# DIARIO DE SESIONES DE LAS CORTES GENERALES

## COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 120 | Pág. 1


# DE SEGURIDAD NACIONAL

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

**Sesión núm. 23**

**celebrada el martes 20 de noviembre de 2018 en el Palacio del Congreso de los Diputados**

---

Página

**ORDEN DEL DÍA:**


**Comparecencia de la señora Olmo Romero (embajadora en misión especial para las amenazas híbridas y la ciberseguridad), para informar sobre diversas cuestiones relativas a la ciberseguridad en España. Por acuerdo de la Comisión Mixta de Seguridad Nacional. (Número de expediente del Congreso de los Diputados 212/001859 y número de expediente del Senado 713/001099) ..... 2**


---


cve: DSCG-12-CM-120

**Se abre la sesión a las diez y cinco minutos de la mañana.**

El señor **VICEPRESIDENTE** (Jiménez Tortosa): Buenos días, señorías. Vamos a dar inicio a la sesión de la Comisión Mixta de Seguridad Nacional atendiendo a la comparecencia de doña Julia Olmo Romero, embajadora en misión especial para las amenazas híbridas y la ciberseguridad, para informar sobre diversas cuestiones relativas a la ciberseguridad en España. Doña Julia, muchas gracias por comparecer en esta Comisión, estamos deseando escuchar su intervención por el tiempo que usted considere oportuno. Y a continuación, daremos la palabra a los portavoces por tiempo de cinco minutos para cada grupo parlamentario.

Muchas gracias, bienvenida al Congreso, y suya es la palabra.

La señora **OLMO ROMERO** (embajadora en misión especial para las amenazas híbridas y la ciberseguridad): Muchas gracias, señor presidente.

Buenos días, señorías. En primer lugar, quisiera agradecer a la Comisión esta invitación. Es un honor para mí poder dirigirme a ustedes en esta ponencia de estudio sobre cuestiones de ciberseguridad. Soy diplomática de carrera, y el pasado mes de marzo tuve la honra de ser nombrada embajadora en misión especial para las amenazas híbridas y la ciberseguridad. Estoy adscrita a la Secretaría de Estado de Asuntos Exteriores, enmarcada en la Dirección General de Política Exterior y de Seguridad, y represento al Ministerio de Asuntos Exteriores en calidad de vocal en el Consejo Nacional de Ciberseguridad.

Como saben, la Ley de la Acción y del Servicio Exterior del Estado de 2014 reconocía la eventual creación de misiones diplomáticas especiales para contenidos de carácter especial. Tras esta ley y en línea con la Estrategia de Ciberseguridad Nacional de 2013, se crea por primera vez esta figura, lo que supuso una mejora cualitativa en el desarrollo de la acción exterior del Estado en materia de seguridad en el ciberespacio. Ahora, recientemente, en marzo se añadió un elemento nuevo, las amenazas híbridas, a la luz de los nuevos desafíos para la seguridad, como así constató la Estrategia de Seguridad Nacional del pasado mes de diciembre. Se trata, por lo tanto, desde esta posición, de contribuir a potenciar y a reforzar la presencia de España en las organizaciones, conferencias, foros internacionales y regionales de los que España forma parte, y en cuyas agendas están presentes las amenazas híbridas y la ciberseguridad, con especial atención a la Unión Europea, y participar en las distintas iniciativas internacionales apoyándose en la coordinación de las posiciones de los diferentes agentes nacionales implicados.

Cuando hablamos de ciberseguridad, lo hacemos de un concepto muy amplio. Para algunos se trata de la creación de confianza y seguridad en la utilización de las tecnologías de la información y las comunicaciones, pero también la ciberseguridad tiene que ver con la seguridad nacional, con la garantía y supervisión de nuestros derechos y libertades, con nuestros valores como sociedad y como país y, en definitiva, con garantizar nuestra propia soberanía y, también, en consecuencia, con la paz y la seguridad internacionales. Es importante recordar y tener en mente que el ciberespacio no es un espacio natural, ha sido creado por el hombre y está considerado como un espacio común global; un espacio interconectado, complejo y diverso, donde no existen fronteras y donde se desdibujan y diluyen las fronteras nacionales. Un espacio con múltiples actores, no solo los Estados, sino también Gobiernos y, además, de forma muy activa, actores no estatales, el sector privado, la industria, los usuarios, los investigadores y la academia. Es un espacio que posibilita avances, prosperidad, crecimiento, desarrollo inclusivo, conocimientos y cercanía; un sinfín de ventajas para la humanidad, pero también del que emanan múltiples amenazas que pueden contribuir a elevar las tensiones, que pueden desestabilizar y causar daños notables en el mundo físico.

Hoy todos somos conscientes de que las amenazas se han incrementado, han proliferado los actores y se han sofisticado los vectores de transmisión. Se han multiplicado también los objetivos y los medios. Y toda esta complejidad nos lleva a tener que actuar desde dentro, desde fuera y también en contra y, en consecuencia, a elaborar respuestas conjuntas nacionales, internacionales y multilaterales y, de la misma manera, abordar todo ello desde una perspectiva integral que implique a todos los sectores, actores e instrumentos disponibles. Esta visión integral ha sido y es la adoptada en la Estrategia de Ciberseguridad Nacional de 2013, que se encuentra ahora en proceso de revisión, y estoy convencida de que lo será en la próxima. En este punto deseo destacar que España cuenta con recursos tecnológicos, herramientas, experiencia, instituciones y un sector privado capaz de todo ello, y con prestigio y respeto internacional en este campo. Entiendo que la Estrategia de Ciberseguridad Nacional ha sido ya explicada por anteriores comparecientes. No obstante, sí quiero retener y subrayar que uno de los principios rectores de la misma

cve: DSCG-12-CM-120

es la cooperación internacional. En este sentido, permítanme recordar que la línea de acción número ocho lleva por título: Compromiso internacional, promover un ciberespacio seguro y confiable en apoyo de los intereses nacionales. De esta misma línea de acción emana el Plan Derivado de Cooperación Internacional y Unión Europea, cuyas acciones se coordinan en el seno de un grupo de trabajo que rinde cuentas posteriormente al Consejo Nacional de Ciberseguridad, está presidido por el Ministerio de Asuntos Exteriores y en el que, además, se sientan, entre otros, el Departamento de Seguridad Nacional, el Centro Criptológico Nacional, el Mando Conjunto de Ciberdefensa, el Centro Nacional de Protección de las Infraestructuras Críticas, el Incibe, el CDTI y la Fiscalía en materia de criminalidad informática.

Permítanme que empiece poniendo de relieve nuestra cooperación en materia de ciberseguridad en algunas organizaciones internacionales. Y voy a comenzar por la OSCE, la Organización para la Seguridad y la Cooperación en Europa, porque en ella se sientan 57 Estados, incluidos Estados Unidos y la Federación Rusa, y se dialoga, creo que de manera fructífera, para reducir los conflictos y los riesgos derivados del uso de las TIC. En su Grupo de Trabajo Informal sobre Ciberseguridad está lográndose poner en marcha dieciséis medidas de fomento de la confianza; medidas que son un ejemplo para otras organizaciones regionales y que han sido tomadas como modelo por la Organización de Estados Americanos y por el Asean Regional Forum. España está acompañando, junto a otros Estados miembros, la implementación de dos de estas medidas; la número ocho relativa a la designación de puntos focales nacionales responsables de la gestión de incidentes, para permitir un diálogo directo entre instituciones competentes de los Estados miembros en caso de incidentes; y la número quince para impulsar la colaboración entre autoridades nacionales responsables de la seguridad de las infraestructuras críticas. Pero también cooperamos en el Consejo de Europa apoyando la labor de la fiscalía contra la criminalidad informática en la expansión del Convenio de Budapest y en las negociaciones sobre el segundo protocolo relativo a la prueba electrónica. Y con la OEA, Organización de Estados Americanos, apoyando e impulsando las capacidades de ciberseguridad para el fomento del gobierno electrónico de la región, a través de la construcción de capacidades en el sector público y privado de estos países, la formación de jueces, de miembros de cuerpos y fuerzas de seguridad de los Estados, de funcionarios y de jóvenes.

