y que va a ser una prioridad en el próximo año 2018. Me gustaría saber cuál es su opinión al respecto.

Ahora me centraré en la cuestión del presupuesto. Según dijo recientemente Enrique Cubeiro, jefe de operaciones del Mando Conjunto de Ciberdefensa, se invierte más en vallas que en ciberseguridad y preguntaba de dónde creen que vendrá el próximo ataque, ¿de la valla o de un *fireware?* Me gustaría que nos diera su opinión al respecto sobre si el presupuesto que actualmente se está dedicando a la ciberdefensa nos llega o no para las dificultades que los expertos nos dicen que vamos a tener en el próximo año con ataques a infraestructuras críticas.

Muchas gracias.

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

Señor Raffo.

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

Me quería sumar al agradecimiento tanto a la señora Milosevich, por su enfoque analítico como profesional en el conocimiento de un aspecto relacionado con esta materia, y también, por supuesto, al general López de Medina por su presencia. A ambos. Creo que ilustran a los que somos representantes de la ciudadanía para poder llevar a cabo el proceso de toma de decisiones, porque no deja de ser esto. Tenemos que ser conscientes de que es nuestra responsabilidad individual, y después colectiva en cada

cve: DSCG-12-CM-67

grupo político, saber discriminar la información que podamos o no compartir o valorar según la procedencia, etcétera y otra es tenerla en consideración y valorarla en sus justos términos.

A mí me correspondía comentar lo relativo a la comparecencia del general López de Medina y creo que, como dijimos en la anterior comparecencia, es difícil abstraerse o sustraerse —depende de cómo se quiera ver— a los recientes acontecimientos que hemos ido sufriendo en España igual que en otros países occidentales. Esto de los hombrecitos verdes que aparecieron en la frontera de Crimea y de Ucrania no vinieron del espacio; no tenían ni logos ni símbolos, ni ellos ni el armamento pesado ni las tanquetas ni los tanques, pero todo el mundo sabía quién estaba detrás. Creo que no hubo ninguna duda. Yo no voy a entrar en las razones que pueda tener cada Estado en defender sus intereses o por cercanía su propio hábitat de círculo de defensa o de seguridad o su círculo saludable para sus propios intereses, pero algo parecido es lo que está ocurriendo. Hay una unidad destacada en el Báltico, en la que participa España, en este caso del Ejército del Aire —no sé si eran Eurofighter— y conjuntamente con la OTAN están desarrollando una tarea que es propia, en mi opinión, no tanto de la guerra como de una nueva guerra fría fruto de una serie de acontecimientos que han pasado. Esto no es distinto a la tensión que pueda estar ocurriendo en el Cáucaso o en Oriente Medio, porque es geopolítica, es geoestrategia dentro del enfoque de la defensa y la seguridad de un país.

Nosotros consideramos por los informes, las comparecencias y las lecturas que hemos llevado a cabo, que mientras que España está implicada en el equipo especializado en la estrategia de comunicación del Este —creo que España tiene ahí una incorporación—, sin embargo, a lo relativo a la presencia en el Centro de Excelencia de Comunicación de la OTAN no tiene una participación tan directa. Si no es así, usted nos corrige. El ministro de Asuntos Exteriores tuvo recientemente un encuentro con sus homólogos a nivel europeo en el que planteó las circunstancias que habían ocurrido y, lógicamente, coincidiendo con los responsables de otros países de la Unión Europea, ofreció una mayor implicación y colaboración del Estado español. Nos gustaría que nos ilustrara un poco sobre cuáles son exactamente estas circunstancias y la situación real en la que estamos, que no significa que no estemos conectados con la OTAN en las medidas y en las acciones que toman sino que significa más implicación por un motivo fundamental, porque este centro de la OTAN —que también se dedica a comunicación estratégica y a asuntos relacionados con la información que circula a través del ciberespacio y sobre las redes— no tiene ningún medio de comunicación potente. Tenemos un idioma con el que tenemos muy poca capacidad de penetración y sin embargo lo entienden millones de personas, es la segunda lengua a nivel mundial, y —como digo— no tenemos ningún medio de comunicación potente, de los clásicos y los habituales, no tenemos un canal de televisión internacional con gran capacidad de penetración pero tampoco tenemos influencia a través de las redes, como está ocurriendo por ejemplo con RT, las redes sociales y la organización y la planificación que hay en este asunto de la desinformación. En Latinoamérica nuestra presencia en ese sentido es muy importante, RT se ve allí muchísimo, tiene una gran capacidad de penetración allí, y las redes sociales conectadas a través del Facebook y Twitter también. Por supuesto, no hace falta que digamos que también en España hay poca gente que ve RT. Yo, por suerte por desgracia, la sigo desde hace ya unos años e identifico una estrategia clara de comunicación, como legítimamente pueden tener otros países. En este sentido, la propuesta iría encaminada a que nos ilustrara sobre la necesidad de reforzar ese papel de los intereses del Estado español, instrumentalizando también nuestra propia lengua para señalar con criterios de veracidad aquella información que circula que es falsa o es una realidad que después se manipula.

Finalmente quiero hacer una pregunta más relacionada con la intervención que están haciendo las Fuerzas Armadas en el Mar Báltico, quisiera saber si ha habido eventos o acontecimientos de contramedidas en temas de telecomunicaciones —lo que se denomina guerra electrónica— o intentos de sabotaje o de incorporarse a los sistemas de información del aparato o de las unidades que trabajan en el Mar Báltico por parte de las Fuerzas Armadas rusas.

