BOLETÍN OFICIAL
DE LAS CORTES GENERALES

SECCIÓN CORTES GENERALES

XII LEGISLATURA

Serie A:
ACTIVIDADES PARLAMENTARIAS 12 de marzo de 2019 Núm. 276 Pág. 1

Otros textos

COMISIONES MIXTAS, SUBCOMISIONES Y PONENCIAS

154/000011 (CD) Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en
573/000003 (S) España.
Informe de la Ponencia.

En cumplimiento de lo dispuesto en el artículo 97 del Reglamento de la Cámara, se ordena la publicación en la Sección Cortes Generales del BOCG, del Informe aprobado por la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España, constituida en el seno de la Comisión Mixta de Seguridad Nacional.

Palacio del Congreso de los Diputados, 1 de marzo de 2019.—P.D. El Letrado Mayor de las Cortes Generales, **Carlos Gutiérrez Vicén.**

cve: BOCG-12-CG-A-276

INFORME DE LA PONENCIA PARA EL ESTUDIO DE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA

ÍNDICE

I. PRÓLOGO.

La revolución tecnológica que estamos viviendo supone un cambio de paradigma que está afectando a la economía, la industria, el comercio, el empleo, la educación y a las propias relaciones sociales. La característica más sobresaliente de estos cambios es la velocidad a la que se están produciendo, lo cual motiva que sea este proceso acelerado de cambio el más disruptivo de cuantos se han vivido en los últimos cien años. Si a ello se le une la globalidad de estos cambios que afectan a todos los países y la intensidad de los mismos, el resultado es un cambio profundo que está modificando nuestras formas de comportamiento como usuarios de esas tecnologías, como consumidores y como ciudadanos, que en los Estados democráticos toman las decisiones políticas que orientan el devenir de los países. Según datos de Naciones Unidas, a finales de 2019, el 50 % de la población mundial, 3.800 millones de personas, dispondrá de conexión a internet en lo que constituye la mayor historia de éxito en cuanto a la implantación de una tecnología nueva por su rapidez e intensidad.

Los beneficios sociales, económicos, comerciales, informativos y tecnológicos de la red son incuestionables. Como ha afirmado la Estrategia Digital de la Unión Europea que pretende lograr un Mercado Único Digital, el futuro de los países que conforman la UE pasa necesariamente por adaptarse de forma rápida a este nuevo paradigma ya que la transformación tecnológica afecta a todos los ámbitos de la vida moderna, desde la educación y el empleo hasta el sistema de protección social. Señala la UE que ese cambio ya se está produciendo, y a gran velocidad. Por ejemplo, en determinadas categorías de empleo hasta un 90 % de las funciones requiere competencias digitales. Europa ha de ser receptiva a estos cambios si quiere proteger a sus ciudadanos y darles la posibilidad de aprovechar las nuevas oportunidades que se abren. Se calcula que la digitalización de la fabricación aportará a la UE 1,25 billones de euros de aquí a 2025, y que los incrementos de productividad en el sector servicios, también serán muy importantes así como las mejoras en el sector primario a través de lo que se conoce como smart farming o agricultura conectada.

En este sentido, cuestiones tales como la confianza, la ciberseguridad y la administración electrónica serán esenciales para encarar el futuro con garantías de éxito. Según la Estrategia Digital antes citada, el Mercado Único Digital podría aportar hasta 415 000 millones de euros cada año al PIB de la UE. Por otra parte, teniendo en cuenta que en el nuevo entorno geopolítico las grandes potencias mundiales están apostando decididamente por disputar la supremacía tecnológica es evidente que ni la UE ni los Estados Miembros pueden quedar atrás en ese proceso acelerado de adaptación. Los Estados en los sistemas democráticos tienen la obligación de proteger a sus ciudadanos y crear las condiciones necesarias para asegurar sus derechos y libertades fundamentales, así como de crear las condiciones que posibiliten un desarrollo económico justo y equilibrado.

cve: BOCG-12-CG-A-276

Ahora bien, existe una preocupación constante por asegurar que ese proceso de desarrollo y de cambio de paradigma no se vea frenado por las cuestiones relativas a la seguridad en la Red. Se trata de un riesgo que se percibe puede ser crucial para el futuro del mundo en su conjunto. Por esta razón, el Foro Económico Mundial de Davos ha señalado en su «Informe de Riesgos Globales de 2019» que los ciberataques son el quinto gran riesgo mundial en nivel de probabilidad tras los fenómenos climáticos extremos, los desastres naturales, el cambio climático y el robo de datos.

Ante esta amenaza, los Estados están obligados a proteger a sus nacionales y a sus intereses geopolíticos y económicos. Por ello, la protección frente a estos riesgos es una materia que recae de lleno en el ámbito de la política de Seguridad Nacional, entendida, según afirma el artículo 3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, como la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos.

Por esta razón y debido a la trascendencia de asegurar un adecuado nivel de ciberseguridad frente a los riesgos múltiples que surgen de la Red, la Estrategia de Seguridad Nacional de 2017 señala como amenaza y desafío para la seguridad nacional la vulnerabilidad del ciberespacio*:* «Las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. El ciberespacio es un escenario con características propias marcadas por su componente tecnológico, fácil accesibilidad, anonimidad, alta conexión y dinamismo. En los últimos tiempos, las acciones negativas en el ámbito de la ciberseguridad han aumentado notablemente en número, alcance y sofisticación. Tales acciones adquieren creciente relevancia para España, un país altamente interconectado y que ocupa una posición de liderazgo en Europa en materia de implantación de redes digitales».

A este respecto, el citado documento señala la creciente actividad tanto por parte de Estados, que persiguen la expansión de sus intereses geopolíticos, como de organizaciones terroristas, grupos de crimen organizado y actores individuales. Estos actores sacan ventaja de algunas de las características del ciberespacio tales como el carácter anónimo que el ciberespacio ofrece para conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución. Como manifestaciones concretas de esos riesgos señala el robo de datos e información, los ataques ransomware y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas. Así mismo, indica que el ciberespacio es el medio para la realización de actividades ilícitas, acciones de desinformación, propaganda o financiación terrorista y actividades de crimen organizado, así como de actividades que pongan en riesgo la propia privacidad de los ciudadanos o sus derechos fundamentales a la libertad de información o a la libertad de expresión.

Especial mención merece la amenaza que suponen los ciberataques contra las infraestructuras críticas, es decir, de aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas. Se incluyen aquí las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información y de la comunicación sobre las que descansa el funcionamiento de los servicios esenciales que permiten el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento del sector público (administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnologías de la información y de comunicaciones, transporte, alimentación y sistema financiero y tributario). A este respecto, se debe tener en cuenta que la mayoría de estos servicios esenciales son proporcionados por empresas privadas, con lo cual es imprescindible una adecuada colaboración público-privada.

Por esa razón la Estrategia de Seguridad Nacional señala como objetivo prioritario de la política de seguridad nacional española la garantía de un uso seguro de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable.

Por otra parte, los informes de los organismos públicos competentes de velar por la ciberseguridad en España señalan un constante aumento de los incidentes y amenazas año a año; así el CCN-CERT, dependiente del CNI, indica en su informe sobre «Ciberamenazas y Tendencias 2018» que durante 2017 este organismo gestionó un total de 26.500 incidentes, lo cual supuso un aumento respecto a 2016 de un 26,5 %. El Centro Criptológico Nacional, en su actividad diaria, ha podido constatar que los actores estatales y los criminales profesionales continúan siendo las amenazas más importantes, al tiempo que la

cve: BOCG-12-CG-A-276

ciberguerra, los ciberconflictos y la guerra híbrida se hacen cada día más presente en el mundo, siempre apoyado por acciones en el ciberespacio.

Por su parte, las vulnerabilidades de dispositivos Internet of Things (dispositivos cotidianos conectados a Internet) han propiciado ataques disruptivos que justifican la necesidad de mejorar la resiliencia digital. Además, en 2017 se ha podido comprobar cómo a través de distintos ciberataques se ha intentado debilitar las democracias, interfiriendo en sus procesos electorales y alimentando sus conflictos internos.

El Instituto Nacional de Ciberseguridad (INCIBE), ha resuelto un total de 123 064 incidentes de seguridad en 2017, un 6,77 % más que 2016. De estos incidentes, gestionados por el CERT de Seguridad e Industria (CERTSI) operado por INCIBE, bajo la coordinación con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), 116 642 afectaron a empresas y ciudadanos, 885 a operadores estratégicos y 5.537 correspondieron al ámbito académico de la Red IRIS.

Estas cifras demuestran bien a las claras la necesidad de abordar esta materia como una política de Estado que requiere esfuerzos coordinados de muchos actores y un auténtico compromiso político y presupuestario, además de una ámbito regulatorio claro y adaptado a los cambios constantes en la materia. En definitiva, se trata de lograr que la acción de los poderes públicos, en especial del Poder Judicial y Ejecutivo, sea eficaz a la hora de perseguir y castigar todos los delitos que se cometan en el ciberespacio.

La Comisión Mixta de Seguridad Nacional entendió a principios de la presente Legislatura, la necesidad de estudiar más profundamente la seguridad en el ciberespacio como un aspecto fundamental y transversal que permita que la sociedad española afronte un futuro de cambios de forma segura y con garantías de adaptarse con éxito a este nuevo paradigma tecnológico. Por esa razón, se acordó crear la Ponencia de estudio sobre cuestiones relativas a la ciberseguridad en España. El fruto de la actividad realizada en el seno de esa Ponencia a lo largo del año y 8 meses de trabajo parlamentario es este informe.

II. ANTECEDENTES.

A) Orígenes de la Ponencia.

La Mesa y los Portavoces de la Comisión Mixta de Seguridad Nacional en su reunión celebrada el día 1 de junio de 2017, acordaron someter a la aprobación de la Comisión Mixta de Seguridad Nacional la creación de una Ponencia en su seno para el Estudio de diversas cuestiones relativas a la Ciberseguridad en España.

B) Creación por la Comisión Mixta y normas de funcionamiento.

Dicha iniciativa fue debatida y aprobada, por unanimidad, en la sesión de la Comisión Mixta de Seguridad Nacional, celebrada el día 1 de junio de 2017.

La Ponencia tiene las siguientes características:

1. La Ponencia estará presidida por el Presidente de la Comisión Mixta o por otro miembro de la Mesa que le sustituya, y formarán parte de ella tres representantes del Grupo Parlamentario Popular, dos representantes de los grupos con más de 50 parlamentarios, y uno de los demás grupos parlamentarios, quienes además podrán designar un suplente. Asimismo podrán participar en sus reuniones los miembros de la Mesa de la Comisión.

El Letrado de la Comisión Mixta asesorará a la Ponencia y redactará sus acuerdos e informes.

2. El objeto de la actividad de la Ponencia consistirá en el estudio de las múltiples cuestiones que se suscitan relativas al ámbito de la ciberseguridad.

3. Si la Ponencia decidiese realizar alguna comparecencia o solicitar datos o documentos, su tramitación se hará de conformidad con los procedimientos reglamentarios ordinarios. Las comparecencias podrán celebrarse en la propia Ponencia o mediante sesiones de la Comisión Mixta.

4. Los acuerdos que tuvieren que adoptarse en el seno de la Ponencia se ajustarán al criterio del voto ponderado en función del número de miembros de los Grupos Parlamentarios en los Plenos de ambas Cámaras.

5. El plazo para la finalización de sus trabajos concluirá el 1 de diciembre de 2017. En el caso de que la Ponencia decida elaborar un informe, dicho documento deberá ser sometido a la consideración de la Comisión Mixta de Seguridad Nacional antes de dicha fecha.

cve: BOCG-12-CG-A-276

Este plazo puede ser prorrogado hasta el final del siguiente periodo de sesiones por acuerdo de la propia Comisión Mixta.

C) Prórroga y posterior finalización de sus trabajos.

El 30 de noviembre de 2017 la Comisión Mixta de Seguridad Nacional acordó su prórroga, hasta el 30 de junio de 2018.

El 18 de septiembre de 2018 la Comisión Mixta de Seguridad Nacional acordó su prórroga hasta el 18 de abril de 2019.

El Informe de la Ponencia ha sido aprobado en la sesión de la Comisión Mixta de Seguridad Nacional del día 28 de febrero de 2019.