Además, trabajamos también con el Foro para la Gobernanza en Internet, una plataforma global y multiactoral de Naciones Unidas que busca facilitar el diálogo sobre políticas públicas relacionadas con Internet. La última conferencia anual de este foro tuvo lugar la semana pasada en París, en el marco de los actos celebrados por Francia con motivo del centenario del armisticio. Una conferencia que fue inaugurada por el Presidente Macron y por el secretario general de Naciones Unidas, de la que salió el llamado Llamamiento de París para la confianza y la seguridad en el ciberespacio. Un llamamiento que ha sido ratificado ya por más de sesenta países, entre ellos España, más de un centenar de empresas, organizaciones de la sociedad civil, universidades y centros de pensamiento, entre ellos el Real Instituto Elcano. De igual modo trabajamos en el Foro Global para la Capacitación Cibernética, organización gubernamental con más de ochenta países que persigue aumentar las capacidades en materia de ciberseguridad contribuyendo, entre otras cuestiones, a reducir la brecha digital entre países y avanzar a través del desarrollo digital en la consecución de los Objetivos de Desarrollo Sostenible. Lo hacemos también en la Coalición para la Libertad en Línea, foro también gubernamental formado por una treintena de países que persigue, mediante la coordinación de esfuerzos y el trabajo conjunto con la sociedad civil, el reconocimiento y protección de los derechos humanos y de las libertades fundamentales *online*, de la misma manera que se respetan y protegen *offline*. Y por supuesto, trabajamos también con Naciones Unidas, y muy especialmente con la Unión Europea, en lo que me detendré más tarde.

Antes de entrar en ello, quisiera hacer una referencia a nuestra cooperación bilateral con otros países. Hemos firmado ya memorandos de entendimiento con una decena de países, con Andorra, Argentina, Brasil, Chile, India, Marruecos, Paraguay, Perú y Túnez. A ellos hay que sumar el recientemente firmado por el presidente del Gobierno de España y el presidente de la República de Chile, con motivo de la visita de este último a Madrid el pasado mes de octubre. Se trata en todos los casos de documentos de contenido amplio que permiten sentar las bases para la institucionalización de relaciones más estrechas, y que están posibilitando a otros organismos de la Administración poner en marcha una colaboración directa y específica con sus homólogos de otros países. Como pueden comprender, esto es una agenda que no para de crecer. La ciberseguridad está hoy entre las mayores preocupaciones de los líderes mundiales, es una cuestión ineludible en todos los foros internacionales y cada vez más presente en las agendas bilaterales. Piensen sus señorías en el Foro de Davos, en la Cumbre ASEM, el G-20 o la Conferencia de Munich. Decía Kissinger que el ciberespacio desafiaría toda la experiencia histórica, y así

cve: DSCG-12-CM-120

ha sido. La mayoría de los analistas están convencidos de que el orden internacional derivado de la Segunda Guerra Mundial ha cambiado. Y ello resulta más evidente si pensamos en ciberseguridad, en Internet y en la debilidad de la regulación internacional del ciberespacio.

Con ello entro ya a hablarles de Naciones Unidas. Pensemos en Internet como un bien público global y en el ciberespacio como un espacio público también global. El área donde se gestionan los bienes públicos y donde se protegen esos intereses públicos globales es el derecho internacional, y frente a ellos o para ellos las legislaciones nacionales no resultan del todo eficaces. Sin embargo, nuestra civilización está marcada por una idea central que es la del derecho, y a pesar de que la ciberseguridad es una aspiración común, su ecosistema, el ciberespacio, carece de regulación tal y como la entendíamos en ese orden salido de la Segunda Guerra Mundial. En este contexto, consideramos que el papel de Naciones Unidas sigue siendo fundamental. La organización ha tratado el tema desde 1998, cuando Rusia presentó por primera vez un proyecto de resolución sobre los «Avances en la información y las telecomunicaciones en el contexto de la seguridad internacional». Una resolución que fue aprobada sin votación. Sin embargo, no fue hasta la creación del primer grupo de expertos gubernamentales en 2010, cuando empieza a concretarse la necesidad de avanzar en la gobernanza del ciberespacio. Hasta la fecha se han reunido cinco grupos de expertos, pero solamente los de 2013 y 2015 han dado resultados positivos aprobándose sus informes por consenso. Me permito recordar que España participó en el grupo de expertos de 2015. De estos informes podemos constatar que hay consenso entre la comunidad internacional en que el derecho internacional es aplicable al ciberespacio, lo que incluye el respeto a los derechos humanos, así como a la Carta de Naciones Unidas en su totalidad, lo que supone igualdad soberana y no intervención en asuntos internos. Del mismo modo, la obligación de los Estados de fomentar un ciberespacio abierto, seguro, estable, accesible y pacífico y de respetar una serie de normas sobre el comportamiento responsable de los Estados. No obstante, tras la última Resolución de 2016 presentada por Rusia, copatrocinada entre otros muchos países por España y aprobada sin votación por la Asamblea General, la comunidad internacional no ha sido capaz de seguir avanzando conjuntamente en este terreno, lo que ha producido un cierto parón en la regulación del ciberespacio.

¿Qué consideramos qué hay detrás de esta situación o de esta imposibilidad? En primer lugar, estamos todos de acuerdo en la aplicación del artículo 7 de la carta, es decir, del principio de no intervención, pero si acudimos al artículo 51, al derecho a la legítima defensa en caso de agresión, ahí nos encontramos en cómo la definimos en el ciberespacio; si existe agresión, existiría el derecho a la legítima defensa, pero para desencadenar una respuesta, un ataque, hay que buscar el origen, hay que trazarlo y atribuirlo. Y recordemos, además, que en el ciberespacio tenemos actores estatales —solamente ellos son sujetos de derecho internacional— y también actores no estatales. En segundo lugar, nos separa la defensa y el mantenimiento de los derechos en el ciberespacio de la misma manera que los tenemos reconocidos en el mundo físico, lo que incluye el derecho a la libertad de expresión o el derecho a la privacidad. Y en tercer lugar, una concepción misma del ciberespacio que nos lleva a concepciones diferentes que se sustancian en conceptos distintos de soberanía; mientras que unos apostamos por un ciberespacio abierto, seguro y estable, resultado del esfuerzo conjunto de múltiples actores —Estados, sector privado, sociedad civil, comunidad técnica—; otros se inclinan por la sola y exclusiva presencia de los Estados como actor privilegiado y exclusivo para gobernar la red.

En este contexto este año, por primera vez, se han presentado dos resoluciones distintas en la Asamblea General. Primero lo hizo la Federación Rusa con una propuesta radicalmente distinta de lo que habían venido siendo sus propuestas anteriores en este campo y, posteriormente, quizá como reacción o consecuencia de la anterior, la de Estados Unidos que, curiosamente, estaba calcada de las que la Federación Rusa había presentado en los años anteriores. El resultado es que ambas han sido aprobadas, y que a partir de enero de 2019 vamos a tener dos procesos paralelos cuya implementación vamos a seguir con atención: un grupo de trabajo de composición abierta planteado por la Federación Rusa, y el grupo de expertos gubernamentales planteado por Estados Unidos. Cabe destacar que en ese momento la mayor parte de los oradores se expresaron en el sentido de buscar la complementariedad entre ambos grupos. España apostó y ha apostado siempre desde el principio del debate por evitar la polarización. Y en línea con nuestros socios europeos defendemos la necesidad de buscar el consenso partiendo de consensos anteriores; esto es, la necesidad de un marco estratégico para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio; la aplicación, como ya hemos dicho, de la carta en su totalidad y del derecho internacional y la creación de medidas de fomento de la confianza y, sobre todo, el papel central de Naciones Unidas en este proceso.

cve: DSCG-12-CM-120

En este contexto, ¿qué estamos haciendo en Europa? Desde la Estrategia de Ciberseguridad de la Unión Europea de 2013, Europa ha ido ganado conciencia de la importancia de la ciberseguridad e incrementando sus actividades en este campo y, al mismo tiempo, avanzando hacia un ecosistema cibernético capaz de asegurar la prosperidad, el crecimiento, la seguridad de la Unión Europea y la integridad de nuestras sociedades libres y democráticas. El salto se produce en el mes de septiembre pasado, coincidiendo con la Presidencia estonia del Consejo, tras la aprobación de la comunicación conjunta «Resiliencia, disuasión y defensa: fortalecer la seguridad de la UE». Europa llega al convencimiento de la necesidad de apostar por una agenda digital en toda su amplitud. Una agenda que contemple la ciberseguridad desde una perspectiva integral, coherente, a escala nacional de la Unión Europea y global, que considere que las ciberamenazas tienen un impacto real en la democracia, en nuestra seguridad y en nuestra prosperidad económica. En esta línea Europa está convencida de que el mercado único será digital o no será mercado ni será único y, por lo tanto, ha de ser seguro.