El señor **PRESIDENTE:** Muchas gracias, señor Raffo.
Termina el turno de intervenciones el señor Cosidó.

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

Quiero darle la bienvenida al general López de Medina, no como una fórmula de cortesía parlamentaria. Hasta hace poco tiempo, los únicos uniformados que veíamos en el Congreso de los Diputados eran los jefes del Estado Mayor cuando venían a explicarnos el presupuesto. Y, como es algo relativamente excepcional que tengamos uniformados —no en esta Comisión sino en el conjunto del Congreso—, quiero

cve: DSCG-12-CM-67

expresarle el enorme orgullo que sentimos como españoles y como representantes de los ciudadanos por nuestras Fuerzas Armadas, que con intervenciones como las suyas acreditan una vez más su profesionalidad y su competencia, además de transmitirnos seguridad y tranquilidad.

Quiero además que transmita la felicitación de mi grupo porque ustedes nacen el 19 febrero de 2013 y han trabajado mucho y bien. Creo que las Fuerzas Armadas de España —usted me desmentirá si no es verdad—, en el marco de la Unión Europea y de la Alianza Atlántica, están en el pelotón de cabeza en lo que a ciberdefensa se refiere, aunque no vamos a ponernos más medallas de las necesarias. Y eso, en buena parte, con unos recursos muy limitados, en los que no vamos a entrar porque somos el grupo que apoya al Gobierno, me parece que tiene mucho mérito para usted como mando y también para todo el equipo que usted dirige, por lo que quisiera que les hiciera llegar nuestra felicitación.

Creo que usted debería tener cuatro estrellas, no porque usted las merezca, que todo llegará, no se trata de una cuestión personal. De los cinco componentes que tiene en estos momentos nuestra defensa me parece que probablemente el más prioritario en este momento debería ser la ciberdefensa. Las dos estrellas que usted luce como general de división ponen de manifiesto o vienen a simbolizar que todavía no hemos desarrollado una capacidad de ciberdefensa que esté a la altura de la que tenemos en el ámbito del Aire, de la Armada o del Ejército de Tierra. Quizás sea más equiparable a la que desarrollamos en el ámbito del espacio, en el caso de España. Pero quiero decirle que para nosotros esta es una prioridad para el Ministerio de Defensa y el grupo parlamentario lo apoyará al cien por cien. Estoy seguro, sin adelantar nada, que las conclusiones de esta Comisión remarcarán la importancia, la prioridad que debe tener este componente de nuestra política de defensa.

Como esta sesión es pública y además se publica, a lo mejor le hago alguna pregunta que no puede contestar. Soy plenamente consciente y no me lo tomo como que usted no sepa ni mucho menos aún como una descortesía. Conteste usted a lo que le parezca y lo que crea que es inoportuno contestar no lo conteste. En el caso del Mando de Ciberdefensa, me atrevo a sugerir a la Presidencia, previa felicitación por lo que he dicho de haber traído a este compareciente, que este es uno de los centros que por su especial naturaleza sería oportuno visitar, si es posible, en algún momento posterior.

Me gustaría, general, si pudiera, que fuese un poco más explícito en la definición de las amenazas. A mero título de ejemplo, porque todas las comparaciones son odiosas, tengo aquí el Worldwide Threat Assessment of the US Intelligence Community y son muy claros. Las amenazas en materia de ciberamenazas: Rusia, China, Irán, Corea del Norte y algún otro país. Es bueno que sepamos a qué nos enfrentamos y que definamos con claridad cuáles son nuestras amenazas. Probablemente, no le corresponde a usted hacer un *assessment* de estas características, pero podría ser útil que tuviéramos una definición de las amenazas que vaya más allá de decir que hay actores nacionales, grupos de crimen organizado o grupos terroristas. ¿Exactamente nos puede relatar qué nivel de amenaza tenemos, es decir, qué casos concretos de ataques se están produciendo a nuestros sistemas de información, de comunicaciones de las Fuerzas Armadas? Como usted dice, esto no se puede probar, pero ¿de dónde creemos, en base a nuestras propias fuentes, que esos ataques pueden venir?

Segunda cuestión. Todos hemos coincidido en que hay un déficit de regulación internacional en el ámbito de la Unión Europea y en el ámbito global. Este déficit es especialmente dramático o crítico en lo que se refiere a la ciberguerra. Paradójicamente, es como si hubiéramos vuelto a la Edad Media. No hay norma alguna sobre cómo hacer la ciberguerra. No sé si nos puede dar alguna indicación sobre al menos nuestras reglas de enfrentamiento, es decir, qué puede hacer y qué no en base a las reglas de enfrentamiento que manejamos en el ámbito de la ciberguerra.

Dice que tenemos una excelente estrategia de ciberseguridad. Esta es una percepción que a lo mejor me desmiente radicalmente, pero usted lo dice muy bien: no hay ningún sistema que sea invulnerable. Le digo más, se está poniendo en evidencia que somos muy vulnerables. Me da la impresión de que una buena parte del esfuerzo que realizamos, también en el ámbito de la defensa, es una defensa muy pasiva, un intento de blindar nuestros sistemas. Me planteo si no sería necesario hacer una revisión. Por deformación de anteriores responsabilidades, en la lucha contra el terrorismo, por ejemplo, poner bolardos es muy importante, pero es más importante todavía ser capaz de anticiparse a las acciones terroristas y desmantelar las células que están operando. El futuro debería ir por ahí, sin perjuicio de que —insisto— tengamos que tomar todas las medidas necesarias para garantizar unos dispositivos que sean realmente seguros.