III. COMPOSICIÓN DE LA PONENCIA.

Coordinador:

José Manuel García Margallo y Marfil (GP)

Ponentes:

Luis Aznar Fernández (GSPP)
Joan Comorera Estarellas (SGPPOD)
Ignacio Cosidó Gutiérrez (SGPP)
Juan Antonio Delgado Ramos (GCUP-EC-EM)
Mikel Legarda Uriarte (GV-EAJ-PNV)
César Luena López (GS)
Bernat Picornell Grenzner (SGPER)
Juan Carlos José Raffo Camarillo (SGPS)
Luis Miguel Salvador García (GCs)
Ana Belén Vázquez Blanco (GP)
Jordi Xuclà i Costa (GMx)

Ponentes Suplentes:

Félix Alonso Cantorné (GCUP-EC-EM)
Emilio Álvarez Villazán (SGPS)
María Vanessa Angustia Gómez (SGPPOD)
María Jesús Bonilla Domínguez (GP)
Luis Manuel García Mañá (SGPS)
Miguel Ángel Gutiérrez Vivas (GCs)
Francisco Javier Yanguas Fernández (SGMX)

IV. SESIONES CELEBRADAS.

La Ponencia ha celebrado dos sesiones acordándose celebrar las comparecencias en la Comisión con total de 18 sesiones, realizadas en el orden y con el siguiente objeto:

28 de septiembre de 2017

— Celebración de la comparecencia de D. Joaquín Castellón Moreno, Director Operativo del Departamento de Seguridad Nacional (núm. expte. 212/000983).

16 de noviembre de 2017

— Celebración de la comparecencia de D. Alberto Hernández Moreno, Director General del Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE) (núm. expte. 212/001015).

cve: BOCG-12-CG-A-276

23 de noviembre de 2017

Celebración de las siguientes comparecencias:

— De D.ª Mira Milosevich Juaristi, investigadora principal del Real Instituto Elcano y profesora asociada de Historia de Relaciones Internacionales del Instituto de Empresa (IE University) (núm. expte. 219/000906).
— Del General de División, Excmo. Sr. D. Carlos Gómez López de Medina, Jefe del Mando Conjunto de Ciberdefensa (MCCD) (núm. expte. 219/001048).

30 de noviembre de 2017

Solicitud de prórroga de los trabajos de la Ponencia.

14 de diciembre de 2017

Celebración de las siguientes comparecencias:

— D. Janis Sarts, Director of the NATO STRATCOM Center of Excellence (núm. expte. 219/000926).
— D.ª Elvira Tejada de la Fuente, Fiscal de Sala Coordinadora en materia de criminalidad informática (núm. expte. 219/001075).

28 de febrero de 2018

Celebración de las siguientes comparecencias:

— De D. Xabier Mitxelena Ruiz, Security Iberia Lead en Accenture (núm. expte. 219/001044).
— De D. Carlos Sánchez, Director Ejecutivo y miembro de la Junta Directiva de la Plataforma en defensa de la Libertad de Información (núm. 219/000931).
— De D. Jesús Romero Bartolomé, Socio responsable de soluciones de seguridad de PwC (núm. expte. 219/001045).

12 de abril de 2018

Celebración de las siguientes comparecencias:

— De D. Fernando Picatoste, Socio Risk Advisory (Deloitte) (núm. expte. 219/001131).
— Del General de División D. José Luis Goberna Caride, Subdirector general del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) (núm. expte. 212/001203).

24 de mayo de 2018

Celebración de las siguientes comparecencias:

— De D. Pedro Pablo Pérez García, CEO Unidad Ciberseguridad Telefónica (Eleven Paths) (núm. expte. 219/001245)
— De D. Fernando Sánchez Gómez, director del Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC) (núm. expte. 212/001636).
— De D. Miguel Rego Fernández, Socio de iHackLabs (núm. expte. 219/001246).

28 de junio de 2018

Celebración de las siguientes comparecencias:

— De D. David Maeztu Lacalle, abogado especializado en Internet, propiedad intelectual y tecnología, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001288).
— De D. Carlos León de Mora, Director de la Cátedra Telefónica Inteligencia en la Red y Director del Grupo de Investigación Tecnología Electrónica e Informática Industrial (TIC-150) de la Universidad de Sevilla, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001289).
— De D.ª Yolanda Quintana, Periodista experta en ciberseguridad, autora de los libros «Ciberactivismo» (2012) y «Ciberguerra» (2016), editorial Catarata, ante la Comisión Mixta de Seguridad Nacional, para que evalúe la situación actual de los derechos de los usuarios de Internet y las supuestas campañas de

cve: BOCG-12-CG-A-276

desinformación que constituyen supuestos ciberataques en contra de organismos públicos y privados en España (núm. expte. 219/000932).

18 de septiembre de 2018

Celebración de la siguiente comparecencia:

— De D. Javier Candau, Jefe del Departamento de Ciberseguridad del Centro de Criptológico Nacional, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/001726).

9 de octubre de 2018

Celebración de la siguiente comparecencia:

— De D. Luis Fernando Hernández García, Coronel del Área Técnica de la Jefatura de Información de la Guardia Civil, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/001760).

16 de octubre de 2018

Celebración de la siguiente comparecencia:

— Del Director del Gabinete del Presidente del Gobierno para la presentación de la Estrategia de Seguridad Nacional 2017 y el Informe Anual de Seguridad Nacional 2017 (núm. expte. 212/001714).

23 de octubre de 2018

Celebración de la siguiente comparecencia:

—De D. Enrique Cubeiro Cabello, Capitán de Navío y Jefe de Operaciones del Mando Conjunto de Ciberdefensa (MCCD), para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/001793).

8 de noviembre de 2018

Celebración de la siguiente comparecencia:

— De D. Rafael Pérez Pérez, Comisario Principal de Policía Nacional y Director de la Unidad Central de Ciberdelincuencia encuadrada en la Comisaría General de Policía Judicial, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/001819).

20 de noviembre de 2018

Celebración de la siguiente comparecencia:

— D.ª 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 (núm. expte. 212/001859).

13 de diciembre de 2018

Celebración de las siguientes comparecencias:

—De D. Fernando Ruiz Pérez, Responsable de Operaciones del Centro Europeo del Cibercrimen (EC3) de Europol, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001522).

—De D. Daniel Barriuso Rojo, Global CISO: Chief Information Security Officer and Technology Risk, del Grupo Santander, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001523).

cve: BOCG-12-CG-A-276

23 de enero de 2019 (sesión extraordinaria)

Celebración de las siguientes comparecencias:

— De D. Javier de la Cueva González-Cotera, abogado y doctor en Filosofía y profesor asociado de la Universidad Complutense de Madrid, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001552).

— De D. José María Cavanillas de San Segundo, Chief Big Data & Security Officer, responsable de ciberseguridad de la empresa ATOS, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001553).

—De D. Jorge Bermúdez González, Fiscal Delegado adscrito al Servicio de Criminalidad informática de la Fiscalía General del Estado, para informar con carácter general sobre la ciberseguridad en España (núm. expte. 212/001895).

14 de febrero de 2019

Celebración de las siguientes comparecencias:

— Del Secretario de Estado Director del Centro Nacional de Inteligencia, para informar con carácter general sobre la ciberseguridad en España (núm. expte. 212/002361).

— De D. Javier Lesaca Esquiroz, doctor en Historia Contemporánea e investigador visitante en la Universidad de Columbia, para informar sobre diversas cuestiones relativas a al ciberseguridad en España mediante el sistema de videoconferencia (núm. expte. 219/001551).

— De la Subsecretaria del Ministerio del Interior, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/002362).

V. COMPARECENCIAS CELEBRADAS.

V.1. **Resúmenes de comparecencias celebradas.**

COMPARECENCIA DEL **SEÑOR DIRECTOR DEL GABINETE DEL PRESIDENTE DEL GOBIERNO Y SECRETARIO DEL CONSEJO DE SEGURIDAD NACIONAL (MORAGAS SÁNCHEZ),** PARA PRESENTAR, AL AMPARO DEL APARTADO 2 DEL ARTÍCULO 13 DE LA LEY 36/2015, DE 28 DE SEPTIEMBRE, DE SEGURIDAD NACIONAL, EL INFORME ANUAL DE SEGURIDAD NACIONAL 2015 Y EL INFORME ANUAL DE SEGURIDAD NACIONAL 2016. [Núm expte. 212/000206 (CD) y núm. expte. 713/000090 (S)]. Sesión de 14 de febrero de 2017.

Si bien es cierto que la comparecencia arriba citada fue anterior a la creación de la Ponencia de estudio, no puede soslayarse el hecho de que es procedente incluir esta comparecencia como antecedente a la creación de la Ponencia por dos razones; la primera por ser el citado alto cargo responsable de la política pública de ciberseguridad y, en segundo lugar, porque los informes a los que se hace referencia son esenciales para determinar la situación de la ciberseguridad en España. Así pues, el Director de Gabinete del Presidente, en su comparecencia del 14 de febrero de 2017, aportó datos muy relevantes entre los cuales se encuentra la estrategia de ciberseguridad nacional aprobada en 2013 ha ofrecido un extraordinario marco de coordinación y ordenamiento de la ciberseguridad en España. A este respecto, también es importante reseñar que el Consejo de Seguridad Nacional aprobó 9 planes derivados del Plan Nacional con actuaciones concretas dirigidas a alcanzar objetivos. También señala y esto es muy relevante, que en 2015 se reformó la legislación con nuevos tipos penales para combatir la ciberdelincuencia, el ciberterrorismo y los delitos de odio así como se aumentaron las acciones de concienciación y sensibilización.

A continuación, se refirió a las acciones realizadas en 2016 para incrementar las capacidades de prevención, detección e investigación y respuesta, y para garantizar la seguridad de los sistemas de información y las redes de comunicación de las administraciones públicas o del sector privado. Por ello, se cuenta ahora con un conocimiento más amplio sobre las ciberamenazas, dado el aumento de capacidades de todos los sectores en los que se trabaja, y en especial, la colaboración y cooperación del sector privado, primordialmente en el ámbito de las infraestructuras críticas, la defensa o la ciberdelincuencia y el ciberterrorismo. La colaboración internacional, fundamentalmente en el marco de la

cve: BOCG-12-CG-A-276

Unión Europea, ha posicionado a España en el mapa de la ciberseguridad como una nación avanzada en este sentido, que defiende activamente la necesidad de garantizar un ciberespacio abierto y seguro. A continuación, hace referencia a la entrada en vigor el 9 de agosto, de la Directiva de la Unión Europea sobre las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y los sistemas de información en la Unión, comúnmente denominada Directiva NIS, por su denominación en inglés, Network and Information Security.

Señala que se trata de la primera regulación global en la materia en la historia europea, pues su finalidad es el establecimiento de una política del ciberespacio en consonancia con los valores en los que se funda la Unión. Apunta al papel crucial de las redes y sistemas de información y su esencialidad en las actividades económicas y sociales, y en particular, al aumento de la seguridad como fundamento para el correcto funcionamiento del mercado interior. Concluye afirmando que esta Directiva supondrá un gran reto, pero también una excelente oportunidad para configurar las estructuras nacionales e internacionales de ciberseguridad.

A continuación, indica que el adiestramiento en esta materia resulta esencial y tiene una dimensión internacional intrínseca, y por ello señala la relevancia del ejercicio Cyber Europe 2016, organizado cada año por la Agencia Europea para la Seguridad de la Información y Redes, Enisa, bajo la coordinación nacional en España del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno.

El compareciente concluye con una referencia a la protección de las infraestructuras críticas. Señala que es esencial garantizar la seguridad, protección y resiliencia de las infraestructuras de los sectores estratégicos de la sociedad que prestan servicios esenciales a los ciudadanos, y es un desafío constante adecuar el Plan de protección nacional de infraestructuras críticas a las nuevas amenazas, punto en el que es preciso mencionar el ajuste con respecto al Plan de prevención y protección antiterrorista. Concluye afirmando que este es un sector en el que la colaboración público-privada es indispensable y la responsabilidad compartida se convierte en axioma.

COMPARECENCIA DEL **SEÑOR COMISARIO EUROPEO PARA LA UNIÓN DE LA SEGURIDAD, SIR KING,** PARA TRATAR ASUNTOS RELATIVOS A SU COMPETENCIA. [Núm. expte. 219/000233 (CD) y núm. expte. 713/000105 (S)]. Sesión de 21 de febrero de 2017.

En la comparecencia del Comisario Europeo para la Unión de la Seguridad, que tenía por objeto tratar diversos aspectos relativos a la seguridad en el ámbito de la Unión Europea, Sir King hizo amplias referencias a la situación de la ciberseguridad dentro del ámbito comunitario. A este respecto, señaló la relevancia de trabajar para garantizar que las empresas de Internet nos ayuden a localizar y acabar con el fomento ilegal de la radicalización, como por ejemplo el contenido relacionado con Daesh. La labor de la Unidad de Referencia de Internet de la Unión Europea, radicada en Europol, es muy importante a este respecto. Esta unidad ha señalado ya más de 15.000 puntos en su primera fase operativa, lo que ha dado como resultado que las empresas de Internet hayan eliminado este material en más del 92 % de los casos. La Asociación por la Industria de la Tecnología de la Información y el Foro de Internet de la Unión Europea son muy importantes para desarrollar nuevas herramientas que puedan detectar contenido ilegal, para que no puedan moverlo a otro sitio de la web, así como para ayudar a nuestra sociedad civil a combatir la propaganda extremista y violenta.

Asimismo, anunció el próximo lanzamiento por parte de la Comisión de un programa de empoderamiento de la sociedad civil de la Unión Europea. Con este fin, la Red de radicalización y centro de excelencia contribuirá a la creación de una red de organizaciones de la sociedad civil para desarrollar e impartir formación para nuestros interlocutores que trabajan en este ámbito en todos nuestros países de la Unión Europea.