Con esta convicción, Europa pasa de una posición reactiva a una proactiva; pasa a buscar sinergias para avanzar hacia una autonomía estratégica, a mejorar su resiliencia, la capacidad de respuesta y a reforzar la cooperación internacional. Hay que recordar también que, hoy por hoy, Europa es un importador neto de productos y soluciones de ciberseguridad y que depende, en gran medida, de proveedores no europeos. En este contexto, la Comisión Europea presentó el llamado Paquete de Ciberseguridad, cuyas líneas maestras pueden agruparse en tres puntos: en primer lugar, asegurar una eficaz ciberresiliencia y la confianza en el mercado único digital. Entre las acciones en este campo destacaría la reforma de la Agencia Europea de Ciberseguridad, Enisa, y la creación de un marco común homogéneo de certificación de productos y servicios que busca la seguridad en el diseño. Esta ley está en proceso de aprobación en el Parlamento Europeo. Además, se ha transpuesto a todos los países la llama Directiva NIS para lograr una mayor seguridad en las redes, en España por el Real Decreto-ley 12/2018; el *Blue Print* o marco general común para la gestión de crisis y la respuesta rápida a emergencias, a través del que se está trabajando en una taxonomía común de calificación de incidentes; el reforzamiento del CERT de la Unión Europea, es decir, de los equipos de respuesta rápida de emergencia a incidentes y la creación de una red europea de centros; la entrada en vigor, el pasado mes de mayo, del Reglamento General de Protección de Datos; y la futura creación del centro europeo de competencia en ciberseguridad y la red de centros nacionales de competencia, una propuesta de reglamento presentada por la Comisión en septiembre y que se encuentra actualmente en discusión en el grupo de trabajo del Consejo. Es una propuesta interesante que persigue la creación de una industria tecnológica europea, y que consagrará definitivamente la colaboración público-privada en esté ámbito. Para ello plantea reunir todos los fondos dedicados a ciberseguridad, que hoy se encuentran dispersos en diferentes organismos y programas de la Unión Europea, en ese único centro europeo, lo que significa, probablemente, la gestión de un presupuesto para el período 2021-2027 en torno a los 2700 millones de euros.

Como segunda línea maestra del Paquete de Ciberseguridad, crear las capacidades para prevenir, disuadir, detectar y responder a actividades maliciosas en el ciberespacio mediante el reforzamiento de Europol; la directiva contra el fraude en Internet y la falsificación de los medios de pago distintos del efectivo, también en fase de aprobación en el Parlamento Europeo; la directiva para el acceso transfronterizo a pruebas electrónicas presentada por la Comisión en abril; los avances en el Convenio de Budapest; el reforzamiento de la respuesta diplomática a través de la llamada «caja de herramientas» y de la disuasión con las capacidades de defensa de los Estados miembros. Cabe recordar que esta «caja de herramientas», aún cuando es todavía un instrumento en construcción, contempla todo un abanico de medidas —diplomáticas, políticas y económicas— bajo el paraguas de la Política Exterior y de Seguridad Común, incluyendo las de carácter restrictivo, es decir, sanciones. En este punto no podemos olvidar tampoco la ciberdefensa europea en el marco de la Cooperación Estructurada Permanente, con el papel del Fondo Europeo de Defensa. **(El señor presidente ocupa la Presidencia.)**

Por último, en tercer lugar, reforzar la cooperación internacional en favor de un ciberespacio global, abierto, libre, pacífico y seguro. La Unión Europea es consciente de que los avances en la cooperación digital internacional tienen lugar en un entorno cambiante y reconoce esa naturaleza interconectada. Nos hemos referido ya a la posición europea en los debates de Naciones Unidas y a que la Unión Europea no es partidaria, como hemos apuntado, de propugnar un tratado internacional sobre el ciberespacio por esa concepción multiactoral que defendemos. Sin embargo, hay una apuesta clara por fortalecer capacidades en terceros Estados y para ello posee un instrumento específico, el Instrumento para Contribuir a la Paz y a la Estabilidad. Se han adoptado ya líneas de la Unión Europea para la construcción de capacidades y

cve: DSCG-12-CM-120

se trabaja en la puesta en marcha de la Red exterior de construcción de capacidades. Sobre este punto permítanme añadir que la Estrategia Global de la Unión Europea de 2016 reafirmaba la autonomía estratégica también en el ciberespacio. Y además, cabe recordar que el Consejo Europeo de noviembre del año pasado afirmó que un ciberataque podía constituir base suficiente para que un Estado miembro invocara la cláusula de solidaridad del Tratado de Funcionamiento de la Unión o la de asistencia mutua en el Tratado de la Unión Europea. Al mismo tiempo, como señalaba antes, se ha avanzado en la utilización de la «caja de herramientas». Se acudió por primera vez condenando el uso malicioso de las TIC y los ciberataques causados por WannaCry y NotPetya.

Por otra parte, y consciente de que algunas medidas previstas en la caja no requieren de atribución, pero otras sí, el Servicio Europeo de Acción Exterior ha circulado recientemente un documento al objeto de empezar a desarrollar lo que podríamos llamar una cultura común de atribución. Sin duda, todo un desafío de carácter técnico y político que requiere reflexión. Resulta evidente que la atribución de actividades cibermaliciosas puede basarse en un gran número de elementos de variada naturaleza que comprenderían datos técnicos derivados de análisis forenses, evidencias de inteligencia e información de fuentes abiertas, junto a otros elementos de carácter político. Se trata, en todo caso, de un proceso cuyos métodos, procedimientos, definiciones y criterios pertenece a la esfera soberana de los Estados, lo que no va a impedir en Europa avanzar en un entendimiento común sobre cómo ha de orientarse la atribución y cómo han de ser evaluadas las circunstancias de cada situación.

En este contexto, el pasado 4 de octubre, a raíz del ciberataque contra la Organización para la Prohibición de Armas Químicas, y por el que Reino Unido y los Países Bajos acusaron a Rusia, el presidente de la Comisión, el del Consejo y la Alta Representante hicieron público un comunicado en el que, tras expresar su seria preocupación y deplorar lo ocurrido, reafirmaban su determinación por reforzar la resiliencia de la Unión Europea y la de los Estados miembros. No obstante, no formalizaron una atribución del hecho, limitándose a recoger la información proporcionada por los dos países antes citados.

El último Consejo Europeo, de 18 de octubre, destacó la necesidad de reforzar la disuasión y la resiliencia europeas, condenó el ataque contra la OPAQ, pidió que, como herramienta de disuasión y respuesta, se iniciara el estudio sobre el posible establecimiento de sanciones frente a los ciberataques y que se tomaran medidas para la protección de los sistemas democráticos de la Unión frente a la desinformación, especialmente de cara a las elecciones al Parlamento Europeo.

Si me lo permiten, porque creo que puede ser de su interés, entraremos en este último aspecto. Además de las elecciones al Parlamento Europeo, la Comisión calcula que el próximo año tendrán lugar en Europa una veintena de procesos electorales de diferente naturaleza y procedimiento. Así se puso de manifiesto en la pasada Conferencia de Alto Nivel sobre Interferencia Electoral, celebrada en Bruselas los pasados días 15 y 16 de octubre; una conferencia para aclarar que proteger la integridad de los procesos es una prioridad, es una cuestión de seguridad. La Unión Europea constata que ha visto cómo en los últimos tiempos muchos de estos procesos han sido objeto de ataques y sufrido intentos de manipulación. Como decía, estas amenazas se concretan, bien en los ataques dirigidos contra los sistemas tecnológicos asociados al proceso electoral, o bien afectan al comportamiento con el fin de manipular la intención de voto. Por tanto, para la Unión Europea es necesario fortalecer y reforzar la ciberseguridad y, al mismo tiempo, combatir la desinformación.

En el último discurso sobre el estado de la Unión, el presidente Juncker señalaba que para disfrutar de elecciones justas, seguras y transparentes, en un momento en el que el riesgo de manipulación nunca ha sido tan alto, los procedimientos electorales han de adecuarse a la era digital. Sobre esta base, a las medidas de ciberseguridad que están en curso, y a las que ya me he referido, la Comisión ha sumado otras, de carácter más específico, con los siguientes objetivos. En primer lugar, protección de datos. La Comisión ha elaborado una guía para la aplicación al proceso electoral del Reglamento General de Protección de Datos dirigida a partidos políticos, fundaciones, autoridades nacionales electorales y plataformas digitales, con el objetivo de evitar riesgos derivados o causados, como vimos tras el caso Facebook/Cambridge Analytica.