Estructura. La estrategia de ciberseguridad es muy importante porque aquí tenemos una multiplicidad de actores que es necesario coordinar. Usted ha insistido mucho en su exposición en la necesidad de

cve: DSCG-12-CM-67

coordinar. Con todo el respeto, pero a veces esto de la ciberseguridad me recuerda al fútbol alevín. Tiene sentido porque la estrategia es de 2013, es decir, tiene cuatro años.

Los que hemos tenido el privilegio de ver a nuestros hijos jugar al fútbol con seis o siete años nos hemos dado cuenta de que allí donde está el balón está todo el equipo, independientemente de cuál sea la posición que debería ocupar en el campo. Aquí nos pasa un poco igual, es decir, que cuando tenemos un ataque de desinformación todos nos ponemos detrás de esa pelota cuando en realidad el campo tendría que estar más compartimentalizado. Yo creo que usted es afortunado porque es de los que más clara y delimitada tiene su misión, pero aun así usted tiene también dentro de la Secretaría de Estado de Seguridad un centro de telecomunicación e información. Usted ha mencionado los cuarteles generales. No le pido que se moje porque esto de los organigramas es un debate siempre complicado, pero ¿tenemos demasiados actores en el campo de la ciberseguridad? ¿Sería bueno ir a una convergencia de actores, no solamente en el ámbito de una gran agencia de ciberseguridad, sino en el ámbito del Ministerio de Defensa, centralizando más la misión? ¿O es mejor optar por un modelo, como he intuido que usted ha defendido, de centralidad en la dirección pero descentralidad en las operaciones y en los ejecutores de esas directrices?

No lo ha mencionado usted, pero da la impresión de que el elemento central de nuestra estrategia de seguridad nacional, que es la disuasión, en este ámbito no funciona mucho. Yo creo que es un ámbito en el que es especialmente complicado hacer ciberdisuasión. No sé si usted tiene alguna idea de cómo podemos ciberdisuadir a quienes nos atacan.

Termino ya rapidísimamente, presidente, que me temo que me he extendido más de los cinco minutos. Usted ha hablado de que el factor humano es fundamental, y no puede haber más coincidencia. Me gustaría saber cómo seleccionan y cómo retienen, porque, como bien decía la anterior compareciente, ella recomienda a su hijo que estudie ciberseguridad porque esto tiene mucho futuro y me temo que la demanda va a ser tremenda, de forma que las personas más capacitadas del sector público van a tener que resistir tentaciones muy importantes de ofertas del sector privado. ¿Cómo garantizamos esa seguridad del factor humano, que yo coincido al cien por cien en que es lo critico? Ustedes tienen militares —probablemente ser militar es un plus de confianza—, pero tienen también civiles. No sé si su idea es ir a civilizar más el mando —en el sentido de incorporar más civiles, que civilizado está— o mantener más un *core* uniformado, como precisamente un plus, no infalible en ningún caso, pero un plus de garantía frente a posibles vulnerabilidades. Yo soy muy entusiasta de la reserva y está la idea de los ciberreservistas. Le adelanto que me gusta la idea, pero no sé si desde el punto de vista operativo cree que puede tener utilidad y operatividad.

Termino hablando de capacidades tecnológicas. ¿Tenemos cierta autonomía en el ámbito de nuestro sector industrial de ciberseguridad o somos muy dependientes del exterior? ¿Qué hacen ustedes en I+D+i como mandos? ¿O esto lo hace la Secretaría de Estado? ¿Nos puede poner algún ejemplo de proyectos que en estos momentos estén creando una potente industria de ciberseguridad, que además sería un valor muy competitivo para nuestro país?

Ya son las dos y media, pero nos gustaría que pudiera hablarnos un poco del futuro. Es decir, vamos a un mundo de inteligencia artificial, Internet de las cosas, nueva generación de semiconductores, y en general el gap que hasta ahora Occidente había mantenido en términos tecnológicos, de manera muy particular Estados Unidos, parece que se cierra, es decir, que tenemos potencias con menos recursos aparentemente, con menos tecnologías, pero que son enormemente competitivas en términos de poder desarrollar ciberguerra o ciberataques. ¿Cómo vamos a ser capaces de gestionar este nuevo mundo?

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

Yo voy a pedirle al general que haga uso del laconismo militar que le es propio porque, como usted ha recordado, son las dos y media y corremos el riesgo de que pase aquí lo que en aquella conferencia, que el conferenciante dijo: los que vayan a abandonar la sala que lo hagan en silencio para no despertar a los que se han quedado. **(Risas).**

El señor **GENERAL DE DIVISIÓN, JEFE DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD** (Gómez López de Medina): Gracias.

Señor Salvador, la situación de guerra, como creo que sus señorías conocen, requiere de una declaración formal, o sea, es un estado desde el punto de vista del derecho internacional. Es difícil llegar al estado de guerra; puede haber mucha actividad, estar en una situación de conflicto o de crisis. Es decir, todo eso es gris; entre la paz y la guerra hay muchos valores intermedios. Hablar de guerra en los términos

cve: DSCG-12-CM-67

en que hemos hablado aquí es por ser un poco más expresivos, pero en ningún caso hay que dramatizarlo. Yo creo que deberíamos poder hablar con total libertad y con total naturalidad utilizando ese término como cualquier otro.

¿Se han cumplido las previsiones que tuvimos al principio? Sí, la verdad es que sí. Sí en cuanto a posibilidad de crecimiento, pero nos ha sorprendido la velocidad que ha adquirido esto; es decir, la dirección que ha seguido no, pero la velocidad sí.