Asimismo, insiste en la necesidad de trabajar también para reforzar nuestra resiliencia, para proteger nuestra infraestructura crítica, como por ejemplo, los sistemas de tecnología de la información o aeropuertos, puertos y espacios públicos —por así decirlo, los objetivos más blandos—, así como también la resiliencia de la sociedad en general. En este sentido, señala que, en febrero de 2017, la Comisión organizó la primera reunión sobre protección de objetivos blandos con los Estados miembros, con el fin de crear una red permanente para poder compartir mejores prácticas entre especialistas y acordar normas y procedimientos conjuntos. A este respecto, señala que España ha sido un país pionero en este ámbito y su experiencia, puede redundar en beneficio del resto de la Unión Europea. Continúa señalando que, en todas estas actividades, los Estados tienen que cumplir aquello que se ha acordado de forma conjunta:

cve: BOCG-12-CG-A-276

aplicar y poner en funcionamiento nuestra legislación comunitaria. La cooperación sobre seguridad solo será efectiva si se garantiza la trasposición de las normas acordadas y se llevan a la práctica.

En este sentido, insiste en que los Parlamentos nacionales desempeñan un papel clave a la hora de trasponer esta legislación comunitaria a las legislaciones nacionales. Los Estados miembros se enfrentan al desafío de trasponer la Directiva sobre el fichero de nombres de pasajeros a la legislación nacional, para que este sea operativo no más tarde de mayo de 2018. Este PNR, el fichero de registros de pasajeros, es importante para responder a la amenaza terrorista. Sin embargo, para que este fichero funcione sobre el terreno se deberá trabajar mucho porque es complejo y constituye un desafío técnico. Por ello, la Comisión se ha ofrecido a ayudar a los Estados miembros para aplicar este proceso y también ofrecer una financiación adicional de 70 millones de euros.

Para concluir, Sir King hizo referencia a la ciberdelincuencia como amenaza señalando que debemos mejorar nuestra resiliencia, contando con una línea sólida de defensa contra los ciberataques. Las amenazas son reales y pueden tener consecuencias terribles, como ha quedado de relieve, la coordinación es esencial tanto en el nivel nacional como en el nivel comunitario y, por ello, es imprescindible el apoyo al Centro de Ciberdelincuencia de Europol, para que pueda convertirse en un centro importante a la hora de coordinar nuestra lucha en esta materia. La Directiva de red y sistemas de seguridad determina el marco para la cooperación de la Unión Europea. Esta norma permitirá facilitar el intercambio de información entre los Estados miembros y también mejorará la cooperación operativa, lo que va a suponer una diferencia importante.

Señala que es necesario trabajar contra aquellos que cometen ciberataques, garantizando que las mismas normas que se aplican fuera de la Red se apliquen también en línea, dentro de la Red. Ello requiere una labor efectiva de nuestras fuerzas de seguridad, ya que no es fácil capturar a los delincuentes del ciberespacio. Las pruebas que se necesita obtener son a menudo intangibles y puede haber problemas de jurisdicción para las autoridades judiciales y de seguridad; por ello, la Comisión recibió un claro mandato político en junio del pasado año para proponer nuevas soluciones al acceso transfronterizo de las pruebas electrónicas, acordando una herramienta importante que va a permitir la cooperación transfronteriza en las investigaciones penales: la Directiva sobre la orden de investigación europea, que habría de ser transpuesta en mayo de 2017. Por último, concluye señalando que la Comisión va a trabajar con los Estados miembros para garantizar que esta transposición se realiza de forma oportuna y efectiva.

COMPARECENCIA DEL **GENERAL BALLESTEROS MARTÍN, DIRECTOR DEL INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (IEEE),** PARA INFORMAR SOBRE DIVERSOS ASPECTOS RELATIVOS AL TERRORISMO YIHADISTA INTERNACIONAL. [Núm. expte. 212/000957 (CD) y núm. expte. 713/000464 (S)]. Sesión de 14 de septiembre de 2017.

Si bien es cierto que la comparecencia del General Ballesteros se produjo ante la Comisión para tratar el fenómeno del terrorismo yihadista internacional, es interesante resaltar varios aspectos de los expuestos en esta comparecencia al estar referidos a cuestiones relativas a ciberseguridad. Así hizo referencia al entramado de medios de comunicación digitales imprescindible para poder llevar a cabo la estrategia de radicalización y para captar combatientes de los grupos yihadistas radicales. Asimismo, señala que los medios de comunicación también se utilizaron para intimidar a las poblaciones occidentales desde el ciberespacio. En este sentido, señala que en junio de 2017, el Daesh presentaba en una infografía el esfuerzo mediático realizado en los tres años de vida del califato y aun poniendo en cuestión la veracidad absoluta de las cifras que ofreció, su magnitud resulta significativa, más de 41 230 mensajes han sido emitidos en estos tres años, que se desglosan en 1670 mensajes de audio, 2880 de vídeo, 4540 comunicados escritos y 32 140 reportajes fotográficos. Para llevar a cabo este inmenso esfuerzo, el Daesh organizó 46 agencias de información y productoras con un despliegue de más de 1000 puntos de distribución. Asimismo, señala que tiene productoras en Afganistán, en Egipto, en Yemen, en Libia, en África Occidental, en el Cáucaso ruso, en Argelia, en Túnez y en Arabia Saudita, y esas productoras tienen como finalidad elaborar productos específicos para cada uno de esos territorios. Las principales productoras que grabaron las ejecuciones y narraron la vida del califato son Al Furqan, significa el criterio, considerada la más importante por la elaboración de vídeos de alta calidad en árabe y Al Hayat, la vida, que está orientada hacia los musulmanes que viven en países occidentales. Esta productora elaboró vídeos, audios y escritos en inglés, alemán y francés y en ocasiones, hasta en dieciséis idiomas.

cve: BOCG-12-CG-A-276

El Daesh dispuso además de una cadena de emisoras de radio llamada Al-Bayan, que emite en árabe con boletines informativos en kurdo, en inglés, en francés y en ruso. Por su parte, la productora de audio Ajnad elabora piezas de audio en las que se incluyen canciones vocales -las instrumentales están prohibidas para los salafistas- y los nasheeds, que son los himnos religiosos. Asimismo, señala que dispuso de un periódico semanal en árabe denominado Al Naba, en el que una semana después de los atentados de Barcelona y Cambrils se publicaba un reportaje sobre los mismos y amenazaba a toda España. Indica que también es importante el papel de Telegram, continúa, es el twitter, pero de origen ruso y es mucho más complejo. Es utilizado porque tiene un sistema de codificación que es más difícil de decodificar. Les sirvió a las comunicaciones en la red profunda cuando ya van captando el interés de posibles yihadistas. Cada día se cierran miles de cuentas yihadistas y ellos lo saben, por eso, mantienen cuentas inactivas que son activadas para reemplazar a las que son suprimidas y para eso, utilizan los hashtag y las palabras claves como los testigos, el palo -el stick- que se utiliza en las carreras de relevos.

Concluye señalando que los combatientes del Daesh utilizaron con profusión las redes sociales desde Siria y desde Irak para establecer contacto con amigos y familiares que vivían en sus países de origen y contarles sus hazañas y las bondades de vivir en las tierras del califato. Esto favoreció la radicalización y la captación de nuevos combatientes que viajaban a Siria, mientras las milicias del Daesh iban conquistando nuevos territorios, permitiendo acelerar los procesos de radicalización. Así, mientras Al Qaeda tardaba casi un año en radicalizar a alguien y forzar que fuera a hacer la yihad, estos señores en dos o tres meses lograron radicalizar a muchísimos jóvenes.

COMPARECENCIA DEL **SEÑOR CASTELLÓN MORENO, DIRECTOR OPERATIVO DEL DEPARTAMENTO DE SEGURIDAD NACIONAL,** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/000983 (CD) y núm. expte. del Senado 713/000475 (S)]. Sesión de 28 de septiembre de 2017.

El señor Castellón Moreno comienza señalando la singularidad y complejidad del ciberespacio y las acciones negativas que en este dominio se realizan. Además, señala que en el ciberespacio no hay límites ni fronteras y por ello la seguridad interior y la seguridad exterior se mezclan. Ello es debido a que el ciberespacio es considerado junto con los océanos y el espacio aéreo como un nuevo global commons, es decir, como un espacio común que conectó el mundo y que permite el libre flujo de personas, bienes, información, servicios e ideas. Unos espacios, por otra parte, insuficientemente regulados por la legislación, de difícil control y de fronteras difusas, es decir, afirma que son espacios propicios para la propagación de amenazas con altas probabilidades de éxito ya que la tecnología avanza pero frecuentemente no viene acompañada por medidas de seguridad. Continúa señalando que una de las principales dificultades que afectan al ciberespacio es saber quién está detrás de un ciberataque, tarea ardua que en ocasiones, tiene pocas probabilidades de obtener resultados.

El compareciente hace referencia a que hemos de entender incluido dentro del concepto de ciberseguridad todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Asimismo, señala que no considera dentro del ámbito propio de la ciberseguridad todas aquellas acciones que utilizan el ciberespacio para ejercer campañas de influencia o daño reputacional por no suponer una alteración tecnológica, aunque eso sí son acciones ilícitas contra un uso legal y seguro del ciberespacio. También informa que desde 2016 los ciberataques más comunes son el ransomware, el robo de datos, la denegación de servicios o la desfiguración de páginas web, el espionaje o el hackeo de dispositivos móviles. Los datos ponen en evidencia una creciente tendencia a la explotación de las vulnerabilidades tecnológicas como recientemente han puesto de manifiesto a nivel mundial los incidentes conocidos como WannaCry y Petya. Por otra parte, señala que el ciberespacio es también utilizado por grupos terroristas como medio e instrumento para realizar actividades de propaganda, comunicación interna, formación y adoctrinamiento.

En definitiva, insiste en que la ciberseguridad es una materia transversal en sí misma que afecta a todos los ministerios de la Administración General del Estado, a todas las Administraciones Públicas, a la sociedad y al país en su conjunto. Prueba de ello son las cifras relativas a 2016, año en el cual se registraron 106 000 incidentes de ciberseguridad en empresas, ciudadanos e infraestructuras públicas, mientras que las administraciones públicas hicieron frente a unos 21 000 incidentes de ciberseguridad.

A continuación, comienza a describir el marco de gobernanza de ciberseguridad en España, señalando como hitos importantes en esta materia, la creación del Consejo Nacional de Ciberseguridad en 2014 y la

cve: BOCG-12-CG-A-276

aprobación del Plan Nacional de Ciberseguridad. Todo ese esfuerzo institucional ha supuesto que España se encuentre en el grupo de cabeza a nivel internacional. Según la Unión Internacional de Telecomunicaciones, organismo perteneciente a Naciones Unidas, España se encuentra en el puesto 19.º a nivel mundial en materia de protección de la ciberseguridad y en el puesto 7.º a nivel de la Unión Europea, por delante de países como Alemania, Italia o Dinamarca.

Continúa describiendo el modelo de gestión de crisis en el marco del sistema de seguridad nacional que ha avanzado significativamente. El Departamento de Seguridad Nacional es el órgano de la Presidencia del Gobierno que comunica las labores técnicas de los Certsi, los centros de respuesta ante incidentes de ciberseguridad, con las decisiones estratégicas del Consejo Nacional de Ciberseguridad y el Comité de Situación, órgano este último, que asiste al Consejo de Seguridad Nacional en materia de gestión de crisis. Es un comité de carácter único que se apoya en el centro de situación del Departamento de Seguridad Nacional.

Por lo que se refiere a la cultura de la ciberseguridad, el compareciente señala que hay que decir que nadie es un consumidor pasivo de seguridad. La hiperconectividad y el desarrollo tecnológico, unidos al crecimiento del número de usuarios, hacen inevitable la exposición a amenazas en el espacio donde interactuamos. Es esencial desarrollar una cultura de ciberseguridad que nos haga más resilientes como sociedad, fomentando la concienciación sobre el uso seguro de la tecnología y la importancia de nuestra privacidad en la Red. Si bien la seguridad absoluta no existe, casos relacionados con el cibercrimen, como el robo de datos, de números de tarjetas de crédito, la extorsión o el acoso, demuestran que la concienciación sobre las amenazas existentes y la adopción de medidas de autoprotección redundarán en la disminución de nuestra vulnerabilidad.

Finaliza su comparecencia señalando la importancia de la colaboración público-privada. A este respecto, se trata de un factor clave en la lucha contra las ciberamenazas que proporciona una visión más completa de la ciberseguridad. Debe recordarse que más del 80 % de los servicios esenciales en España están en manos del sector privado e indica el problema que constituye la escasez de profesionales de la TIC, ya que la Comisión Europea calcula que la demanda de empleos en esta materia podría alcanzar en el año 2020 los 825 000 vacantes dentro de la Unión Europea.