En segundo lugar, transparencia. La Comisión considera que las regulaciones *offline*, como la transparencia, la limitación de gasto, las jornadas de reflexión o el tratamiento equitativo por parte de los medios, no se encuentran suficientemente garantizadas *online*. En este sentido, y ya en abril pasado, lanzó un conjunto de medidas para combatir la desinformación en línea. Como resultado de ello, en septiembre se firmó un código de conducta y buenas prácticas que compromete a las plataformas y a la industria publicitaria. Ahora realiza una serie de recomendaciones —insisto, recomendaciones— que

cve: DSCG-12-CM-120

incluyen la necesidad de que partidos políticos, fundaciones y organizaciones electorales informen a la ciudadanía de los fondos invertidos en publicidad electoral *online*; que informen de qué partido o grupo político de apoyo se encuentra tras las publicidad política *online* y cómo y a quién se dirige la llamada publicidad *targuetizada*.

Junto a ello, la cooperación europea y nacional. Al objeto de detectar potenciales riesgos, incluyendo potenciales amenazas híbridas, recomienda la puesta en marcha de una red de cooperación electoral europea sobre la base de cada red electoral nacional; una red nacional que recomienda que esté integrada por autoridades con competencia en asuntos electorales *offline* y *online* y de puntos focales nacionales que deberían ser creados en cada Estado miembro.

En cuanto a la ciberseguridad, la Comisión recomienda medidas organizacionales y técnicas para gestionar los riesgos de seguridad en las redes y en los sistemas en el ámbito y en el contexto electoral.

Por último, multas. La Comisión propone sanciones financieras, hasta del 5 % del presupuesto del partido político o fundación, y la imposibilidad de recibir subvenciones del presupuesto general de la Unión, en el caso de infracciones al Reglamento General de Protección de Datos si se ha producido una intención de manipular.

Con todo ello, la Comisión busca tener una hoja de ruta en la materia y está trabajando, junto a diferentes instancias del Consejo, en un plan de acción que tendrá que presentar el próximo mes de diciembre.

Para terminar, me quiero referir muy brevemente a las amenazas híbridas, un término que para muchos es una metáfora, que trae al primer plano todas las complejidades y dilemas de ese desafío del que hablaba Kissinger. Podemos definirlas, y para ello voy a optar por la definición reflejada en nuestra Estrategia de Seguridad Nacional, como acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones o campañas de manipulación de la información o elementos de presión económica y financiera. La estrategia reconoce que estamos ante un tipo de amenaza que compromete o puede comprometer la seguridad nacional y que, además, es ambigua y difícilmente atribuible. Y me permitiría añadir que, además, es difícil de reconocer.

Desde el Ministerio de Asuntos Exteriores abordamos esta cuestión a través, principalmente, de dos vías. Por una parte, en la Unión Europea, a través de la participación en el Grupo de la Presidencia para contrarrestar las amenazas híbridas, que ha visto prorrogado su mandato hasta 2020; por otra parte, con nuestra presencia en el Centro Europeo de Excelencia para contrarrestar las amenazas híbridas, con sede en Helsinki, y del que somos miembros fundadores.

En cuanto a la Unión Europea, el gran salto se produce con la aprobación en abril de 2016 del marco conjunto para combatir esa amenaza. La Unión Europea reconoce la dificultad de homogeneizar su definición y que, al estar en relación directa con la seguridad y defensa nacionales, y siendo las vulnerabilidades específicas de cada país, su combate constituye una responsabilidad primaria de los Estados miembros. Sin embargo, pueden ser abordadas de manera más eficaz a través de una respuesta coordinada a escala europea. De ahí que plantee, a través de veintidós acciones concretas, elevar la conciencia sobre la misma y contribuir a mejorar nuestra resiliencia. Estas medidas tienen cuatro objetivos básicos, entre los cuales están ayudarnos a reconocer la naturaleza híbrida de la amenaza, para lo que recomienda trabajar en conciencia situacional y en monitorizar posibles riesgos. Para mejorar esta conciencia se crea la célula de fusión híbrida para compartir inteligencia e intercambiar información; es una célula que ya esté en pleno funcionamiento en el Centro de Situación de Inteligencia de la Unión Europea. Se reconoce también la necesidad de consolidar la comunicación estratégica y se propone la creación del centro de Helsinki. Además, continuar construyendo resiliencia europea, entendiendo como tal nuestra capacidad para prevenir, responder y recuperarnos de las crisis, protegiendo las infraestructuras críticas y adaptando las capacidades de defensa de la Unión y aumentando nuestra ciberseguridad.

Con la evolución de los acontecimientos, y en especial tras el ataque de Salisbury, el Consejo Europeo de junio pasado reiteró la necesidad para la Unión Europea de seguir potenciando sus capacidades frente a esta amenaza, lo que da lugar a una nueva comunicación conjunta que sus señorías deberán enmarcar junto a los esfuerzos de los que ya hemos hablado en materia de ciberseguridad y en materia de desinformación. Una nueva comunicación que constituye el marco actual en el que estamos trabajando. Esta comunicación, como digo, da un paso adelante e intensifica la respuesta en los siguientes campos. Se fortalecen los ámbitos de inteligencia con un reforzamiento de la célula de fusión y sus competencias se amplían a los riesgos nucleares, biológicos, químicos y bacteriológicos, a la contrainteligencia, al ciberanálisis, así como a la desinformación reconociéndola como un riesgo para nuestras democracias.

cve: DSCG-12-CM-120

Se refuerza la comunicación estratégica de manera que se busque una difusión de una información más coherente a través de las tres *StratCom Task Forces*.

Por otra parte, el Centro Europeo de Excelencia para contrarrestar la amenaza híbrida surge en el contexto al que nos acabamos de referir. No solamente es el resultado de una decisión del Consejo Europeo, sino también de la Declaración de Varsovia, en la que el secretario general de la OTAN, el presidente de la Comisión y el del Consejo animan tanto a socios como a aliados a su creación. El documento constitutivo se firmó en abril del pasado año en Helsinki, con la participación inicial de doce países, y la UE y la OTAN actúan como organizaciones invitadas. Hoy el centro reúne a un total de dieciocho Estados miembros. Este centro pretender ser una referencia para combatir las amenazas, fomentar y difundir una comprensión común de las mismas y promover el desarrollo de una respuesta integral y transversal, a escala nacional, en todos los niveles de Gobierno, coordinada con la OTAN y la Unión Europea. A nuestro juicio, se trata de un centro necesario por la inexistencia de institución internacional específica alguna que trate en exclusiva esta cuestión y por poner en práctica la colaboración Unión Europea-OTAN para hacer frente a este tipo de amenaza que, sin duda, constituye la esencia de los conflictos del siglo XXI.

Voy a finalizar aquí. A modo de conclusión, permítanme reiterar que nos enfrentamos a amenazas de tipo complejo que, como hemos visto, requieren también de soluciones complejas; amenazas que tienen un carácter transversal, a veces difuso, incluso ambiguo, y que, por tanto, exigen que nuestra perspectiva sobre las mismas, la forma en que queremos combatirlas, contemple al conjunto de la sociedad, lo que los ingleses llaman un *whole of society approach*, es decir, una perspectiva integral que se complementa igualmente con el esfuerzo del conjunto del Estado y con la coordinación y colaboración a todos los niveles, tanto a escala nacional como internacional o multilateral.

Muchas gracias por su atención. Quedo a la espera de las preguntas que sus señorías quieran formularme.

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

Vamos a dar la palabra ahora a los distintos grupos parlamentarios presentes en la sala, empezando por el Grupo Parlamentario Confederal de Unidos Podemos-En Comú Podem-En Marea.

Tiene la palabra la señora Angustia.