En cuanto a los presupuestos, hasta ahora me han dado los fondos que he pedido, no puedo ser más lacónico, pero lo que viene a continuación, por el motivo que he dicho antes, va teniendo otra dimensión. Es decir, este es un movimiento uniformemente acelerado, donde la velocidad va aumentando, y por tanto hacen falta más recursos con ese factor de aceleración.

La coordinación va bien, pero es un término que obviamente siempre se puede mejorar; de hecho, hay mucho esfuerzo en ese sentido, nos vemos con mucha frecuencia. Esos cinco actores que he comentado antes nos conocemos por nuestros nombres y nos relacionamos habitualmente, coincidimos en muchos eventos y eso obviamente facilita mucho las cosas porque el factor humano cuenta mucho, que tengas una conexión, una empatía fácil con el resto de actores facilita mucho las labores, es así realmente. Pero hay que hacer más, hay que automatizarlo más para que esa velocidad de coordinación real aumente, pero en ello estamos.

Paso a referirme al señor Comorera. La Directiva NIS aporta algo que era muy necesario. Cuando nos referimos a operadores de servicios esenciales y proveedores de servicios digitales, que son los dos mundos, la verdad es que en la Unión Europea había una discontinuidad muy grande, cada Estado se comportaba de una manera determinada. En España teníamos y tenemos una buena infraestructura en ese sentido, con una ley de infraestructuras crítica, concretamente la Ley 8/2011, pero no en todos los Estados era igual. La Unión Europea fue consciente de eso, porque esa discontinuidad era un problema a la hora de lo que pretende la Unión Europea, que sea lo mismo vivir en Holanda que vivir en Italia a todos los efectos, para los ciudadanos, para las empresas, para el capital, para todo. Esas discontinuidades eran muy problemáticas pues la normativa era diferente. Y si hablamos de empresas que eran «multinacionales» —entre comillas— dentro de la Unión Europea, tenían instalaciones en España y en otra nación donde la normativa no era igual, los problemas eran evidentes, independientemente de que lo que se pretendía era establecer unos mínimos en cuanto a la protección de esos servicios. ¿Para qué? Obviamente para proteger, en primer lugar, a los ciudadanos; esa es la idea de la Directiva NIS.

¿Qué papel tenemos en la defensa de los ciberincidentes? Esa es nuestra primera misión, defendernos de esos ataques, pero no podemos olvidar en ningún momento cuál es el ámbito de actuación, que es lo que decía antes. Nosotros no defendemos España, contribuimos a. Pero nuestra primera misión es defender nuestros propios recursos y ese es el planteamiento.

En cuanto al Internet de las cosas, el impacto es grande porque aumenta el número de usuarios de Internet, aunque sea una cosa realmente, pero el número es enorme, y al ser enorme, si no se tienen en cuenta criterios de ciberseguridad en esas cosas, comienzan los problemas; se puede *hackear* de forma masiva —es fácil hacerlo—, incluso convertir esos elementos a su vez en robots para que hagan algo; no tiene que ser muy complicado, pero como son millones de acciones simultáneamente el efecto sobre el sistema víctima es normalmente de denegación de servicio.

Le doy las gracias por preguntarme sobre infraestructuras críticas. Hasta hace nada nos preguntábamos quién estaría interesado en atacar una infraestructura crítica, por ejemplo en dejarnos sin energía eléctrica. ¿Un grupo terrorista? Supongámoslo, porque indudablemente le iba a dar notoriedad, que es lo que se pretende. ¿Un Estado con el fin de hacernos daño desde un punto de vista estratégico? Y casi te quedabas ahí, pero desde hace un tiempo hemos visto que hay un tercer actor, que es simplemente un delincuente organizado que, mediante una acción de *ransomware*, te puede bloquear una infraestructura crítica y a continuación pedirte un rescate por ello. Que yo sepa, la primera infraestructura que sufrió ese efecto fue el metro de San Francisco; puedo estar equivocado, pero me llamó mucho la atención porque llegué a esa conclusión: ya hay más gente interesada en actuar sobre una infraestructura crítica, para pedir dinero a cambio. Esa es una novedad que hace que esta actividad, debido a la vulnerabilidad o al interés de actores para actuar sobre infraestructuras críticas, aumente de manera muy importante.

Quique Cubeiro es mi jefe de operaciones. **(Risas).** Hay que gastar más dinero en ciberseguridad, es cierto. Quique es un magnífico conferenciante y además un señor muy gracioso y muy agudo, y me lo imagino poniendo ese ejemplo. Hay que gastar más dinero en ciberseguridad y sobre todo el sector

cve: DSCG-12-CM-67

privado. Es cierto que las medianas y pequeñas empresas tienen pocos recursos para dedicarlos a ciberseguridad, pero son víctimas muy fáciles de ese tipo de acciones.

Senador Raffo, participamos en el Centro de Excelencia de Ciberdefensa de Estonia. No sé si se refería a él. Es de una serie de naciones, como todos los centros de excelencia…

El señor **RAFFO CAMARILLO:** Me refería al que depende del Servicio de Acción Exterior de la Unión Europea. Hay dos. En uno estamos implicados directamente —hay una relación de países— y hay otro, que yo creía que era este, pero entonces me refiero al East Stratcom Task Force.

El señor **PRESIDENTE:** Ese es de la Unión Europea.