COMPARECENCIA DEL **SEÑOR DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, S.A., INCIBE (HERNÁNDEZ MORENO),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm expte. 212/001015 (CD) y núm. expte. 713/000503 (S)]. Sesión de 16 de noviembre de 2017.

El Director General comienza describiendo las competencias y funciones del INCIBE, organismo que tiene encomendada la protección de ciudadanos y de empresas privadas en el ámbito digital, señalando la gran oportunidad que puede suponer para el desarrollo de España, ya que se presenta la oportunidad de contribuir al desarrollo de la industria y la creación de puestos de trabajo en un nuevo sector profesional.

Indica que el ciberespacio es un dominio asimétrico en la medida en que pueden producirse impactos de gran profundidad con poca inversión y por parte de un grupo reducido de personas, siempre que estas tengan el conocimiento técnico adecuado. Por ello, el ciberespacio es un medio muy atractivo para la comisión de actividades delictivas amparadas en el anonimato. Señala a este respecto que uno de los ámbitos en los cuales hay que actuar sin falta es el Internet de las cosas, ya que para 2020 se calcula que habrá más de 25 000 millones de dispositivos conectados a Internet. Por esa razón, entiende que la ciberseguridad es un asunto de todos y no solo un asunto reservado a los organismos o personas que trabajan en ese ámbito. Además, hay un aumento exponencial de los incidentes de seguridad notificados al INCIBE en los últimos años, que se debe entre otras razones, además de por el aumento de los incidentes, a una mejora de la relación de confianza entre el INCIBE y empresas privadas, las cuales comunican ahora más que antes los citados ciberincidentes.

En este sentido, continúa indicando que la primera línea de actuación de cualquier organismo público en esta materia debe ser la concienciación. Por eso, el INCIBE está llevando a cabo campañas de concienciación en colegios y en medios de comunicación y ha lanzado un programa de voluntariado para que todos aquellos profesionales que quieran aportar en este ámbito puedan hacerlo. Indica que ya son 300 los cibercooperantes que contribuyen a esta iniciativa y señala que se ha desarrollado una iniciativa pionera en el mundo denominada Cybercamp que reunió en León a más de 20 000 personas. Otra iniciativa relevante señaló fue el Cybersecurity Summer BootCamp que reúne la ciudad de León a 300

cve: BOCG-12-CG-A-276

personas de 30 países para formarse en ciberseguridad, incluidos jueces y fiscales españoles. Continúa resaltando la importancia de la cooperación internacional en esta materia, destacando la cooperación con la organización de estados iberoamericanos en materia de ciberseguridad.

Por otra parte, destaca que a día de hoy España tiene más de 140 empresas especializadas en la ciberseguridad, siendo este un sector con crecimiento anual del 13 %. A este respecto, señala que uno de los retos es encontrar el talento necesario para atender la demanda. Se estima que en los próximos años se producirá una necesidad de dos millones de puestos de trabajo relativos a la ciberseguridad en todo el mundo.

COMPARECENCIA 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. [Núm. expte. 219/000906 (CD) y núm. expte. 715/000293 (S)]. Sesión de 23 de noviembre de 2017.

Como señala la compareciente al inicio de la sesión, su objetivo consiste en informar sobre la desinformación en el ciberespacio y las guerras de información que se practican en las redes sociales y otros servicios de Internet. Siendo esto una de las manifestaciones de la guerra híbrida practicada en los últimos años por parte del Gobierno ruso. Seguidamente analiza los hechos relativos a una posible injerencia de Rusia en los acontecimientos políticos vividos en Cataluña en el último año.

Señala que las informaciones más llamativas al respecto que difundió el señor Assange han sido reproducidas por las redes de bots, que está comprobado su especialización en difundir noticias procedentes de Russia Today y Sputnik. En todo caso, indica que hoy en día la desinformación tiene como objetivo confundir y desacreditar a personas, grupos de personas u organizaciones. Pone como ejemplo de estas actuaciones lo ocurrido en las elecciones presidenciales en los Estados Unidos, en la campaña del Brexit o en las elecciones en Francia y Alemania aunque reconoce que sus afirmaciones se basan en deducciones y en los documentos oficiales publicados.

En definitiva, señala que de lo que se trata es de influir en los procesos, objetivo por otra parte, que es común a muchos países y que el mejor antídoto para contrarrestar dichas campañas de información es la calidad democrática de los Estados y la solidez de las convicciones liberales.

COMPARECENCIA 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. [Núm. expte. 212/001048 (CD) y núm. expte. 713/000522 (S)]. Sesión de 23 de noviembre de 2017.

El General comienza haciendo una descripción de lo que podemos entender como dominio ciberespacial. Lo describe como un espacio artificial o virtual pero real porque está compuesto de servidores, cables y equipos electrónicos. Se trata de un nuevo dominio en el cual el tiempo y la distancia no existen, en el cual tampoco hay fronteras y que afecta a todas las actividades de la sociedad, habiendo generado un entorno legal muy complejo.

Desde un punto de vista operativo afirma que en este ámbito no existe la paz, lo cual no significa que estemos en guerra, ya que siempre en mayor o menor grado se reciben ataques. Además en este ámbito todavía no se han articulado mecanismos de control de armamentos. En cuanto a las ciberarmas señala que estas son de un solo uso y sobre las cuales es posible hacer ingeniería inversa. Los ataques tienen planeamientos y preparaciones muy largas pero la ejecución es tremendamente corta como puso de relieve el incidente del WannaCry. Continúa señalando que en el ciberespacio defender es mucho más caro que atacar y además el atacante tiene poco que perder y mucho que ganar ya que es posible alcanzar al adversario en profundidad. En definitiva, la OTAN ha definido el ciberespacio como un quinto dominio de las operaciones militares en la cumbre de Varsovia en julio de 2016. Si bien señala que todas las actuaciones de todas las Administraciones Públicas son imprescindibles para aumentar la ciberseguridad del país; la más transversal de todas es la de mejorar la cultura de ciberseguridad de los ciudadanos.

Seguidamente, en su comparecencia el General pasa a describir el proceso de creación del Mando Conjunto de Ciberdefensa que alcanzó su capacidad operativa inicial en septiembre de 2013. Describe las misiones del mando cuya principal función es reaccionar contra las agresiones en el ciberespacio que se produzcan sobre las Fuerzas Armadas siempre que esa reacción sea oportuna, legítima y proporcionada

cve: BOCG-12-CG-A-276

dentro de los parámetros establecidos por el Derecho internacional. Señala, asimismo, la relevancia de la concienciación en las Fuerzas Armadas ya que requiere poca inversión y es tremendamente beneficiosa siendo la primera línea de defensa del sistema.

Para concluir, hace referencia a las numerosas colaboraciones con las empresas privadas y con las universidades como fuente de captación del talento, ya que son el ámbito en el cual se lleva a cabo la investigación y el desarrollo. Se muestra partidario de aumentar sustancialmente esa colaboración para aunar esfuerzos en el empeño común de aumentar la ciberseguridad en España.

COMPARECENCIA DEL **SEÑOR SARTS, DIRECTOR OF THE NATO STRATCOM CENTER OF EXCELLENCE,** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/000926 (CD) y núm. expte. 715/000308 (S)]. Sesión de 14 de diciembre de 2017.

El compareciente comienza presentando el centro que preside, el cual es un centro acreditado por la OTAN y creado por 12 países, pero que no forma parte de la estructura de la OTAN, y cuya misión es investigar la guerra de la información que incluye la utilización de las redes sociales o el aspecto digital del flujo informativo. Señala que la forma en la cual los ciudadanos perciben la realidad se ha transformado precisamente por la prevalencia de los medios digitales a la hora de informarse. Ello ha supuesto que cualquiera pueda tener la capacidad de ejercer una influencia de la información que recibe. Así son grandes proveedores de servicios digitales como Facebook, Google o Youtube los que seleccionan información de forma personalizada que llega a nuestros dispositivos cerrando así el canal de información a noticias que en principio no parezcan acordes con nuestras opciones políticas o sociales. Es lo que se conoce como el fenómeno de la burbuja de la información.

A esto hay que añadir el papel de la robótica y a este respecto señala que más del 80 % de las cuentas de las redes sociales no corresponden a personas reales sino a redes de bot, que parecen humanos pero que en realidad son programas robotizados. Pone como ejemplo el hecho de que según investigaciones del centro que dirige, el 85 % de los contenidos en ruso de twitter en los cuales aparece la palabra OTAN, Letonia o Estonia era generado por Robots y en inglés la cantidad llegaba al 50 %. Continúa apuntando a los otros grandes factores que están contribuyendo a configurar este fenómeno informativo que son el uso masivo del big data y de la inteligencia artificial. El problema reside en que esas herramientas se están empleando en ocasiones con el fin de crear divisiones emocionales en la sociedad rompiendo los diálogos o consensos en el seno de esa sociedad para lo cual se utilizan en muchas ocasiones las noticias falsas.

Otro vector importante que se está produciendo es el uso de la realidad aumentada con capacidad para alterar las imágenes o los vídeos gracias a una tecnología que ya está disponible, lo cual puede contribuir a socavar de manera muy importante la confianza en las instituciones y los Estados. La mejor forma de evitar estas situaciones es intentar garantizar que la sociedad aumente su resistencia frente a estas campañas de desinformación. A este respecto, señala que un debate abierto en profundidad en los medios de comunicación y en el ámbito político aumenta la resiliencia de la sociedad por lo cual es importante introducir estos asuntos en el sistema educativo, en los medios de comunicación y hacerlos accesibles al público en general.

Por todo ello, concluye que el Centro que dirige es capaz de dar formación y asistencia a los gobiernos nacionales para poder desarrollar esas capacidades. No obstante, concluye afirmando que para poder contrarrestar con éxito este tipo de campañas es necesario disponer de una narrativa nacional sólida y que cuando los gobiernos no disponen de la credibilidad suficiente para responder a estos fenómenos es muy efectiva la actividad de entidades no gubernamentales que asumen la carga de ir desmontando las noticias falsas exponiendo cuál es la realidad de los hechos. Concluye invitando al Gobierno de España para que se una a los doce Estados que ya forman parte del Centro de Excelencia de la OTAN de Comunicación Estratégica (Nato Stratcom).

COMPARECENCIA DE LA **SEÑORA FISCAL DE SALA COORDINADORA EN MATERIA DE CRIMINALIDAD INFORMÁTICA (TEJADA DE LA FUENTE),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/001075 (CD) y núm. expte. 713/000557 (S)]. Sesión de 14 de diciembre de 2017.

La Sra. Tejada comienza su comparecencia describiendo la composición y actuaciones del área especializada en criminalidad informática de la Fiscalía, creada hace 6 años e integrada en la actualidad por más de 150 fiscales. Esta es descrita por ella misma como la punta de lanza de lucha contra la

cve: BOCG-12-CG-A-276

ciberdelincuencia. Asimismo, señala como muy decisiva la colaboración que las unidades especializadas en investigación tecnológica de los cuerpos policiales prestan a los citados fiscales.

Continúa señalando que en estos momentos estamos viviendo la aparición de nuevas conductas impensables hace 20 ó 30 años de planificar y llevar a cabo delitos tradicionales que ahora se cometen de una forma distinta gracias a las herramientas tecnológicas. Señala que para hacer frente a esta nueva realidad es necesario mejorar la investigación tecnológica sin que ello suponga afectar o limitar los derechos fundamentales. Asimismo, continúa describiendo los fenómenos de ciberdelincuencia con los que la Fiscalía se está encontrando, indicando que el delito más común es el de estafa con un 61 % de los procedimientos judiciales incoados por ciberdelitos durante el año 2016. Resalta que dentro de este grupo de delitos destaca la oferta fraudulenta de bienes y servicios, el phising y la utilización fraudulenta de tarjetas de débito o crédito conocida como carding.

No obstante, afirma que uno de los aspectos que más le preocupa a la Fiscalía son los delitos cometidos a través de la Red relativos a la libertad sexual de los menores. El acoso a los menores a través de la Red con fines de carácter sexual se ha visto sustancialmente incrementado en los últimos años. La gravedad de estas conductas se centra en la extrema vulnerabilidad de los menores frente a este tipo de comportamientos, cuya persecución presenta mucha complejidad. La investigación en esta materia se centra en el rastreo de la Deep web y de los sistemas de mensajería instantánea Whatsapp y Telegram, en los cuales la investigación resulta especialmente compleja.

Por otra parte, señala que la completa implementación de la trasposición al ordenamiento jurídico interno de la Directiva NIS va a suponer un incremento sustancial de la notificación a las autoridades de los ciberataques. En este sentido, afirma que la Fiscalía ya se ha anticipado a este escenario mediante la Circular 3/17, en la que se analizan los tipos penales concernidos. Señala también la dificultad de perseguir delitos de odio, amenazas o acoso cuando los contenidos se difunden a través de plataformas cuyos responsables radican en otros Estados.