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

Gracias, señora embajadora. Bienvenida a esta Comisión y muchas gracias por su comparecencia y por la claridad al exponer el inicio del marco de trabajo en el que la misión especial para amenazas híbridas y seguridad debe moverse. Voy a empezar por un par de cuestiones respecto a lo que corresponde a nuestro Estado para pasar a partir de ahí al marco de coordinación de la Unión Europea y de la OTAN. Evidentemente, supongo que lo primero que hace cuando llega al puesto en el mes de marzo es una valoración de Estado o informarse de lo que los diferentes organismos hacen en materia de ciberseguridad y amenazas híbridas. Entiendo que se trataba no solo de conocer el trabajo del Centro Criptológico, del Centro Nacional para Protección de Infraestructuras Críticas, del Mando Conjunto de Ciberdefensa, etcétera, sino, además, saber cuáles eran las posibilidades de coordinación entre diferentes organismos y la nueva misión especial. ¿Cuáles son los puntos fuertes, ya que todavía tendrá fresca esta primera tarea de recopilación de responsabilidades y acciones conjuntas? ¿Cuáles cree que son los puntos fuertes de nuestro sistema en el marco de la ciberseguridad? También nos gustaría saber si cree que tenemos una estructura que resulte útil y efectiva en dos vías: en primer lugar, para combatir de forma coordinada con todos los agentes implicados en el marco de la ciberseguridad y las amenazas híbridas; en segundo lugar, si tenemos la posibilidad en nuestro sistema de actuar de forma sincronizada para que sean efectivas.

A lo largo de todas las comparecencias, en esta ponencia de ciberseguridad, probablemente el punto de mayor acuerdo haya sido no solo la potencialidad que tiene nuestro sistema, sino la que tiene nuestro Estado para ser desarrollador de tecnología propia para contribuir al campo de la ciberseguridad. ¿Qué cree que debemos avanzar para que esta capacidad se desarrolle de forma efectiva y podamos ser no solo un espacio con potencialidad de sistemas, sino que podamos desarrollar nuestra propia tecnología?

A partir de aquí, me voy al marco de la Unión Europea. La figura de la misión especial para amenazas híbridas y ciberseguridad aparece ya si no en todos los países del marco de la Unión Europea, en casi todos. ¿Cuáles son los marcos de trabajo que tiene fijados esta misión, con sus espacios equivalentes en otros Estados, y cuáles son los niveles de coordinación propios que se exigen a esta responsabilidad?

cve: DSCG-12-CM-120

Centrándome también en el marco de la Unión Europea, parece evidente que tras los pasos dados desde el mes de septiembre en el Parlamento Europeo, sobre todo a través de los espacios conjuntos que se delimitan en el llamamiento del país, cada vez vamos a hablar más de una normativa conjunta, de una normativa de Gobierno para el ciberespacio en dicho marco de la Unión Europea. ¿Cuáles son los cambios que para nuestros sistemas y nuestras estrategias supondría esta necesidad de normativa conjunta o qué vías de coordinación empezarían a ser efectivas en esta normativa de Gobierno del ciberespacio?

Le pregunto exactamente lo mismo en el marco de la OTAN. Existe un marco de coordinación y de seguridad, que parece muy diferente en los distintos Estados, que de alguna forma nos obliga a tener determinados espacios de política conjunta. ¿Cuáles son las posibilidades a partir de aquí con todos los cambios y avances que sobre todo en el último año se han producido en este marco? ¿Cuáles son los pilares fundamentales en los que parece que podemos avanzar juntos en un marco de estrategia dentro de la OTAN?

Si hablamos de seguridad ciudadana, la comparecencia ha estado muy centrada en el marco de defensa, pero parece que es imposible alcanzar estándares de ciberseguridad y de protección contra las amenazas híbridas sin la colaboración ciudadana. ¿Cuáles son las limitaciones y, por tanto, cuáles son los esfuerzos de una sociedad formada, informada, implicada en materia de ciberseguridad? ¿Cuál es exactamente el nivel de coordinación que encuentra la misión en este momento en el marco de las empresas y de la actividad privada, que será primordial para hacer esa coordinación de trabajo efectivo?

Si hablamos en términos de amenazas híbridas —vuelvo al marco puramente internacional—, desde el punto de vista de la embajadora de la misión, ¿cuáles son las principales amenazas que tienen en este momento tanto de la Unión Europea como la OTAN?

A continuación, le hago la última pregunta. ¿Cree —supongo que no es la primera vez que se la hacen, pero creo que es interesante conocer la respuesta de la embajadora— que la defensa y la resiliencia siguen siendo el marco de trabajo de la ciberseguridad o tenemos que empezar a entender otro tipo de capacidad y, por tanto, ampliar esos marcos de trabajo en este campo?

Nada más. Muchas gracias.

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

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

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

Gracias, señora embajadora, por su exposición, por la amplitud de la misma, incluso por su nombramiento, porque de alguna manera es reciente, ya que fue hace ocho meses, en marzo de este año. Su nombramiento denota, además, el interés y la importancia que dan los Gobiernos de España —también el hecho de que usted esté hoy aquí— a la materia que atañe a esta Comisión, a la ciberseguridad, a las ciberamenazas, a la ciberdefensa. Por tanto, le doy la enhorabuena por su trabajo y por la exposición que ha hecho, que ha sido muy amplia.

Usted ha tratado mucho temas, y me permitirá que me centre en uno de los que ha tratado al final de su intervención, y en el que he visto, según algunas intervenciones suyas que he podido escuchar en otros foros, que es una experta, al menos una conocedora más profunda de lo que podamos ser algunos de los presentes en esta Comisión y, desde luego, yo mismo. Me voy a referir en concreto, porque no quiero perder la oportunidad —un principio de oportunidad que en ocasiones los políticos solemos aprovechar— que nos da tenerla hoy aquí, a la modalidad de las ciberamenazas relacionadas con las acciones de desinformación en línea. La he escuchado hablar sobre este tema en varios foros, en el Foro del Consejo Atlántico, también en unas jornadas del Mando de Ciberdefensa, y a mi grupo le interesa especialmente que nos ilustre sobre este tema en la medida de sus posibilidades, y sin que esto suponga ningún compromiso. Usted es diplomática y no va a tener ningún problema en hacerlo, seguro que con muchísimo acierto. Fundamentalmente me gustaría que nos informe sobre el estado de la cuestión en este momento. Tenemos recomendaciones de la comisaria Gabriel que, en principio, no se concretan en la necesidad de legislar sobre el tema, pero que en otro momento hablan de la posibilidad de legislar sobre el tema. Situación en relación con las próximas elecciones europeas. Usted ha hecho referencia a la guía, al discurso de Juncker y a la patata caliente que de alguna manera la Comisión pasa a los Estados para decir: Son ustedes los que en este momento tienen que poner en marcha las medidas para evitar que haya una injerencia en esas elecciones europeas. Quisiéramos saber si es posible conocer el estado de la cuestión en España, si es que usted lo conoce.

cve: DSCG-12-CM-120

Ha mencionado la iniciativa que han adoptado algunos Estados sobre legislar acerca de este tema, concretamente el Gobierno francés, del presidente Macron, ha presentado una proposición de ley. ¿Considera usted que este es un camino adecuado? ¿Recomienda que este sea un camino que pueda explorar el Gobierno de España? Esto nos vendrá muy bien para las recomendaciones que pretendemos hacer al Gobierno de España.

Ciberataques o injerencias, sin sujeto estatal, al menos, identificado. En principio, como usted ha dicho, sin que se le haya atribuido a un autor estatal, en el caso de los Países Bajos se ha expulsado a diplomáticos de determinado país. ¿Cómo responder ante esta situación con el corsé que supone el derecho internacional?

Por último, acuerdo entre el Reino de España y Rusia respecto a la creación de un grupo de trabajo para abordar la expansión de las *fake news*. Ha dicho usted —además, está muy bien—: No soy la embajadora de las *fake news*. No pretendo adjudicarle ese título, pero lo que es evidente es que este tema nos preocupa. Pero hay que partir de la base de que ni todo son *fake news*, ni todas las *fake news* tienen como objetivo vulnerar la estabilidad o los procesos democráticos, ni todas las *fake news* tienen una estrategia deliberada y, por tanto, se confunden muchas cosas en relación con este tema. Yo me refiero a esas que sí tienen una estrategia, que sí tienen una intención deliberada de cambiar relatos —le visto poner el ejemplo de Lituania—, de enfrentar a comunidades dentro de países, etcétera. Quisiera saber qué nos puede contar respecto a ese grupo de trabajo.

Nada más. Muchas gracias. Estoy seguro de que sus respuestas van a ser útiles para esta Comisión.

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

Tiene la palabra el señor González Taboada.

El señor **GONZÁLEZ TABOADA:** Muchas gracias, señor presidente.

Señora embajadora, muchas gracias por acompañarnos en el día de hoy. Le doy la bienvenida en nombre del Grupo Parlamentario Popular. En primer lugar, quiero felicitarla. Decía el compañero del Grupo Socialista que lleva pocos meses y, aunque esto corre muy deprisa seguro que el trabajo que ha ido haciendo ha ido dando sus frutos. A mí me preocupan algunas cosas. Parto de la base de que nos ha expuesto el tema de una manera muy clara y muchas de las dudas que venía a expresarle las ha ido aclarando, cosa que le agradezco. Como usted decía, es una materia compleja, un tema muy delicado, muy sensible y hay argumentos que voy a exponer que me gustaría que nos ampliara.