El señor **RAFFO CAMARILLO:** Ese es una unidad que diseña estrategias de comunicación desde la Unión Europea para promover la imagen y la defensa de los valores de la Unión Europea. Parece lógico que estuviésemos ahí, porque se conecta por arriba con los otros.

El señor **GENERAL DE DIVISIÓN, JEFE DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD** (Gómez López de Medina): Sobre ese centro no le puedo decir nada, honradamente, sí sobre el de ciberdefensa en Tallin, en Estonia, donde sí que estamos; de hecho, las dos personas que allí están dependen de mí, y además España es nación fundadora del centro en 2008. La fundamos siete naciones y ya creo que hay veintiuna. Es un centro que está teniendo un éxito tremendo y ahí hemos estado desde siempre. De hecho, desde mi unidad estamos muy vinculados con ellos en muchos sentidos.

Sobre la observación de Russia Today, no sé si he entendido la idea, pero tenemos dos televisiones internacionales. Tenemos el Canal Internacional y el Canal 24 Horas. A nivel de televisión creo que tienen cobertura mundial; yo desde luego las he visto en América y, por supuesto, en Europa. Podrían ser un vehículo para lo que estamos diciendo apuntando a los activos de veracidad, etcétera. Esas dos de entrada.

Sobre los intentos de los rusos en las campañas del Báltico, quiero comentarles para su tranquilidad que nuestra misión es proteger el ciberespacio responsabilidad del ministerio pero con un énfasis especial para los destacamentos que tenemos en el exterior, especialmente para los destacamentos que estén en ese lugar precisamente. Obviamente las amenazas no son las mismas y, aunque no hay distancia ni fronteras en el ciberespacio, las acciones en el ciberespacio son consecuencia de otros hechos y, desde ese punto de vista, estar desplegado al lado de Rusia no es lo mismo que estar en Mali. Cuando uno de nuestros destacamentos va a realizar una de estas misiones, hay un detenido proceso previo, muy riguroso, para confirmar y asegurarnos de que el sistema que se despliega allí está suficientemente protegido, desde el punto de vista teórico y también desde el punto de vista práctico. Se hace una auditoría en el lugar una vez que se han desplegado, aparte de extendernos ampliamente en la concienciación del personal que va allí en todos los aspectos. ¿Ha habido acciones? Hay actividad permanente y en esas zonas es conocido que hay muchas falsas noticias en relación con todo esto, pero no hemos sido víctimas —o si lo hemos sido, no han tenido efecto— de ningún tipo de ataque sobre nuestro personal allí.

Al señor Cosidó le doy muchas gracias por su bienvenida. Para mí también es un tremendo placer estar aquí compareciendo ante ustedes. Nunca había venido con este rol al Congreso de los Diputados. Había tenido la suerte de venir de visita. En la época en que fui ayudante de su majestad el rey tuve varias oportunidades de pasar por el Congreso, pero obviamente no en esta situación. Muchas gracias.

Omito lo de las cuatro estrellas, porque creo que hay cosas que le van a interesar más. **(Risas).** Y, señor presidente, en cuanto a la visita al mando, ni que decir tiene.

Entro en la definición de las amenazas. El problema es que no se pueden demostrar y, como no se pueden demostrar, nadie quiere ponerlo en esos términos. Ni más ni menos. Si se pudiesen demostrar como otras acciones en otras muchas facetas, en otros muchos campos, no habría tanto problema. Se podría decir: Es que es así y además lo demostramos. Pero esa demostración aquí no existe o está tan coja que no soporta el hecho de que se pueda definir. Ese es fundamentalmente el motivo. A continuación preguntaba qué casos de ataques se están produciendo. Para su tranquilidad, todo lo importante está aislado. Lo que no está aislado, no es que no sea importante, sino que no es importante operativamente. Pero obviamente para relacionarnos con los ciudadanos tenemos que tener una parte de nuestra infraestructura visible, que es donde está nuestra página web; no solamente la del ministerio, sino la de los ejércitos o la de las unidades, donde se puede entrar y hacer gestiones. Esa es la parte visible. Además, tenemos una red corporativa enorme, muy grande, donde los usuarios tienen capacidad de

cve: DSCG-12-CM-67

correo, se puede navegar por Internet, etcétera. Esa, obviamente, es la parte más vulnerable. Como es más vulnerable, lo que hacemos es no tener dentro información que sea importante. Esa gran red sí que recibe multitud de incidentes. Vamos a decir incidentes, porque decir ataque deliberado es demasiado decir. Tenemos un poco lo que se reparte por todos sitios. Tenemos *spam* todo el que quiera, tenemos *phishing* todo el que quiera. Todas esas campañas de Hacienda, de los bancos, todo eso nos llega también, y tenemos cosas más selectivas con ese mismo tipo de vector de ataque, a lo mejor más depurado. Lo que sí que quiero darles es el mensaje positivo de que en los tres años de eficacia real que tenemos en este asunto lo que hemos visto —y por eso animo siempre que puedo a todos los organismos— es una mejora debido a la concienciación. Hace tres años el número de archivos adjuntos en una campaña de *phishing* que se clicaban era enorme y ahora no lo es porque la gente ya empieza a escamarse, si me permiten la expresión: Esto no me suena nada, ¿será verdad, será mentira? Y luego, que también es importante, lo utilizan en su vida privada, que también está bien. Por tanto, insisto, la concienciación es fundamental.