Para concluir, indica la relevancia de articular instrumentos jurídicos internacionales para lograr una eficaz cooperación entre Estados. A este respecto, cita como ejemplo de eficacia, el Convenio de Budapest, del año 2001, que han ratificado 56 países. En este sentido, la compareciente señala que España se encuentra especialmente implicada en desarrollar todas las potencialidades que este Convenio encierra y justamente ahora se está trabajando en el Segundo Protocolo Adicional a este Convenio.

Finaliza su comparecencia señalando la necesidad de modificar algunos aspectos de la normativa penal tales como la tipificación de la figura de la suplantación de identidad de la Red. Asimismo, sugiere la necesidad de modificar la tipificación de los delitos de injurias y calumnias para permitir ejercer la acción penal una vez que el ofendido ha fallecido para que puedan ejercitarla herederos o familiares del mismo. Señala la conveniencia de sancionar con pena de privación de utilización de Internet o de administrar páginas web para prevenir la reiteración de los comportamientos más graves a aquellos sujetos que han sido condenados por delitos, como por ejemplo, el acoso a menores a través de Internet.

COMPARECENCIA DE **DON XABIER MITXELENA RUIZ, SECURITY IBERIA LEAD EN ACCENTURE,** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001044 (CD) y núm. expte. 715/000356 (S)]. Sesión de 28 de febrero de 2018.

El compareciente empieza señalando que la ciberseguridad ya no es un riesgo potencial sino que es un riesgo real y prueba de ello es que se duplican los incidentes cada año. A este respecto señala que las vulnerabilidades son de dos tipos: la tecnológica y la humana. Asimismo, incide en que se puede decir que hay un antes y un después del WannaCry dado que ha sido el ataque más mediático. En este sentido indica que lo que se necesita ahora es organizar y ordenar la solución a este problema y este empeño hay que llevarlo a cabo abordando directamente el problema desde la raíz.

Señala que estamos abriendo un mundo digital y que tenemos la tentación de observar esta nueva realidad casi como un elemento de diversión pero que no estamos gestionando de verdad los riesgos que estamos generando. Manifiesta que ya se están llevando a cabo en el ámbito europeo iniciativas a este respecto, entre otras, la nueva normativa de protección de datos que coloca responsabilidades en los propios consejos de administración. Ello supone cambiar la visión que hasta este momento se tenía de la ciberseguridad como un coste, pasando a ser más bien un activo de las organizaciones que te diferencia

cve: BOCG-12-CG-A-276

de tus competidores. En cuanto a la dimensión del problema afirma que en el año 2021 el coste de la ciberinseguridad será seis trillones de dólares, es decir dos veces el PIB de España.

En cuanto a los retos señala uno fundamental que es la carencia de profesionales en este ámbito, pero también la necesidad de cambiar la forma de pensar y la forma de hacer en un escenario absolutamente nuevo, para ello será imprescindible definir un nuevo modelo de identidad digital ya que es absolutamente necesario saber quién está al otro lado en el mundo digital. Asimismo, expone que después de las cuatro revoluciones que hemos vivido en los últimos 150 años: vapor, electricidad y petróleo, la revolución actual coloca a los datos como centro de la misma. En definitiva, el activo más valioso para cualquier organización es la información.

Asimismo, señala que es necesario empezar a concienciar desde edades tempranas en el buen uso de la tecnología dado que esa es la clave para ponerle difícil las cosas a los que actúan maliciosamente en el ciberespacio. Manifiesta también que la gobernanza pública regulando esta nueva realidad es clave y esa actividad normativa debe centrarse en la educación en estas materias desde la enseñanza primaria, como ya hacen otros países de nuestro entorno, y del mismo modo que ya se enseña educación vial. Afirma que se deben hacer más esfuerzos en materia de formación profesional.

A continuación, afirma que es necesario poner las bases de un nuevo ciberderecho y que es imprescindible avanzar en el ámbito de las certificaciones de personas, de empresas y de productos. Asimismo, es imprescindible la colaboración público-privada para, entre otras cosas, recuperar parte del talento español que desarrolla su trabajo en otros países. Señala, asimismo, la responsabilidad que como ciudadanos tenemos todos para no difundir las informaciones no chequeadas previamente y que contribuyen a la desinformación en un ámbito de postverdad.

Concluye anunciando que es necesario un plan de transformación que se basa en la generosidad de todos los actores, en una compra pública innovadora y en un liderazgo estratégico.

COMPARECENCIA DE **DON CARLOS SÁNCHEZ ALMEIDA, DIRECTOR JURÍDICO Y MIEMBRO DE LA JUNTA DIRECTIVA DE LA PLATAFORMA EN DEFENSA DE LA LIBERTAD DE INFORMACIÓN (PDLI),** PARA QUE EVALÚE LOS DERECHOS A LA LIBERTAD DE EXPRESIÓN Y DE ACCESO A LA INFORMACIÓN, ASÍ COMO LOS RIESGOS A LOS QUE SE ENFRENTAN LOS USUARIOS DE INTERNET EN ESPAÑA FRENTE A LOS ATAQUES Y VULNERACIONES DE CIBERSEGURIDAD [Núm. expte. 219/000931 (CD) y núm. expte. 715/000320 (S)]. Sesión de 28 de febrero de 2018.

Comienza el compareciente señalando la importancia del debate que se establece entre libertad de expresión y regulación de la seguridad nacional. Afirma que la ausencia de regulación de los contenidos de Internet ha hecho precisamente que Internet sea un éxito basado en el caos. Por ello, la fuerza de la libertad de Internet depende de ese caos. Afirma también que el único poder legitimado para intervenir Internet en materia de contenidos ha de ser siempre el Poder Judicial.

Por otra parte, denuncia la aprobación de una serie de leyes que han restringido la libertad en Internet al introducir el control de contenidos, como la Ley de Propiedad Intelectual, la Ley de Seguridad Ciudadana, la Ley del Código Penal y la Ley de Enjuiciamiento Criminal, señalando que todas ellas fueron aprobadas durante la legislatura 2011-2015, suponiendo un retroceso en materia de derechos.

A continuación, aborda el asunto de las noticias falsas señalando que es necesario llegar a una definición consensuada en esta materia, que todos los actores de la cadena informativa utilicen como base común para fomentar así la no difusión de estas noticias. Para ello es necesaria la implantación de técnicas de verificación de contenidos que cumplan estándares internacionales. En esta materia continúa afirmando que es muy peligroso que una autoridad administrativa se atribuya la facultad de etiquetar lo que es falso y lo que no. En este sentido, expone que se están produciendo detenciones de twitteros y blogueros, lo cual va en contra de la libertad de expresión.

Señala que el anonimato en Internet es consustancial al ejercicio de la libertad de expresión y es un derecho reconocido en el propio reglamento general de protección de datos así como el derecho al cifrado. En este sentido, se refiere a la declaración conjunta sobre libertad de expresión y derecho de información que señala que las noticias falsas son un peligro para las sociedades democráticas, pero que la regulación de esa materia es muy complicada ya que las prohibiciones generales basadas en ideas vagas y ambiguas son incompatibles con las normas internacionales sobre libertad de expresión.

Además, comunica que ya el Código Penal recoge las noticias falsas en varias regulaciones como las de las noticias falsas en materia de cotizaciones bursátiles o las falsas alarmas. Asimismo, hay regulación

cve: BOCG-12-CG-A-276

sobre noticias falsas y propaganda en la Ley de Régimen Electoral. Por ello considera el compareciente que en materia de Código Penal no hacen falta regulaciones adicionales.

Concluye señalando que los estados totalitarios tenían el monopolio de la propaganda pero ese monopolio afortunadamente se ha perdido para siempre.

COMPARECENCIA DEL **SEÑOR ROMERO BARTOLOMÉ, SOCIO RESPONSABLE DE SOLUCIONES DE SEGURIDAD DE PWC,** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001045 (CD) y núm. expte. 715/000357 (S)]. Sesión de 28 de febrero de 2018.

Comienza haciendo referencia a una encuesta realizada en todo el mundo a 4000 empresas de la que se extrae la preocupación por las cuestiones relativas a la ciberseguridad, así como un 25 % de las empresas españolas, a las que se preguntó para realizar el citado estudio contestaron que temen la producción de daños a la vida humana por incidentes relativos a la ciberseguridad, especialmente a todo lo relativo a los sistemas de control industrial. Señala que un campo de actuación importante va a ser todo lo relacionado con el desarrollo normativo de la ley de seguridad de redes y sistemas y el desarrollo reglamentario de la ley de seguridad privada. Por otra parte, señala que tan importante es ya la seguridad física de una determinada organización como su seguridad informática.

Continúa advirtiendo que si bien hace 20 años España era referente en muchas de esas cuestiones, certificados electrónicos con firma digital, tributación por Internet, DNI electrónico, lo cierto es que hoy en día hemos dejado de ser ese referente como país. El punto diferencial con respecto a nuestros países homólogos como Francia o Reino Unido se encuentra en la dotación presupuestaria. Por ello señala que si bien tenemos excelentes profesionales en el ámbito público y en las empresas lo que falta es financiación.

Por último, indica la necesidad de reorganizar las estructuras administrativas de nuestro país de forma tal que haya una figura con nivel de Secretario de Estado que dependa del Presidente del Gobierno para coordinar las actuaciones en materia de ciberseguridad encarnando así la dirección política del cumplimiento de la estrategia nacional de ciberseguridad.

COMPARECENCIA DE **DON FERNANDO PICATOSTE, SOCIO RISK ADVISORY (DELOITTE),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 713/000663 (S) y núm. expte. 219/001131 (CD)]. Sesión de 12 de abril de 2018.

El compareciente comienza exponiendo que el concepto de ciberseguridad que debe ser utilizado se basa en tres palabras: protección, vigilancia y resiliencia. A continuación centra su exposición en el impacto que tienen los incidentes de ciberseguridad entendido como costes económicos, costes operativos y costes reputacionales. En este sentido, insiste en que la crisis del Wannacry puso de manifiesto un trabajo conjunto como nación en el cual ha habido una buena colaboración y de confianza mutua.

En este sentido, insiste en que el actual nivel de colaboración en la industria española de ciberseguridad es excelente tanto en el ámbito público como en el privado. Por ello, pone como ejemplo de modelo a seguir el caso de Israel, que concentra en sus manos el 5 % del mercado mundial de ciberseguridad y con un apoyo muy potente del Estado. Siendo el retorno económico de este esfuerzo muy relevante para este país.

A continuación, señala que España debería seguir tres líneas de actuación en esta materia. La primera consistiría en liderar sin miedo en los entornos nacionales e internacionales. Para ello, es necesario además de la estrategia que ya existe un plan que permita pasar a la fase operativa. En el plano internacional, propone adoptar un papel más activo en cuanto a la participación española en ENISA así como en la OTAN y EUROPOL. En definitiva, propone asociar la marca España a un nivel muy elevado de ciberseguridad. Una segunda línea de actuación consistiría en demostrar que la industria española es líder en ciberseguridad del Internet de las cosas. Una tercera consistiría en potenciar el ecosistema en su conjunto mediante un gran apoyo institucional aumentando el I+D+i. En ese sentido, señala que habría que hacer un esfuerzo más importante en materia de compra pública innovadora. Finalmente propone que se trabaje desde la base para formar cada vez más talento, especialmente en la universidad.

cve: BOCG-12-CG-A-276

COMPARECENCIA DEL **GENERAL DE DIVISIÓN DON JOSÉ LUIS GOBERNA CARIDE, SUBDIRECTOR GENERAL DEL CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (CESTIC),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 715/000416 (S) y núm. expte. 212/001203 (CD)]. Sesión de 12 de abril de 2018.

Comienza el compareciente señalando que estamos en los albores de una cuarta revolución industrial y que en la tecnología radica en muchas ocasiones la seguridad y superioridad de las fuerzas armadas. Continúa señalando que el principal objetivo en el que se encuentra implicado el Ministerio de Defensa es en reforzar la seguridad de los sistemas de información y comunicaciones estratégicos. Continúa detallando los requisitos mínimos recogidos en el Esquema Nacional de Ciberseguridad, y cuáles son las capacidades y competencias del centro que dirige el CESTIC (Centro de Sistemas de Tecnologías de la Información y las Comunicaciones).

Seguidamente, señala los tres grandes planes que está desarrollando en estos momentos en el Ministerio de Defensa. El primero es el Plan de actuación para la seguridad de la información cuyo horizonte de ejecución son 6 años, desde 2018 a 2023. Señala que a su vez, este plan se divide en 6 subplanes según se refieran a instalaciones, documentos, personas, etc. El segundo de los planes generales está enfocado hacia las tecnologías y se denomina Plan estratégico de sistemas de información y comunicación. A este respecto, indica la importancia de homologación y normalización de sistemas y su interoperabilidad. Y por último se refiere al plan de acción del Ministerio de Defensa a la transformación digital orientado a la revisión integral de los procesos y a la racionalización de los sistemas de información y servicios de dicho Ministerio en relación con la Administración General del Estado.