Entiendo de sus palabras que el centro que usted dirige tiene entre sus principales cometidos reforzar la ciberseguridad como desarrollo profesional en un sector de empresas de calidad. Pero la Estrategia Nacional de Seguridad que se aprobó, creo, en diciembre de 2017, subraya que la guerra híbrida está en peligro creciente y dice de manera textual: Los ciberataques, las operaciones de manipulación de información y elementos de presión económica; y apunta que se manifestaba especialmente en procesos electorales. Lo de los procesos electorales me preocupa especialmente. Antes decía usted que para el año que viene están previstos en torno a veinte procesos en la Unión Europea; pocos me parecen teniendo en cuenta que en España vamos a tener un buen número de ellos. Me preocupa que cualquier ciudadano, escuchando las palabras que hoy se están pronunciando aquí o con las que lea en los medios de comunicación, pueda entender que a través de las *fake news* se pueda vulnerar un proceso electoral o que se puedan cambiar voluntades, entendido como lo digo, sin que nadie saque punta a esta expresión. No tengo la más mínima duda de que el Gobierno estará trabajando en esta materia, no solo en el ámbito estatal, sino también en el europeo y en el internacional. Deberíamos explicar de manera clara a los ciudadanos qué son las *fake news* y en qué pueden afectarles.

Detrás de los ciberataques hay organizaciones criminales, no nos vamos a engañar, que están muy organizadas, que operan a nivel internacional, con el interés de desestabilizar Gobiernos. Me gustaría saber cómo afronta España este problema, sobre todo con qué medios podemos hacerlo, ya no tanto económicos, sino sobre todo personales. Quisiera que me aclarara si la oficina para las amenazas híbridas lleva a cabo tareas de investigación y análisis compartidas con otros países, si se coordinan con el resto de países. Me refiero a ello porque entiendo que dichas amenazas no serán tratadas igual en función de lo vulnerable que pueda ser un país, incluso de la ingobernabilidad de cada uno de los países.

Recientemente —lo decía el compañero del Grupo Socialista— se ha suscrito un acuerdo entre los Gobiernos ruso y español, y el ministro Borrell mostraba su especial preocupación por la difusión de noticias falsas respecto a Cataluña. Por lo que he leído, parece que son dieciocho países los que han mostrado ya que hay manipulación, por decirlo de alguna manera, del electorado en Internet. Por ejemplo,

cve: DSCG-12-CM-120

solamente desde 2015 están probados ya 3900 casos de desinformación favorable al Kremlin. Me gustaría que nos ampliara —antes lo ha expuesto, quizá de una manera más somera— en qué se está trabajando en conjunto con la Unión Europea para que los próximos comicios europeos sean lo más limpios posible, lo más transparentes posible, ya no sólo en España sino en el conjunto de la Unión Europea, puesto que, al ser unos comicios europeos, a todos nos interesa, sobre todo, la máxima limpieza, el máximo rigor y que no pueda ocurrir nada en este sentido.

Le decía antes que entiendo que el Gobierno seguro que está trabajando en el tema de las *fake news*. Al hilo de esta cuestión, algunos países ya están implementando medidas legislativas en su legislación. Me gustaría saber si España está trabajando en este sentido y, si es así, si hay algún grupo —lo desconozco— creado a tal efecto en el Congreso y el Senado para poder trabajar en un tema tan sumamente delicado.

En julio de este año se ha aprobado también por parte de la OTAN —se refería a ello la compañera de Podemos— el nombramiento de dos nuevos mandos, uno creo recordar que en Alemania y otro en Estados Unidos, con la creación de treinta batallones y treinta escuadrillas aéreas. Me gustaría saber si por parte del Gobierno de España se debe dotar de miembros a estas escuadrillas y batallones, teniendo en cuenta que como miembros de la Organización Atlántica que somos deberíamos hacerlo, aunque me parece un número muy pequeño, considerando el número de países. No sé si ello significa que no todos tienen que aportar.

También ha hablado usted de la colaboración en seguridad nacional, defensa y mantenimiento del orden público con el resto de los países. Hay dos materias que me preocupan, la fronteriza y la referida a redes, que son muy propias de cada país. Entiendo que las comunidades autónomas no tienen ningún tipo de competencia en esta materia, pero me gustaría saber si hay alguna labor de coordinación por parte del Estado con ellas, sobre todo en materia fronteriza.

En España en 2017 se han producido cerca de 27 000 ciberataques, lo que supuso un 26 % más que el año anterior. Me gustaría saber cómo vamos en el ejercicio 2018, si se puede tener ya algún dato o se puede avanzar algo en este sentido. También me gustaría saber, como máxima responsable que es usted en la materia, dónde considera que está la mayor amenaza en estos momentos en cuestión de ciberataques o ciberseguridad en nuestro país.

Le agradezco su presencia hoy aquí con nosotros, la exposición de todo lo que nos ha contado y, si nos puede aclarar algunas de las dudas, se lo agradeceríamos; si no, en futuras ocasiones o cualquier otro día, podríamos comentarlo. Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor González Taboada.

Tiene la palabra la señora Olmo.

La señora **OLMO ROMERO** (embajadora en misión especial para las amenazas híbridas y la ciberseguridad): Muchas gracias, señor presidente.

Son muchos temas, y voy a ver cómo trato de dar respuesta a todos ellos.

Para contextualizar bien mi labor y mi trabajo y cuál es el sistema de gobernanza en España, diré que hay muchos modelos y que el español es uno descentralizado, con un conjunto de instituciones que tienen competencias determinadas. Por una parte, tenemos el Centro Criptológico Nacional, dependiente del Centro Nacional de Inteligencia, que además se constituye en el centro de respuesta a incidentes de la Administración y del sector público. Tenemos el Instituto Nacional de Ciberseguridad, con sede en León, que se dedica a tres cuestiones importantes: al fomento de una industria tecnológica; en segundo término, a ser el centro de respuesta a incidentes para la industria, junto con el Centro Nacional de Infraestructuras Críticas, y, en tercer lugar, a lo que se denomina alfabetización mediática, cuestión que creo que alguna de sus señorías ha señalado. Tenemos también al mando conjunto de ciberdefensa —y aquí quiero distinguir entre lo que es ciberdefensa y ciberseguridad: ciberdefensa son las capacidades ciber para defender el país, y la ciberdefensa puede y debe llevar implícita ciberseguridad y ser cibernéticamente segura pero tiene unos planteamientos distintos de lo que propiamente es la ciberseguridad— y tenemos también el Centro Nacional de Protección de Infraestructuras Críticas, además de la Secretaría General de Administración Digital, que desde hace tiempo intenta avanzar en ese gobierno electrónico, y todo ello apoyado por el departamento de seguridad nacional, donde nos reunimos de manera colectiva en el Consejo Nacional de Ciberseguridad, que preside el director del Centro Nacional de Inteligencia. ¿Qué quiero decir con esto? Que tenemos un modelo colegiado, un modelo descentralizado, donde se exige la coordinación estratégica y política en este ámbito. Ahora bien, me dirán que los incidentes no esperan a

cve: DSCG-12-CM-120

coordinaciones de este tipo. Es decir, hay un trabajo conjunto permanente de lo que llamamos CERT, centros de emergencia de respuesta a incidentes, que trabajan veinticuatro horas sobre veinticuatro horas. Así, tenemos el CERT del Centro Nacional de Inteligencia, responsable de los ataques a la Administración, el del CNPIC para las infraestructuras críticas, y el del Incibe para la industria, y hay un trabajo conjunto, que creo que algún compareciente anterior explicó con motivo del WannaCry. ¿Cuál es mi papel? Yo me siento en ese consejo. Ahora bien, no tengo un perfil técnico, como habrán visto —soy diplomático—, aunque tampoco es labor del ministerio entrar en esos tecnicismos. Se trata de que esa arquitectura nacional esté inserta en los modelos europeos y se coordine con los de nuestros socios, y, por otra parte, de ver por dónde va el mundo en esta materia, lo que exige un notable esfuerzo —creo que lo hablaba antes con alguna de sus señorías— en un cambio de mentalidad, un esfuerzo de adaptación a un espacio nuevo, que no solo está regido por Estados, en el que se diluyen las fronteras e intervienen casi como pares y al mismo nivel individuos, industria, etcétera, lo que, por tanto, exige un permanente estar en lo internacional para entre todos intentar hacer frente a estos desafíos, porque, en definitiva, son desafíos comunes. ¿Qué es diferente? Son diferentes las vulnerabilidades, cada país tiene un tipo de vulnerabilidad. El nivel económico, de prosperidad, la organización política, los procesos sociales aportan diferentes fortalezas pero también diferentes vulnerabilidades.