¿Qué podemos hacer con las ROE? Defendernos. Es la ROE de siempre: te disparan, contestas. Si alguien entra en mi infraestructura, está en mi casa; esa es una ROE inmediata, para hacer otras cosas hace falta activar otras ROE. Pero sí quiero dejarles el mensaje de que en este dominio o en este ámbito nos movemos o tratamos de movernos igual que los otros. También hacen falta ROE; obviamente, lo inmediato es hacer una traslación de los entornos convencionales. En muchos casos se requieren adaptaciones, pero la mecánica es muy similar.

No solamente protegemos, se hacen más cosas. Lo de proteger transmite una sensación muy estática, efectivamente, pero la defensa que se hace es muy dinámica. Todos los días se cargan los sistemas de defensa con alertas nuevas. Algo muy parecido a lo que hacen en el ordenador de casa cuando actualizan el antivirus, que cargan una serie de archivos de referencia, que es lo que hace el antivirus: comparar con lo que entra y decir si algo es malo o es bueno. Aprovecho para decirles que el mejor antivirus protege poco. No crean que el antivirus es la panacea porque no lo es. Es algo necesario pero no suficiente. Pues hacemos muchas cosas de ese estilo y el sistema de defensa perimetral está permanentemente alertado.

Decía usted que todos detrás de la pelota. Esto de distribuir la ejecución es algo que al principio, sinceramente, no teníamos claro. Había posturas que pensaban que era mejor centralizarlo todo desde el mando. Yo fui abanderado de descentralizar, y verán por qué. Este es un tema totalmente transversal que afecta todo el mundo. Entonces, lo que no podemos pensar es que lo que le sucede al Ejército de Tierra, con todos sus recursos y con toda su extensión, lo vamos a defender desde el Mando Conjunto de Ciberdefensa, por muchos que seamos. No tiene sentido. Además, tampoco podemos dejar a los ejércitos ignorantes de este asunto. De hecho, el segundo objetivo global que tenemos en el mando es llevar la ciberdefensa a todos los rincones del Ministerio de Defensa, y para hacerlo consideramos que lo mejor es que ellos también sean protagonistas de eso. Entonces, ¿quién mejor que la Armada para ciberdefender una fragata F-100? ¿Lo podemos hacer nosotros? No, lo que pretendemos hacer es dar directrices, normalizar, dirigir la orquesta para que todos, en vez de ir detrás de la pelota, guardemos nuestros puestos correctos en el campo de juego, eso sí.

Disuasión. Para ejercer la disuasión hay que tener recursos y, sobre todo, hay que tener la firme voluntad de emplearlos y que el adversario lo sepa. Esos son los componentes de la disuasión. ¿En el ciberespacio puede haber disuasión? Yo creo que sí, igual no tiene el mismo efecto pero si saben que eres bueno y que tienes la firme intención de utilizar tus capacidades, se puede ciberdisuadir.

¿Cómo se retiene al personal? En cuanto a la selección, es el perfil técnico. Pero antes ha habido otro comentario que probablemente era de más calado: somos un mando militar. Por lo tanto, la gran mayoría debe ser de uniforme, porque estamos implicados en operaciones militares. Cuesta darse cuenta de esto, pero hacemos operaciones militares; en el ciberespacio, pero hacemos operaciones militares. Entonces, obviamente, la gran mayoría de la unidad debe ser militar. Por supuesto, también tenemos civiles, claro que sí, porque proporcionan una capacidad técnica importante y también, en los tiempos que corren, una continuidad en el lugar y eso también es muy valioso. Pero yendo a cómo lo retenemos, les puedo asegurar por mi experiencia que para la persona buena en ciberseguridad el dinero no es su primera motivación. Hay que cubrir unos mínimos, no podemos malpagar a la gente, pero si la persona tiene cubiertos unos mínimos, tiene un trabajo interesante, tiene un buen ambiente de trabajo y tiene unas posibilidades de formación que de otra manera no podría lograr, retenemos al personal.

En cuanto a la lealtad del personal, si ven nuestro emblema, el primer término del emblema es «lealtad». En muchas ocasiones me han dicho: pues para obtener recursos de personal, ¿por qué no

cve: DSCG-12-CM-67

hacéis contratos de dos años, de tres años o de seis meses? No podemos hacer eso. No podemos confiar —permítanme la expresión— en cualquiera, sin que el término cualquiera sea peyorativo en este caso. Tenemos que garantizar la lealtad del personal que trabaja con nosotros. Les diría más, incluso no digo no fiarnos de ellos, porque sería absurdo, pero sí establecer estructuras que impidan que una única persona conozca todo. Esto es de sentido común. El caso Snowden fue un ejemplo de ese estilo; una persona que no era un gran sénior de la organización y que, por errores, tenía un gran conocimiento del sistema. Eso hay que romperlo. Por supuesto, toda la gente que trabaja con nosotros tiene una habilitación personal de seguridad en el grado de reservado. Son elementos y elementos que se van poniendo.

Sobre si tenemos capacidad nacional de ciberseguridad, sí. Hay bastantes empresas españolas que son buenas y que son punteras. Les voy a dar mi opinión, que puede estar equivocada, pero es la mía y se la doy con toda sinceridad. Yo creo que el gran motor de esa ventaja ha sido la banca. La banca española es potente. La banca española y toda la banca hoy en día están en primera línea de fuego; combaten en la trinchera del ciberespacio y, si se equivocan, pierden el dinero. Por lo tanto, no pueden equivocarse y, por lo tanto, invierten y al invertir hacen que ese mercado se desarrolle. La banca ha sido la locomotora desde hace unos años, por supuesto lo sigue siendo y sí, hay buena industria. El español es una persona imaginativa, que sale muy bien de los apuros y que trabaja bien bajo presión, normalmente; tiene un perfil bueno para esta actividad, en términos generales. Lo que hay que hacer es lo que ha hecho la banca.