Concluye su exposición realizando algunas reflexiones de carácter general. La primera es que el activo a proteger siempre es la información que permite lograr la superioridad en la toma de decisiones. Cuanto más relevante sea esa información mayores deben ser sus recursos dedicados a su protección. Técnicamente hablando, todos los esfuerzos deben centrarse en los datos aplicando en todo momento el Esquema Nacional de Ciberseguridad.

COMPARECENCIA DEL **SEÑOR PÉREZ GARCÍA (CEO UNIDAD CIBERSEGURIDAD TELEFÓNICA, ELEVEN PATHS),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001245 (CD) y núm. expte. 715/000513 (S)]. Sesión de 24 de mayo de 2018.

El compareciente comienza señalando que el fenómeno de disrupción digital que estamos viviendo hoy en día experimenta un crecimiento exponencial como demuestra el hecho de que en el año 2020 habrá cuatro mil millones de usuarios con acceso a Internet en el mundo. Ahora bien, la gran amenaza que se cierne sobre este horizonte tiene que ver con la ciberseguridad. Señala como ejemplo de ello lo ocurrido en 2013 con información falsa distribuida sobre un atentado en la Casa Blanca que desplomó el valor de la Bolsa de Nueva York en 280 000 millones de dólares. En este sentido, apunta a que ya se está produciendo una nueva Guerra Fría acerca del control de los datos entre las superpotencias.

A continuación, indica que el crecimiento de la productividad económica en los países en los próximos años estará en buena medida condicionado por conseguir entornos seguros en el ámbito digital, y para ello, será clave la resiliencia que consiste en prevenir, detectar, responder y recuperar adecuadamente en tiempo real. A este respecto, señala que, no obstante, ningún país ni ninguna empresa estarán totalmente a salvo de ser hackeadas. Para resaltar la importancia del sector de la ciberseguridad señala que la propia Telefónica obtuvo el año pasado 500 millones de dólares en todo el mundo por servicios en este campo siendo una de las áreas de más crecimiento de la empresa con más de 1500 profesionales dedicados solo en la ciberseguridad. Solo en servicios de seguridad gestionados desde España y prestados en el resto del mundo se calcula que el mercado mundial asciende a 20 000 millones.

Este mercado tan sustancioso está siendo aprovechado por los fondos de inversión y no solo por las empresas. Estos fondos de inversión inviertieron 20 000 millones el año pasado en la creación de startups en materia de ciberseguridad a nivel mundial, estando localizadas estas nuevas empresas especialmente en Silicon Valley, en Texas y en Tel Aviv.

A este respecto, señala el caso de Israel como muy significativo, que, teniendo una cuarta parte del PIB de España, invierte 10 veces más que nuestro país en esta materia, siendo uno de los principales motores de crecimiento de ese país. También es un gran yacimiento de empleo dado que se calcula que a nivel mundial en el año 2021 harán falta 3 millones y medio de profesionales en el sector.

Concluye señalando que España debe realizar una fuerte inversión que no está realizando en estos momentos si quiere situarse en una buena posición para competir a nivel mundial en esta materia.

cve: BOCG-12-CG-A-276

COMPARECENCIA DEL **SEÑOR DIRECTOR DEL CENTRO NACIONAL DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS, CNPIC (SÁNCHEZ GÓMEZ),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/001636 (CD) y núm. expte. 713/000970 (S)] Sesión de 24 de mayo de 2018.

Comienza el compareciente haciendo referencia al Informe del Foro Económico Mundial sobre Riesgos globales de 2018 que señala por orden de importancia los ciberataques como la tercera amenaza más probable y como la sexta con efectos potenciales más negativos a nivel mundial. La ciberseguridad según él, no puede ser considerada como un elemento ni ajeno ni distinto al concepto global superior de seguridad como ya reconoce la Estrategia de Seguridad Nacional.

Seguidamente, y por ser objeto de su ámbito de competencias, se refiere a los posibles ataques contra infraestructuras críticas y servicios esenciales. A este respecto, indica que la Ley 8/2011 de Protección de Infraestructuras críticas señala 12 sectores estratégicos entendiendo estos como áreas diferenciadas dentro de la actividad laboral, económica y productiva que proporcionan un servicio esencial o que garantizan el ejercicio de la autoridad del Estado. El ataque a uno o varios de estos servicios es valorado desde el CNPIC conforme a una serie de parámetros para evaluar su gravedad: victimización, impacto económico, impacto social o impacto sobre el medio ambiente.

Señala que vivimos en sociedades hipertecnificadas y por ello, extremadamente dependientes de las infraestructuras críticas. Asimismo, esas infraestructuras son muy interdependientes con lo cual, el funcionamiento de una estructura o servicio condiciona el funcionamiento de los demás, en cadena. Continúa señalando que en España el 80 % de esas infraestructuras críticas son propiedad de las empresas privadas, lo cual hace imprescindible una interlocución fluida con esas empresas por parte de las autoridades.

En este sentido, señala que ha habido un incremento importante de los incidentes en sistemas y redes gestionados por operadores críticos que han pasado de 18 en 2012 a 855 en 2017. Estos ataques se han dirigido principalmente contra el sistema financiero, el sistema energético, el sistema de transporte y contra las infraestructuras que gestionan el agua. Todo lo anterior motiva que el sistema de gestión de infraestructuras críticas exija una gran coordinación de todos los actores, más de 200, que se dirigen desde la Secretaría de Estado de Seguridad. Ello da lugar a la mayor comunidad de cooperación público-privada de España en materia de seguridad.

En cuanto a las debilidades, el compareciente señala que la más preocupante es la escasa cultura de ciberseguridad que existe, a nivel ciudadano pero también a nivel de directivos de las organizaciones. Concluye señalando que hoy en día es muy difícil garantizar la seguridad de un país tan solo desde la parte pública del sistema. Por ello la colaboración público-privada es fundamental. Asimismo, señala que las políticas de ciberseguridad no son gratuitas y se necesitan recursos y medios adicionales mediante un adecuado respaldo presupuestario. Por ello, reclama el tratamiento de ciberseguridad como una política de Estado de alcance transversal.

COMPARECENCIA DEL **SEÑOR REGO FERNÁNDEZ (SOCIO DE IHACKLABS),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001246 (CD) y núm. expte. 715/000514 (S)]. Sesión de 24 de mayo de 2018.

El compareciente comienza señalando que el hecho de que la economía, la industria e incluso nuestra manera de comunicarnos y relacionarnos sea cada vez más digital incrementa la superficie de ataque en el ciberespacio y por ello aumentan los riesgos. A este respecto, señala de forma previa la importancia que tiene para cualquier país desarrollar políticas públicas y capacidades que tengan como objetivo la generación de talento profesional y el desarrollo de un ecosistema de empresas de ciberseguridad. Continúa indicando que es necesario surtir al mercado de trabajo de profesionales en esta materia dado el incremento de la demanda que no es cubierta por la oferta existente. Se calcula que en Europa en 2022 ese desfase entre oferta y demanda alcanzará los 350 000 profesionales.

Es necesario por ello que las instituciones públicas impulsen el desarrollo profesional en materia de ciberseguridad. Además, continúa señalando que esos profesionales son especialmente necesarios en las Fuerzas Armadas, la Judicatura, las Fuerzas y Cuerpos de Seguridad del Estado ya que la seguridad nacional podría verse debilitada precisamente por la falta de talento. Si a todo lo anterior le unimos la tasa de desempleo que en estos momentos, es de 0, se puede hablar de una enorme oportunidad para un país volcado en los servicios como el nuestro para generar empleo.

cve: BOCG-12-CG-A-276

Para ello, será imprescindible un catálogo de sectores profesionales inventariando capacidades y competencias que permita acortar las discrepancias entre la oferta universitaria de formación reglada y lo que demandan las empresas. A este respecto, señala que falta en el mercado de trabajo una hiperespecialización con perfiles muy concretos que son los que no se encuentran en el mercado de trabajo. Continúa indicando que es necesario detectar talento desde una edad temprana en el propio colegio a partir de los 12 años potenciando los eventos concretos que permiten detectar ese talento.

Por otra parte, señala que hay un enorme campo de posibilidades respecto al crecimiento en Iberoamérica. Se trata de un mercado en el cual las empresas españolas tienen muchas oportunidades de liderar y que por alguna razón hasta ahora, no se está alcanzando ese liderazgo, dado que existe una cierta desconfianza a pedir asesoramiento a otros países pero en cambio, hay una mayor proximidad natural hacia España.

Asimismo, indica que es necesario reducir la dependencia de productos informáticos clave para nuestra ciberseguridad en la medida de lo posible. También incide sobre la necesidad de aprobar un plan de investigación para evitar solapamientos entre las actividades que realizan los centros de investigación y las universidades españolas. En este sentido, abunda en que sería necesario orientar la investigación hacia resultados más prácticos de los que en la actualidad se obtienen, muy centrados en lo teórico.

Por último, incide en que es necesario generar espacios de encuentro entre emprendedores y mecanismos privados de inversión, dado que hay mucho interés en el sector privado por invertir dinero en el sector de la ciberseguridad.

COMPARECENCIA DEL **SEÑOR MAEZTU LACALLE (ABOGADO ESPECIALIZADO EN INTERNET, PROPIEDAD INTELECTUAL Y TECNOLOGÍA),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001288 (CD) y núm. expte. 715/000533 (S)]. Sesión de 28 de junio de 2018.

El compareciente comienza señalando que la ciberseguridad afecta al mundo real y como tal afecta a la seguridad nacional citando como ejemplo la publicación de los mapas de instalaciones militares en todo el mundo mediante los datos publicados por aplicaciones deportivas. Seguidamente, señala la necesidad de tramitar las normas relativas al mundo digital con la mayor agilidad posible, tales como la Ley Orgánica de Protección de Datos.

A este respecto, señala que jurídicamente hablando se plantea un problema con la conservación de datos que en estos momentos por una sentencia del TJUE de 2014 todavía se encuentra en un cierto limbo jurídico, en algunos países de Europa, incluida España, lo cual está dificultando la investigación de delitos graves. Por lo anterior, cree que es urgente adaptar correctamente la normativa española a lo que dictaminó el TJUE en el año 2014 mediante la citada sentencia.

Seguidamente, se refiere a la relación de los hacktivistas o hacker que descubren fallos de seguridad. A este respecto, señala que cuando alguien descubre una brecha de seguridad en el sistema acuden a abogados como él mismo para que amparados en el nivel de secreto respecto a sus clientes, sean ellos los que notifiquen esas brechas de seguridad por miedo a las posibles consecuencias legales. Por ello señala que es necesario facilitar vías de colaboración que permitan detectar, reparar y solucionar esas brechas sin miedo a las posibles consecuencias legales.

Continúa indicando que no considerara positivo militarizar los organismos de coordinación en materia de ciberseguridad. También se muestra partidario de incorporar software libre o de código abierto para reducir la dependencia de las empresas. A este respecto, abunda en que es necesario apostar por incrementar la capacidad técnica para poder auditar los códigos informáticos del que dependen la mayoría de los sistemas.

Concluye haciendo referencia a aspectos relacionados con las criptomonedas especialmente, la incerteza y la inseguridad que provoca la falta de cobertura legal que priva de seguridad jurídica a todas las operaciones relacionadas con la compra y la venta de estos activos. Por ello, recomienda que frente a estas nuevas tecnologías no se puede reaccionar prohibiendo sino que es mejor colaborar, cooperar, facilitar y regular siendo esta la única manera de mantener un cierto control sobre esas operaciones en Internet que pueden encubrir actividades ilícitas.

cve: BOCG-12-CG-A-276

COMPARECENCIA DEL **SEÑOR LEÓN DE MORA (DIRECTOR DE LA CÁTEDRA TELEFÓNICA INTELIGENCIA EN LA RED Y DIRECTOR DEL GRUPO DE INVESTIGACIÓN TECNOLOGÍA ELECTRÓNICA E INFORMÁTICA INDUSTRIAL, TIC-150, DE LA UNIVERSIDAD DE SEVILLA),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001289 (CD) y núm. expte. 713/000992 (S)]. Sesión de 28 de junio de 2018.

Comienza señalando la velocidad a la cual se está produciendo el cambio digital y la evolución de la tecnología. A este respecto, indica que cada año se producen más de 111 billones de líneas de código lo cual resulta muy difícil de auditar. También señala que el volumen de datos almacenados alcanzará, en 2010, 50 veces lo que tenemos hoy día, una cantidad del orden de los 96 petabytes (un petabyte es un billón de terabytes). Indica que toda esta realidad es muy difícil de manejar ya que también esa aceleración tecnológica se traducirá en aceleración social. Dentro de 10 años, el 30 % de las empresas que existen hoy habrán desaparecido ya que el centro de la economía se desplaza hacia los datos, lo cual determina que hoy, las 5 mayores empresas por capitalización bursátil sean 5 empresas tecnológicas no siendo ninguna de ellas europea. A ello se le une la introducción masiva de inteligencia artificial en todos estos procesos. De hecho, afirma que el 50 % de las operaciones en las Bolsas del mundo ya se están haciendo mediante inteligencia artificial.