Hecha esta introducción, me han preguntado en algún momento por las principales amenazas. Me permito decir —y esta es una opinión personal— que España no sufre amenazas específicas por ser España. Nuestro país está inserto en un contexto y sufre el mismo tipo de amenazas que otros países de nuestro entorno. En este sentido, dos de sus señorías han hecho referencia al acuerdo con el ministro ruso, y esto sí me interesa aclararlo. El ministro de Asuntos Exteriores se reunió el pasado 6 de noviembre con su homólogo ruso. Fue una reunión habitual sobre consultas políticas bilaterales, en el marco de dos países que mantienen relaciones estables y fluidas. Es verdad que el ministro Borrell expresó a su homólogo la extrema preocupación por las campañas o la desinformación y manipulación de la realidad en las redes sociales, sobre la situación política en Cataluña, cuestión que considerábamos especialmente grave, porque se habían difundido noticias que podían haber venido de medios de titularidad estatal. El ministro trasladó al señor Lavrov que España nunca había imputado directamente a las autoridades rusas, si bien existe evidencia abundante de que estas campañas provenían o tenían su origen en territorio ruso. Lavrov declinó esta situación, señaló que se situaba en el marco del contexto de creaciones artificiales contra Rusia, pero el ministro reiteró la preocupación y la extrema gravedad. Al objeto de evitar que posibles futuros ataques híbridos, en ausencia de un canal especializado directo para tratarlo, pudieran dañar la relación bilateral, se habló de la creación de un grupo de trabajo *ad hoc*. Es decir, no se trata de un acuerdo, no se trata de un grupo estable de coordinación en materia cibernética. Sería un grupo que eventualmente estaría formado por funcionarios especializados, como marco, como puerta abierta, como vía para evacuar consultas en caso de que se produjera algún tipo de incidente. Por tanto, la prioridad era acabar con estas actividades ilícitas de las que hemos hablado, y se trata —quiero ser muy clara al respecto— de un instrumento adicional, no de un instrumento estable. No se trata de un acuerdo, ni formal ni informal, sino de la posibilidad de establecer y tener este canal abierto, para que en caso de que fuera necesario se pudiera utilizar. Y esta misma información la proporcioné el pasado jueves al Consejo Nacional de Ciberseguridad, puesto que teníamos un interés especial en que estos términos fueran conocidos y esto fuera tomado en consideración.

Hablaba la representante de Podemos de las posibilidades de coordinación. En el ámbito técnico, creo que hacemos un ejercicio de coordinación importante, eficaz y que ha demostrado resultados. Mis colegas de otros organismos —colegas de consejo pero que, en definitiva, pertenecen a un mundo técnico— están orgullosos del efecto y de la actuación que tuvieron las diferentes instituciones españolas con motivo de los ataques del *malware*, especialmente del WannaCry. Estamos sincronizados, además no solamente a nivel nacional, sino que hay una comunicación permanente —la directiva NIS obliga a ello, a establecer esa coordinación— con el centro europeo de respuesta de la Unión Europea, el cual, a su vez y en el marco de la declaración conjunta Unión Europea-OTAN, también tiene coordinación con el centro de respuesta de la OTAN. Por lo tanto, desde el punto de vista técnico, desde el punto de vista de los ataques cibernéticos a diferentes escalas, hay un trabajo, pero no solamente un trabajo sobre el papel, puesto que hay una formalización y unos protocolos, sino que también es una realidad. Y no sólo eso, la coordinación no solamente tiene un carácter institucional entre los organismos técnicos, sino que también, como he explicado antes, se está trabajando en Europa en un modelo de gestión de crisis en este terreno. ¿Por qué? Piensen ustedes en que en este ámbito tenemos que sumar manzanas con manzanas, y lo que

cve: DSCG-12-CM-120

nosotros llamamos incidente a lo mejor otros lo consideran un ataque, por lo que es muy importante que tengamos y compartamos una taxonomía común, para que sepamos de lo que estamos hablando y, en definitiva, en este terreno hablemos de lo mismo.

En cuanto a la potencialidad del desarrollo tecnológico, he hablado ya del reglamento que presentó la Comisión en septiembre. Es un reglamento novedoso, que nos ha llamado la atención a todos los Estados miembros porque sale un poco de repente y casi diría que cuando quedan pocos meses para el final de la legislatura en Europa, pero es un reglamento que aporta enormes posibilidades. Es verdad que existe un convencimiento de que Europa es importador neto de productos, y, por lo tanto, la reacción de la Comisión ha sido la de juntar el presupuesto en un único centro. Estamos hablando de un presupuesto muy interesante, un presupuesto, por ahora y hasta que no se aprueben las perspectivas presupuestarias de la Unión, cercano a los 2700 millones hasta 2027, que, obviamente, también va a exigir unas ciertas contrapartidas presupuestarias nacionales. Pero ¿de qué se trata? De que no se dupliquen esfuerzos tecnológicos entre los Estados miembros, de que se trabaje con un plan tecnológico común para avanzar en una autonomía estratégica y poder realizar proyectos transnacionales en esta materia, que hasta ahora no se han venido haciendo.

Sobre ciudadanía, creemos que es uno de los elementos fundamentales no solamente en el ámbito de la ciberseguridad, sino también en el de la desinformación. En el ámbito de la alfabetización digital, Europa está avanzando y nosotros también. Es responsabilidad primaria del Instituto Nacional de Ciberseguridad. De hecho, hemos trabajado, junto con el instituto, la Organización de Estados Americanos y el BID en iniciar una cosa que llaman los *ciberchallenges*, los ciberdesafíos. Se trata de contribuir a crear entre adolescentes y universitarios una preparación y un interés por este tipo de formación. Pensemos además que es un mercado laboral en auge. Por tanto, es muy importante que avancemos en ello tanto desde el punto de vista de la desinformación, como desde el de la propia seguridad de nuestras sociedades, así como desde el punto de vista del mercado laboral.

Respecto a la desinformación, me gustaría muchísimo ser una experta al respecto. Es verdad que cuando me nombraron los medios de comunicación lo recibieron en esa dirección, recuerdo ese titular referido a embajadora contra las *fake news*. Dicen los expertos que una *fake new* no hace desinformación, que esta se produce cuando se provoca un conjunto de *fake news* en el marco de una estrategia y con un objetivo concreto, ya sea desestabilizar, crear polarización, etcétera. Sinceramente, hay muchos orígenes en la desinformación. Los expertos dicen que incluso hay bases de carácter casi antropológico. Hay quienes dicen que el espíritu crítico de la Ilustración nos ha llevado a dudar de todo. Por otra parte, casi diría que la digitalización, esa hiperconectividad sitúa a cada ciudadano en un medio de comunicación en sí mismo, sitúa a las redes sociales a la vanguardia de nuestra información, realmente nos sitúa en un mundo nuevo y en un contexto nuevo.