¿Qué hacemos en I+D? Por supuesto, el órgano de I+D es la Dirección General de Armamento y Material, dentro del Ministerio de Defensa, pero para este tipo de actividades ellos se apoyan en nosotros y nosotros les ayudamos todo lo que podemos, cómo no. Lo que se procura es desarrollar productos y herramientas que obviamente no están en el mercado porque, si no, no merecería la pena, sería mejor comprarlo —en ningún caso merece la pena reinventar la rueda—, pero sí que hay mucho por hacer y se valora el esfuerzo, el coste, el tiempo, porque si se va a tardar en obtener tres años, en este tipo de actividad no te vale para nada; cuando lo has obtenido ya no sirve o está superado. Hay que evaluar todos esos aspectos. El *gap* tecnológico es así y, sobre todo, el *gap* tecnológico se plantea entre Europa y los demás. Corea del Sur fabrica microchips, también China y Estados Unidos pero Europa no; se ha fraccionado el *gap*, hay que acudir fuera. Ese es un tema tecnológicamente estratégico al que habría que ponerle solución.

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

Hay un segundo turno, pero antes quiero comentar algo, porque ha habido una cierta confusión con la información. Señor Raffo, el día 14 estará aquí el señor Janis Sarts, que es el director del Centro de Excelencia de Comunicaciones Estratégicas de la OTAN, que está en Riga, y en la que, efectivamente, no está España. Entiendo que esa visita será, probablemente, una invitación a que subsanemos esa deficiencia.

Segundo turno, señor Salvador.

El señor **SALVADOR GARCÍA:** Voy a intervenir rápidamente y no por comer, porque estamos acostumbrados —lo digo para no dar una mala imagen al compareciente— o a comer poco o a comer en la cafetería casi con el Pleno empezado.

Mi pregunta no era tanto sobre la coordinación, sobre si están bien coordinados, que presupongo que sí, y usted mismo ha dicho que coinciden y comparten actividad. Me refería más a si el reloj está en hora en todos; es decir, si todos están evolucionando a la par, si el sector de las empresas no va más retrasado que el sector de las Fuerzas y Cuerpos de Seguridad del Estado, si ustedes están más avanzados y, al final, el ciudadano de a pie está totalmente descolgado. Con esto quiero saber si, dentro de esta estrategia nacional, todos estamos trabajando acompasadamente para que la evolución sea conjunta.

Muchas gracias por la comparecencia.

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

Señor Comorera.

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

Quiero agradecer las respuestas concisas a mis anteriores preguntas. Únicamente quiero añadir una pregunta para saber su valoración al respecto y es en relación con la diferenciación entre *hacker y cracker*. En la diapositiva que nos ha puesto antes se distinguía entre acceder y agredir. Esto lo pondría en

cve: DSCG-12-CM-67

consonancia con las dos palabras; es decir, cuál es su valoración sobre la posibilidad de reclutar a personas que consigan acceder sin agredir y denuncien fallos de seguridad, y si sería interesante reclutar a esos perfiles de expertos —por llamarlos de alguna manera— para la ciberseguridad española.

Muchas gracias.

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

Señor Raffo.

El señor **RAFFO CAMARILLO:** Haré una reflexión redundando en un aspecto que considero importante. El general López de Medina nos ha ilustrado muy bien con un *collage* de las distintas organizaciones, tanto públicas como privadas, en concreto universidades y el sector de las empresas, independientemente del tamaño, y los distintos actores y agentes que pueden participar para afrontar, en un contexto muy complejo —y que en vez de dejar de serlo va a seguir siendo cada vez más complejo—, un problema complejo que también va a seguir siendo cada vez más complejo. Sigo considerando que es necesario —y esto es interesante porque creo que realmente ahí va a estar el quid de la cuestión— la incorporación de la visión del ciudadano en el proceso de toma de decisiones. Con esto no quiero decir que hagamos asambleas, sino que hay fórmulas con las que ciudadanos de distintos ámbitos —más allá de la universidad y las empresas—, a través de determinadas técnicas —bien individualmente, bien a través de asociaciones, entidades u organizaciones—, se pueden incorporar y así abrir el campo en la campaña de concienciación dirigida a través de los medios. Sería interesante que nos lo planteáramos porque la dimensión del problema es lo suficientemente amplia, profunda y compleja como para que aprendamos que cada vez que se han dado estas situaciones, si la ciudadanía no tiene abierta una ventana para participar en el proceso de toma de decisiones, no vamos a avanzar lo suficiente, y en una situación como esta vamos a acabar siendo derrotados.

Simplemente quería hacer esta reflexión.

El señor **PRESIDENTE:** Señor Cosidó.

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

Únicamente quiero agradecerle sus respuestas. Creo que es difícil contestar más rápido y con más precisión a tal batería de preguntas que le hemos formulado los distintos grupos.

Tan solo no me ha contestado a un comentario sobre si comparte mi entusiasmo por los ciberreservistas o no, y espero que, si fuera posible, en esa visita pudiéramos conocer otras muchas cuestiones que, sin duda, se han quedado en el tintero y que serían de máximo interés. Le deseo lealtad, constancia, ingenio y destreza porque nos jugamos mucho como país con su éxito.

Gracias.

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

General.

El señor **GENERAL DE DIVISIÓN, JEFE DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD** (Gómez López de Medina):

Estamos todos en hora.

El señor **PRESIDENTE:** Estamos tarde.