Frente a esta realidad, también el número de ciberataques a empresas se multiplica cada año. Se calcula que el año pasado en Estados Unidos se pagaron 1000 millones de euros por rescates debidos a infecciones de ransomware, y que en la web oscura que tiene 50 millones el tamaño de la red a la que accedemos normalmente, se vendieron 500 millones de dólares en productos relacionados con el malware. Las estrategias de defensa frente a esta realidad son varias: unos Estados están intentando fragmentar Internet para controlarla, otros se oponen a ello por desvirtuar la propia esencia de Internet. Lo que sí es cierto es que cada vez los Estados tienen una mayor presencia geoestratégica en Internet, y es necesario que estén presentes en este nuevo ámbito.

A este respecto, señala que es imprescindible formar talento en este país en esta materia y para ello una tarea previa sería elaborar un catálogo de formación y titulaciones que pueda ayudar a las universidades y a otros centros educativos a planificar qué formación es necesaria en el ámbito de la ciberseguridad a corto y medio plazo.

Interesa también establecer un sistema de acreditación para esa formación que dote de certezas al sistema y permita satisfacer la actual demanda que existe y que actualmente no se cubre. A este respecto, considera imprescindible reducir la brecha de género en esta materia que permitiría incorporar talento adicional. A ello se le une un problema general de la Unión Europea que es la carencia de competencias digitales de la población estando España en esta materia en un puesto medio dentro de la Unión Europea. Por tanto, es necesario insistir en la incorporación de habilidades digitales en todas las etapas del desarrollo formativo.

Abundando en la necesidad de acreditar y estandarizar la formación, señala que en España se ofrecen en la actualidad 48 masters sobre ciberseguridad, pero solo 4 son títulos oficiales. Siendo esta un área de especial interés y con mucha demanda por parte del mercado de trabajo, se debería hacer lo posible para que los estudiantes soliciten más formación en esta materia estimulando su interés, así como incrementar los presupuestos para investigación en los centros de I+D.

Seguidamente, señala que la inteligencia artificial será la tecnología estratégica del siglo XXI, lo cual tendrá consecuencias en materia de destrucción de puestos de trabajo y aunque se crearán otros nuevos, se prevé una destrucción de empleo muy rápida. Por ello hay que anticiparse y compensar esa destrucción con la creación de nuevos puestos de trabajo en nuevas profesiones. Señala que la inteligencia artificial afectará a una gran cantidad de tecnologías diversas. A este respecto insiste en la necesidad de acometer un esfuerzo serio en esta materia ya que si no podemos convertirnos en lo que se denomina una cibercolonia de otras potencias mundiales, razón por la cual la UE está preparando una estrategia sobre inteligencia artificial para Europa.

También incide en la necesidad de entender los aspectos éticos y legales de la utilización de los algoritmos que califica como cajas negras que pueden tener sesgos que influyan en las decisiones que el algoritmo toma. Concluye señalando la relevancia que la inteligencia artificial va a tener para la ciberseguridad, y la necesidad de la investigación de la excelencia en esta materia suponiendo un esfuerzo en el cual el país tiene que ponerse a la altura de lo que le demanda el desarrollo tecnológico.

cve: BOCG-12-CG-A-276

COMPARECENCIA DE LA **SEÑORA QUINTANA (PERIODISTA EXPERTA EN CIBERSEGURIDAD, AUTORA DE LOS LIBROS «CIBERACTIVISMO», 2012, Y «CIBERGUERRA», 2016, EDITORIAL CATARATA),** PARA QUE EVALÚE LA SITUACIÓN ACTUAL DE LOS DERECHOS DE LOS USUARIOS DE INTERNET Y LAS SUPUESTAS CAMPAÑAS DE DESINFORMACIÓN QUE CONSTITUYEN SUPUESTOS CIBERATAQUES EN CONTRA DE ORGANISMOS PÚBLICOS Y PRIVADOS EN ESPAÑA. [Núm. expte. 219/000932 (CD) y núm. expte. 715/000321 (S)]. Sesión de 28 de junio de 2018.

Comienza su intervención señalando que en este ámbito se produce siempre una tensión entre la obligación de los Estados de procurar la seguridad de sus ciudadanos y el respeto a las libertades de estos. Las nuevas tecnologías han incrementado de forma notable la realización del derecho de los ciudadanos a la información y el derecho a intervenir en los asuntos públicos. No obstante, al lado de estos derechos surgen nuevas amenazas como los fenómenos de cibervigilancia global y las nuevas formas de censura. Continúa señalando que la arquitectura de Internet es una garantía para la libertad de expresión en el ciberespacio gracias al anonimato relativo, la distribución descentralizada y los múltiples puntos de acceso. Por otra parte, a esta realidad se le une la total dependencia tecnológica que se ha ido introduciendo en nuestras vidas ya que utilizamos aplicaciones y dispositivos que no controlamos. Incide en que según sea el enfoque con que se tratan estas materias determinaremos el marco en el cual se propondrán las soluciones.

En cuanto a la referencias de la ciberguerra señala que se trata de un fenómeno muy complejo que podría ser catalogado como un conflicto que se libra en el ciberespacio pero que al mismo tiempo, supone una continuación de los conflictos convencionales. En esta materia es especialmente relevante el problema de la atribución. A este respecto, señala que la mayoría de las atribuciones se producen por el método de la deducción intentando acumular el mayor número de pruebas. No obstante, ello no solventa totalmente el problema de la atribución de los ciberataques, especialmente, debido a los ciberataques de bandera falsa.

También indica que en esta materia otro de los vectores es la disputa por el control político de las actuaciones dentro del reparto de competencias en las diversas administraciones. Seguidamente, incide en la importancia del debate sobre el cifrado en las comunicaciones y la protección de las infraestructuras críticas señalando, a este respecto, que las soluciones en esta materia no pueden ser individuales sino globales.

Por último, se refiere a la variable de acciones de propaganda y desinformación y a la libertad de información ya que la forma de limitar esas acciones de influencia no puede ser restringir el libre flujo de la información. En este sentido, señala que la transparencia de los algoritmos es una condición fundamental frente a los intentos de algunos países como Alemania, Francia o Reino Unido, de limitar la libertad de acceso de información.

Concluye señalando que los Estados siguen siendo a día de hoy el actor más peligroso en el ciberespacio y que hay que tener en cuenta los daños colaterales de las operaciones de ciberguerra como se puso de manifiesto con los ataques de WannaCry o Petya. Asimismo, insiste en la necesidad de proteger la libertad de información en la red estableciendo algún tipo de regulación de protección de las filtraciones como único medio para que la ciudadanía tenga acceso a información relevante que permanece oculta y que es obtenida mediante intrusiones en equipos informáticos.

COMPARECENCIA DE **DON JAVIER CANDAU ROMERO, JEFE DEL DEPARTAMENTO DE CIBERSEGURIDAD DEL CENTRO CRIPTOLÓGICO NACIONAL,** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 713/001031 (S) y núm. expte. 212/001726 (CD)]. Sesión de 18 de septiembre de 2018.

El compareciente comienza explicando la organización y estructura del CCN organizado en dos departamentos: el de ciberseguridad y el de productos y tecnologías. Este último es el que desarrolla los productos de cifra para las fuerzas armadas, la Presidencia del Gobierno y los ministerios y en general para la Adminsitración General del Estado. Asimismo, señala que el CCN-CERT es el CERT gubernamental nacional cuya misión principal es apoyar a todo el sector público, Estado, Comunidades Autónomas y Entes Locales. Seguidamente señala que durante los 10 años de existencia del CCN-CERT se han desarrollado muchas herramientas de detección, auditoría y análisis, sobre todo se han llevado a cabo muchas acciones de formación. Seguidamente, afirma que España está tomando un papel líder en muchos países iberoamericanos con los cuales el CCN está ejerciendo un papel de liderazgo.

A este respecto, señala que son fundamentales los siguientes pasos a la hora de poner en pie una política pública de ciberseguridad. El primero es disponer de una estrategia. A continuación, es necesario

cve: BOCG-12-CG-A-276

establecer un modelo de gobernanza puesto que es muy importante establecer una normativa posibilista, es decir, un marco de medidas de seguridad de obligado cumplimiento, tarea para la cual señala la aplicación de la nueva directiva NIS será de una gran ayuda. A continuación es necesario tener una buena capacidad de detección.

Seguidamente, se refiere al modelo de gobernanza en España que tiene varios niveles: el técnico, el operativo, el estratégico y el político. Con la nueva directiva NIS se otorga al CCN-CERT el papel de coordinador cuando se produzca un incidente grave. Este modelo de gobernanza más la aplicación del Esquema de Seguridad Nacional coloca a España en estos momentos con un marco de gobernanza de los más avanzados dentro de la Unión Europea. A este respecto, señala también la obligatoriedad de realizar auditorías, requisito que no incluye la directiva NIS pero sí el Esquema de Seguridad Nacional. Seguidamente, se refiere a la necesidad de mejorar la capacidad de vigilancia, para ello señala que es imprescindible seguir desarrollando el sistema de alerta temprana de internet en el cual colaboran los organismos con carácter voluntario. A este respecto, comunica que también Congreso y Senado están incluidos dentro de este sistema.

Continúa señalando que otra prioridad debe ser la detección de talento y la capacitación. A este respecto el CCN forma todos los años a unos seiscientos funcionarios público en ciberseguridad. Esta formación se complementa con la impartida a través de la plataforma Atenea para hacer formación online. Por otra parte, indica que en el nuevo marco regulatorio la obligación de notificación de incidentes se ha vuelto algo compleja y por ello el CCN está trabajando en una plataforma de notificación única lo cual facilitaría el cumplimiento de este trámite, dicha plataforma ha sido denominada LUCÍA que permite que la notificación vaya directamente a la autoridad que lo necesita.

Por otra parte, y en cuanto a los motivos de ciberincidentes notificados en 2017, 27 000, señala que las principales preocupaciones no provienen tanto del ciberterrorismo sino que las notificaciones principales son el ciberespionaje, el ciberdelito, el ciberconflicto, la guerra híbrida, el ataque a infraestructuras críticas y la desinformación. Seguidamente pasa a dar detalles de la gestión del incidente WannaCry, incluida la elaboración de la vacuna contra ese virus denominada NoMoreCry.

Concluye su intervención señalando que es necesario sensibilizar al nivel de decisión política a mejorar las capacidades de vigilancia y de intercambio de información unido a la necesidad de proteger los datos y utilizar productos certificados, todo ello también en el marco de una cooperación público-privada mucho más extensa.

COMPARECENCIA DEL **SEÑOR HERNÁNDEZ GARCÍA (CORONEL DEL ÁREA TÉCNICA DE LA JEFATURA DE INFORMACIÓN DE LA GUARDIA CIVIL),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/001760 (CD) y núm. expte. 713/001042 (S)]. Sesión de 9 de octubre de 2018.

El compareciente comienza señalando los importantes cambios globales que se están produciendo en los últimos años y su influencia en el ámbito político, social y económico. Frente a ello, también señala que, como toda creación humana, estos cambios están siendo utilizados para satisfacer los ilícitos intereses de individuos fuera de la ley. Define la ciberseguridad como el esfuerzo coordinado de todos los actores públicos y privados que coadyuvan al libre ejercicio de los derechos y libertades en el ciberespacio. Entre sus prioridades están la protección de la privacidad, la integridad y el honor de las personas y la defensa de la propiedad privada.

Refiriéndose ya al ciberdelito señala las dificultades para combatirlo debido al factor geográfico que dificulta mucho la acción penal ya que hay que coordinar los derechos penales y procesales de diversos países. No obstante, existe un mecanismo muy potente sobre cibercriminalidad que es el Convenio de Budapest. En cuanto al ciberterrorismo, señala que, a día de hoy, es un riesgo de baja probabilidad pero de alto impacto si llegara a producirse; no obstante, debe ser considerado como un riesgo emergente.

Por otra parte, y en relación a la Guardia Civil, indica que su principal fortaleza en este ámbito, como en todos los demás, es la inquebrantable vocación de servicio al pueblo español. Otra ventaja evidente es el despliegue de la Guardia Civil que tiene implantación en todo el territorio nacional. Asimismo, señala que ya en el año 1996 se creó el grupo de delitos telemáticos, siendo una unidad pionera en Europa.

Por otra parte, señala que otra fortaleza consiste en que la Guardia Civil no utiliza herramientas comerciales sino que durante años se ha esforzado por dotarse de herramientas tecnológicas adaptadas a sus necesidades reales. A este respecto, señala que también tienen activados programas de detección,

cve: BOCG-12-CG-A-276

selección, formación y entrenamiento en todas las disciplinas vinculadas con la ciberseguridad dentro de la Guardia Civil.

En cuanto a las debilidades indica que el marco presupuestario es insuficiente para cubrir todas las necesidades. Asimismo, señala la necesidad de cubrir los recursos humanos hasta completar las plantillas previstas. En esta materia de selección de talento y recursos humanos considera que el concepto de ciber-reserva es una iniciativa muy interesante que puede paliar las carencias. En este sentido, continúa afirmando que es esencial la especialización con personal cada vez más cualificado en el marco de una formación de excelencia.