Es verdad que la Comisión —esta es una opinión personal— recibió en un primer momento algunos comentarios acerca de que no podía ir más allá. Había elementos como el derecho a la privacidad y el derecho a la libertad de expresión, el poder que hoy tienen las plataformas y los servicios digitales que estaban en juego. Recuerdo que por el mes de marzo, cuando me nombraron, la comisaria Gabriel dijo que la Comisión no iba a legislar sobre esta materia y que era responsabilidad de los Estados. Posteriormente la Comisión creó un grupo de expertos, en el que participaron algunos periodistas españoles, junto a periodistas de otros Estados miembros, que hizo una serie de recomendaciones a la Comisión a la vista de la situación. Entre las conclusiones de ese grupo de expertos se hablaba de la creación de un código de buenas prácticas que incluyera a las plataformas y a la industria publicitaria, se hablaba de la creación de un sistema de *fake checkers* independiente, de manera que hubiera una especie de red independiente de verificadores de información sobre la velocidad de los asuntos; se hablaba de la alfabetización digital, de la alfabetización mediática; se hablaba del interés compartido por todos de avanzar y mejorar en un periodismo de calidad y, obviamente, de compaginar todo ello con la ciberseguridad. Y este resultado del grupo de expertos se tradujo en una comunicación de la Comisión y en una serie de recomendaciones. El tiempo avanza y ya no es solamente la comisaria Gabriel la que está en ello, es decir, también está el comisario King en Seguridad, la comisaria de Justicia y el comisario de Interior. ¿Qué quiere decir esto? Que la seguridad de los contextos de los procesos electorales no es una cuestión solamente de una parte de la sociedad, de un comisario o de una parte de la Comisión. Se llega al convencimiento de que esta es una cuestión integral de seguridad, derechos, deberes, obligaciones, libertades, industria, etcétera. Así se saca este conjunto de recomendaciones al que me he referido, recomendaciones que tienen un distinto valor jurídico y que probablemente tendrán distinta

cve: DSCG-12-CM-120

implementación. Recordemos que tenemos veintiocho o veintisiete procedimientos electorales distintos en Europa: unos de carácter más tradicional, en papel, con cuentas y actas firmadas; otros totalmente digitalizados; unos con sistemas electorales en el exterior, con circunscripciones, y otros no. Por lo tanto, la Comisión no puede ir al detalle, primero porque es una cuestión soberana de los Estados, y, además, por esa diferente concepción de cada proceso electoral. La Comisión lo que hace es dar recomendaciones. En ese marco, hay una enmienda legislativa en referencia a la posibilidad de establecer multas por la falta de respeto al Reglamento de Protección de Datos, y lo demás por el momento se mantiene a nivel de recomendación; pero, en ese plan de acción que presentará la Comisión en diciembre, vamos a ver, porque podría ir más allá, o mantenerse en el nivel de recomendación.

Respecto a las comunidades autónomas, creo recordar en este momento que Andalucía, Valencia y Cataluña tienen centros de respuesta a incidentes. Son centros de carácter técnico que tienen coordinación permanente con los CERT nacionales que he señalado, y hasta la fecha no he oído que haya habido ninguna dificultad, sino todo lo contrario. La comunidad técnica tiene un espíritu de colaboración permanente, y es curioso ver cómo, independientemente del país al que pertenezcan en Europa, hablan el mismo lenguaje. Entonces, creo que hay una coordinación buena, los resultados han sido eficaces y en todos los procesos, reuniones y foros se nos encuentra. Hay un diálogo normal, habitual y técnico entre estas instituciones.

Creo que no me he dejado nada, señor presidente.

El señor **PRESIDENTE:** Muchísimas gracias, señora embajadora. Para que no siga usted con esta perplejidad, le diré que hay un segundo turno, en que los portavoces podrán expresar si ha habido alguna cuestión no resuelta, con lo cual puede estar usted tranquila.

Tiene la palabra la señora Angustia.

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

Sólo quiero agradecer a la embajadora las respuestas y, de nuevo, su primera intervención, así como desearle suerte y éxitos en el trabajo que les queda por delante.

El señor **PRESIDENTE:** Muchísimas gracias.

Tiene la palabra el señor Hernando.

El señor **HERNANDO VERA:** Gracias, señora embajadora, por sus respuestas.

Solamente dos cuestiones. Una que sí ha olvidado, relativa a su opinión respecto a la legislación francesa, cómo la valora de cara a nuestra propia legislación. Y, segundo, cómo está, si ha evolucionado algo —lo acaba de mencionar, se vio entre las recomendaciones— el tema de los *fake news checkers*, los verificadores de noticias, si se ha creado ya alguna norma sobre quién va a formar parte de esos comités de verificación, qué naturaleza van a tener, etcétera, es decir, si ha evolucionado mínimamente esa recomendación.

Muchísimas gracias por toda la información que nos ha suministrado.

El señor **PRESIDENTE:** Gracias.

Tiene la palabra el señor González.

El señor **GONZÁLEZ TABOADA:** Gracias, señor presidente. Con la venia.

Gracias, señora embajadora.

Ha dejado muy claro la diferencia entre ciberseguridad y ciberdefensa, concepto que yo no tenía tan claro al principio de la intervención. Le agradezco su claridad al respecto, al igual que en el resto de las respuestas, y, sobre todo, también en relación a la aclaración sobre la reunión del ministro Borrell con el ministro Levrov, porque es verdad que lo que se deducía de lo que yo, por lo menos, personalmente, leí en los medios de comunicación difiere mucho de lo que usted nos ha expuesto. Es una aclaración importante, sobre todo porque tampoco se puede criticar una reunión si no se tienen todos los puntos muy claros. Y sobre la alfabetización digital, un tema que me preocupa pero no había expuesto en mi intervención, nos lo ha aclarado. Por tanto, nada más que agradecerle su presencia en nombre del Grupo Parlamentario Popular, las ideas que nos ha dado y especialmente la claridad de su exposición.

El señor **PRESIDENTE:** Gracias.

¿Alguna reacción por parte de la compareciente?

cve: DSCG-12-CM-120

La señora **OLMO ROMERO** (embajadora en misión especial para las amenazas híbridas y la ciberseguridad): Gracias a todos. Gracias, señor presidente.

Efectivamente, se presentó a la Asamblea Nacional francesa un proyecto de ley. Pero había una cierta controversia en el país, puesto que no deja de ser un tema delicado, dado que afecta a las plataformas, a la libertad de expresión, puede afectar a la privacidad y afecta a la garantía de esos derechos mediante eventuales actuaciones del Poder Judicial. Sin duda —es una opinión personal— es un acto valiente. Sé que hay debates parlamentarios, no conozco al detalle su desarrollo, pero, si le sirve de ilustración, el presidente Macron el otro día, cuando inauguró el Foro de Gobernanza en Internet junto al secretario general de Naciones Unidas, decía que había dos modelos de ciberseguridad en el mundo, un modelo californiano y un modelo chino, el primero basado en el poder de las plataformas, los servicios digitales y la industria publicitaria *online* por encima de todo, y el segundo basado en el monopolio del Estado, y que entre estos dos modelos cabía un tercero, un modelo de regulación democrática, un modelo de regulación donde se garantizara todo, derechos y libertades del sector privado, y se impidiera a los actores maliciosos hacer uso de esos vectores, de esas capacidades en su favor, es decir, una capacidad democrática de las sociedades europeas para poder combatir la ciberdelincuencia, el terrorismo *online*, el lanzamiento y la difusión de mensajes de odio, etcétera, sin que ello menoscabe la libertad de expresión, la privacidad ni las posibilidades de progreso económico. No sé si es la cuadratura del círculo, pero, desde luego, como planteamiento es interesante y quizás haya que ir por ahí. Es decir, la red presenta enormes ventajas tecnológicas, económicas, políticas y sociales y, al mismo tiempo, amenazas y ventajas para los actores maliciosos para cometer actos ilícitos, ya sea en el ámbito civil, penal, político o, simplemente, por falta de respeto.

Acerca de los verificadores, es un tema interesante y ha sido propuesto por ese grupo de alto nivel, ese grupo de expertos periodistas, profesionales que hacen un periodismo tradicional, aunque no deja de ser un tema de difícil puesta en marcha. Hay una red internacional de verificadores que tiene capacidad de decidir quiénes están en esa red y está funcionando en algunos ámbitos, pero lo hace a modo de recomendación. Como decía algún estudioso, pensemos en que antes en las facultades de Periodismo se decía que la verdad es sagrada y las opiniones deseables, mientras que ahora algunos dicen que las opiniones se han convertido en verdaderas y los hechos son opinables. Por lo tanto, es ese debate, que también está sufriendo el periodismo tradicional, el que se pone de manifiesto en todas estas medidas. Es un debate sobre el que el Eurobarómetro ya ha dado datos: el 85 % de los ciudadanos menores de cincuenta años se informa a través de las redes sociales. Por lo tanto, estamos ante un panorama completamente distinto al que hemos tenido hasta la fecha. Y lo que hace la Comisión tanto con el código de conducta de buenas prácticas contra las plataformas como respecto a esta red de verificadores es avanzar —es una opinión personal— hacia un método de prueba y error, en el que todo se va a evaluar. La idea es que la Comisión haga una valoración de todo ello en diciembre, que reúna a todos los actores implicados y se presente un plan de acción, porque, como digo, creo que estamos en un contexto mundial nuevo, y, por lo tanto, estamos aprendiendo.

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

Concluimos aquí los trabajos de este día y, por tanto, se clausura esta comparecencia y esta sesión.

**Se levanta la sesión a las once y treinta y cinco minutos de la mañana.**

cve: DSCG-12-CM-120