El señor **GENERAL DE DIVISIÓN, JEFE DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD** (Gómez López de Medina):

No, perdón, no estamos todos en hora. Probablemente, en la Administración sí que hay un interés por estar todos en hora por encima de cualquier otra circunstancia; luego, hay dificultades que no facilitan ese sincronismo. Pero en el mundo empresarial, que obviamente se mueve por la cuenta de beneficios —no nos engañemos—, va a depender de lo que impacta la ciberseguridad en su cuenta de beneficios. Vuelvo al ejemplo de antes: la banca, indudable; ahora, la empresa que se debate en esos dos estados que decía antes: la incredulidad y la resignación, probablemente el reloj se le atrasa, pero habría que ponernos a todos en hora, es absolutamente necesario y cierto.

Lo relativo a este personal al que nos referíamos —contestando al señor Comorera— lo iba a enlazar con la ciberreserva, porque he sido consciente al hacerme esa pregunta de que no le había contestado;

cve: DSCG-12-CM-67

me da cancha para hablar de la ciberreserva. La ciberreserva, en mi opinión, es una magnífica idea porque reúne varias virtudes. Primero, tenemos una fuerza, un aumento de fuerza de una manera muy flexible cuando sea necesario, y con gente extraordinariamente cualificada, gente que aporta casi lo más valioso, que es la ilusión, la motivación. Eso es muy valioso y lo van a traer; y, además, les diríamos: y no les vamos a pagar nada. El único sueldo es la satisfacción de defender a su nación, a su Estado; esa es la única satisfacción. Lo único que le vamos a pagar son los gastos, porque no le vamos a hacer perder dinero. Ese sería el banderín de enganche. Además, tiene más virtudes, y es que pueden colaborar *online*, no tienen que venir, no serían ciberreservistas de una unidad convencional, lo que además de estar presente requiere incluso unas condiciones físicas; no es necesaria esa condición física. Necesitamos su talento, eso es lo que necesitamos sobre todo.

Les añado un matiz —les estoy contestando a los dos, perdónenme—, y es que estamos haciendo operaciones y cuando tengo a alguien en operaciones, quiero que sea militar. Entonces haría dos ciberreservas: una militar y otra civil, o dos elementos dentro de la ciberreserva. Hay muchas tareas que no son estrictamente de operaciones que podrían ser desempeñadas perfectamente por alguien en su condición de civil, pero cuando pasamos a realizar operaciones de cualquier tipo, creo que lo apropiado es que las ejecute personal con condición de militar. Pero podríamos dar entrada a todo este personal brillante y, además, podríamos responder creo que es al artículo 30 de la Constitución, que dice que los españoles tienen derecho a participar en este esfuerzo; también le daríamos salida a eso. Obviamente, habría que organizarlo, no es algo trivial; habría que crecer progresivamente. Es decir que si ahora alguien me dice: pongo 2000 personas, le diría que mejor no **(Risas),** vamos a hacerlo poco a poco; crecer con un determinado ritmo sería fenomenal. Además, no seríamos inventores; ya hay realidades de ese estilo en otras naciones.

Señor Raffo, muchas gracias por la pregunta sobre la incorporación del ciudadano. El ciudadano tiene un valor tremendo porque, entre otras cosas, es el que paga. Su decisión es capaz de cambiar el mercado y le voy a poner un ejemplo. A principios de los noventa te comprabas un vehículo y el ABS era una opción cara. Sin embargo, era una opción que te daba seguridad para ti y para los tuyos. ¿Por qué empezó a popularizarse? Porque el ciudadano lo quería y se hizo cada vez más barato. Ahora cualquier vehículo, aunque sea el más elemental, tiene ABS. Cuando el ciudadano empiece a decir que quiere ciberseguridad y que quiere ciberseguridad, la Internet de las cosas tendrá ciberseguridad porque, si no, no comprará esa cámara y comprará otra.

¿Qué es lo que hace falta? En mi opinión, un elemento iniciador. Hay que concienciar al ciudadano, pero para eso hace falta el poder del Estado. Hay que poner en marcha esto. Hay que poner en marcha de verdad la línea de acción número 7 de la Estrategia de Ciberseguridad Nacional. Nosotros lo hacemos en nuestro ámbito. Nuestra población objetivo son 140 000 personas y nuestras familias, y hacemos multitud de actividades para que la audiencia no se nos aburra cuando la digamos diez veces que tiene que cambiar la contraseña. Si se aburre, hemos perdido. Tenemos que conseguir que no se aburra y le preste atención. Le hemos dado muchas vueltas y hacemos muchas acciones de concienciación. Como les decía antes, es extraordinariamente rentable por cuatro perras, pero hay que mover a una cantidad de personas muy importante con, por ejemplo, programas de televisión que sean didácticos. La verdad es que el caldo de cultivo existe porque cada vez la gente está más sensibilizada. Como saben, España es de las naciones que utiliza más teléfonos inteligentes, una capacidad importante y, por supuesto, vulnerable. Por tanto, tendríamos posibilidades para trasladar ese conocimiento, esa inquietud y esa concienciación al ciudadano. A partir de ahí, cuando tuviese esa cultura, actuaría por sí solo y tendría criterio para elegir, para valorar lo que le ofrecen y para rechazar lo que no debe ser y lo que no cumple los criterios que ha aprendido en ese proceso de concienciación.

El señor **PRESIDENTE:** Muchísimas gracias, general.
Damos por terminada la comparecencia.

Eran las tres y quince minutos de la tarde.

cve: DSCG-12-CM-67