Concluye afirmando que la colaboración público-privada va a ser esencial puesto que más del 80 por ciento de las infraestructuras críticas son gestionadas por el sector privado y por ello hay que generar sinergias positivas entre ambos sectores. Termina diciendo que si bien hay que descargar de dramatismo todo lo relacionado con la ciberseguridad, es necesario tomarla en serio porque de ello depende la seguridad y el bienestar del futuro de la sociedad española.

COMPARECENCIA DEL **SEÑOR DIRECTOR DEL GABINETE DEL PRESIDENTE DEL GOBIERNO (REDONDO BACAICOA),** PARA PRESENTAR LA ESTRATEGIA DE SEGURIDAD NACIONAL 2017 Y EL INFORME ANUAL DE SEGURIDAD NACIONAL 2017. [Núm. expte. 212/001714 (CD) y núm. expte. 713/001029 (S)]. Sesión de 16 de octubre de 2018.

La comparecencia del Director del Gabinete del Presidente del Gobierno se produjo para presentar la Estrategia de Seguridad de 2017 no obstante, es necesario aportar las referencias que hizo a la ciberseguridad como materia esencial de actuación en el marco general de la Seguridad Nacional. En este sentido señaló que una de las prioridades de la nueva estrategia se refiere a la protección de las infraestructuras críticas. Esfuerzo en el cual se inscribe la aprobación del Plan Estratégico del Sector TIC que evidencia la preocupación por ciberataques de dimensión global.

En este sentido, afirma que los sistemas de información de inteligencia españoles han seguido monitorizando las acciones contra intereses españoles e intensificando la contrainteligencia en el ciberespacio. Por todo ello, se ha potenciado el sistema de atención temprana frente a ciberataques.

Por ello anuncia que se ha puesto en marcha la revisión de la Estrategia de Ciberseguridad Nacional de 2013. Esta revisión se debe fundamentalmente a la adaptación de nuestra normativa a la directiva NIS y a la necesidad de adaptar nuestras capacidades de prevención, detección y respuesta a las continuas y novedosas amenazas en el ciberespacio. También enuncia que se está preparando la puesta en marcha del Centro de Operaciones de Seguridad para la Administración General del Estado. Asimismo, indica que se ha procedido a crear una Comisión Permanente de Ciberseguridad para facilitar la coordinación interministerial en situaciones de gestión de crisis o incidentes.

COMPARECENCIA DEL **SEÑOR CUBEIRO CABELLO (CAPITÁN DE NAVÍO Y JEFE DEL ESTADO MAYOR DEL MANDO CONJUNTO DE CIBERDEFENSA, MCCD),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/001793 (CD) y núm. expte. 713/001065 (S)]. Sesión de 23 de octubre de 2018.

El compareciente comienza remontándose a los orígenes del mando conjunto de ciberdefensa como unidad militar. Señala que cinco años después España cuenta con una aceptable capacidad militar de ciberdefensa. Informa que está próximo a terminar las obras de un edificio que albergará el CERT del Ministerio de Defensa así como un simulador muy sofisticado con campo de maniobras virtual que sirve para llevar a cabo planes de formación y adiestramiento especializado.

Asimismo, muestra su satisfacción por los múltiples canales de cooperación tanto a nivel nacional como internacional, muy especialmente en el ámbito iberoamericano ya que el mando conjunto de ciberdefensa es también modelo de referencia para varios de esos Estados. Continúa afirmando que en el ámbito estatal se cuenta con una estructura adecuada de órganos de decisión que ya ha tenido ocasión de demostrar su eficacia en el marco de un modelo de gobernanza que funcione y en el que están claras las responsabilidades, cometidos y ámbitos de actuación.

Indica que existe en España una cultura de ciberseguridad que se plasma en datos tales como que España ocupa el 9.º puesto internacional y el 4.º europeo por número de empresas y organizaciones certificadas con la norma ISO-27001. Asimismo, se han incorporado nuevos tipos penales para responder al ciberdelito y hay una Fiscalía especializada en criminalidad informática. En este sentido, afirma que

cve: BOCG-12-CG-A-276

cybersecurity index otorga a España el séptimo puesto mundial en cuanto a ciberseguridad. Tras analizar las principales vulnerabilidades que se producen a la hora de defender sistemas de los ciberataques, señala que entre las medidas necesarias se encuentra la de conseguir que nuestra sociedad desarrolle una cultura de ciberseguridad intensa, empezando por introducir esta materia en el sistema educativo, es decir, en los colegios.

También hay que potenciar la ciberinteligencia como elemento fundamental para conocer al adversario y explotar lo que las nuevas tecnologías pueden ofrecer, tales como la inteligencia artificial, el blockchaim, la computación cuántica o el machine learning.

Para acometer este esfuerzo colectivo señala que hace falta un plan integral de ciberseguridad que aborde todos los aspectos implicados y permita identificar medidas concretas y asignación de responsabilidades, medios y recursos. Ello se enmarcaría en un necesario pacto de Estado sobre ciberseguridad que podría dar estabilidad y continuidad a este esfuerzo.

COMPARECENCIA DEL **SEÑOR COMISARIO PRINCIPAL DE POLICÍA NACIONAL Y DIRECTOR DE LA UNIDAD CENTRAL DE CIBERDELINCUENCIA ENCUADRADA EN LA COMISARÍA GENERAL DE POLICÍA JUDICIAL (PÉREZ PÉREZ),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/001819 (CD) y núm. expte. 713/001082 (S)]. Sesión de 8 de noviembre de 2018.

El compareciente comienza señalando que el ciberespacio se ha convertido en el canal vehículo por donde circulamos todos y por eso debemos protegernos. Precisamente, para eso, añade el Cuerpo Nacional de Policía en el año 1995 creó un grupo sobre criminalidad informática dentro de la policía judicial. A día de hoy, la unidad central de ciberdelincuencia, incardinada en la Comisaría General de Policía Judicial, se encarga de perseguir los delitos tecnológicos, tanto aquellos en los que se utiliza la red para hacer daño a otros equipos o sistemas como aquellos delitos tradicionales en los que internet es un instrumento para la comisión de dichos delitos.

Una de las conclusiones iniciales que hay que sacar es que en esta materia la ley siempre va por detrás de las tecnologías aunque se han producido avances sustanciales gracias a la modificación de la Ley de Enjuiciamiento Criminal llevada a cabo en 2015. A este respecto, ofrece algunas cifras que dan una imagen cierta de la dimensión del problema ya que en 2017 los delitos conocidos por la Secretaría de Estado de Seguridad en el ciberespacio alcanzan las 81 000 infracciones con un incremento del 22,1 por ciento respecto a 2016. De todos esos delitos, el 74,4 por ciento corresponden a estafas a través de internet y el 14 por ciento al delito de amenazas y coacciones. En consonancia con estos datos, la eficacia policial ha mejorado un 27 por ciento y el número de detenidos el año pasado ha sido superior a 4900 personas.

Insiste en la necesidad de que los hechos delictivos se denuncien aunque también señala que las empresas son reacias a ello porque supone reconocer formalmente un fallo de seguridad y lleva aparejado un coste reputacional. Además del objetivo operacional de perseguir el delito el compareciente indica que otro objetivo específico tiene que ver directamente con las personas, los internautas y la protección de los colectivos sociales más débiles a este respecto, como son la infancia, a través de la distribución de pornografía infantil. En este sentido, señala que su unidad detuvo el año pasado a 337 personas en relación con este tipo de delitos, algunas de ellas en operaciones coordinadas en varios continentes. A este respecto, cita dos operaciones, la «Operación Tantalio» y la «Telón de Acero».

Otro objetivo que centra los esfuerzos del Cuerpo Nacional de Policía en esta materia son los delitos de fraude informático que se han incrementado notablemente conforme la población ha empezado a comprar por internet.

En cuanto a las propuestas de mejora, insiste en que la formación es algo esencial. En este sentido, abunda en que es necesario incorporar a los planes de estudio asignaturas relativas a medios cibernéticos y los riesgos que entraña. Así, señala que el Cuerpo Nacional de Policía desarrolla contactos directos con colegios sobre nociones básicas de ciberseguridad para niños.

Por otra parte, también señala que hay que mejorar las herramientas forenses para el análisis y tratamiento de las evidencias digitales que se incautan en registros. Por último, destaca la participación de la unidad que dirige en dos proyectos de la Comisión Europea incluidos en el programa «Horizonte 2020» llamados «Titanium» y «Ramses» financiados por la Unión Europea con el objeto de crear una plataforma que permita almacenar y analizar tanto los malware financieros como las monedas virtuales.

cve: BOCG-12-CG-A-276

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. [Núm. expte. 212/001859 (CD) y núm. expte. 713/001099 (S)]. Sesión de 20 de noviembre de 2018.

La embajadora, Sra. Olmo, comienza haciendo referencia a las funciones que desempeña como embajadora en misión especial, siendo su principal empeño contribuir a mejorar y reforzar la presencia de España en las organizaciones, conferencias, foros internacionales y regionales de los que España forma parte con especial atención a la Unión Europea. Continúa afirmando que el ciberespacio es un espacio común global en el que no existen fronteras y en el que participan múltiples actores y del cual se derivan grandes oportunidades pero también múltiples amenazas.

Seguidamente, la embajadora hace un repaso de todos aquellos organismos internacionales que se han preocupado por asuntos relacionados con la ciberseguridad, como la OSCE, el Consejo de Europa, la OEA y las Naciones Unidas, respecto a esta última organización resalta la participación en el Foro para la Gobernanza en Internet, órgano del que surgió el denominado Llamamiento de París para la confianza y la seguridad en el ciberespacio ratificado por 60 países, entre ellos España, y más de un centenar de empresas, organizaciones, universidades y centros de pensamiento entre los cuales se cita el Real Instituto ElCano. También destaca la cooperación bilateral en esta materia con una decena de países mediante memorandos de entendimiento, entre otros, Argentina, Brasil, Chile, la India, Marruecos o Perú.

A continuación, realiza un repaso sobre las dificultades que el derecho internacional público encuentra a la hora de ser aplicado en el ciberespacio. A pesar de las dificultades, señala que hay que reafirmar la aplicabilidad del derecho internacional en el ciberespacio, lo cual incluye el respeto a los derechos humanos así como a la Carta de Naciones Unidas en su totalidad. Asimismo, afirma que si se ha producido un cierto parón en la regulación jurídica del ciberespacio se debe en parte a la existencia de dos concepciones diferentes sobre la soberanía aplicada al ciberespacio. Mientras unos países apuestan por su apertura, seguridad y estabilidad, otros se inclinan por la sola y exclusiva presencia de los Estados como actores exclusivos para gobernar la red.

Respecto a Europa, la estrategia de la Unión Europea en el año 2013 ha ido creando conciencia de la importancia de la ciberseguridad, ello ha motivado iniciativas como la Directiva NIS, el Reglamento General de Protección de Datos, el futuro Centro Europeo de Ciberseguridad y la creación y actual reforma de la Agencia Europea de Ciberseguridad (ENISA). Para lograr una acción más coordinada se está planteando reunir todos los fondos relativos a ciberseguridad, hoy dispersos en diferentes organismos y programas en un único centro europeo, ello significa que probablemente ese presupuesto alcance la cifra de los 2.700 millones de euros para el período 2020-2027.

Por otra parte, señala que el Consejo Europeo de 2017 afirmó que un ciberataque podía constituir base suficiente para que un Estado miembro invocara la causa de solidaridad del Tratado de Funcionamiento de la Unión, además el Presidente Juncker, en el último discurso del Estado de la Unión, señaló las prioridades para los próximos años que son la protección de datos, la transparencia y la cooperación europea y nacional incluida una red de cooperación electoral europea para prevenir irrupciones en los procesos electorales.

La embajadora concluye su exposición haciendo alusión a las amenazas híbridas entendidas como acciones combinadas, que pueden incluir junto al uso de métodos militares clásicos los ciberataques, las operaciones o campañas de intervención de la información u otras herramientas. La principal dificultad radica en atribuir esas acciones. En definitiva, se trata de problemas complejos que requieren soluciones complejas en las cuales la cooperación y un whole sociality aproach es necesario para tener garantía de éxito.

COMPARECENCIA DEL **RESPONSABLE DE OPERACIONES DEL CENTRO EUROPEO DEL CIBERCRIMEN (EC3) DE EUROPOL, DON FERNANDO RUIZ PÉREZ.** [Núm. expte. 713/001107 (S) y núm. expte. 219/001522 (CD)]. Sesión de 13 de diciembre de 2018.

El compareciente comienza explicando las funciones de Europol en esta materia que básicamente consisten en prestar apoyo a las unidades nacionales en la lucha contra el crimen organizado, el terrorismo y la ciberdelincuencia. Asimismo, se facilita el traslado de información entre agencias policiales lo cual permite cruzar toda esa información y alcanzar visiones globales. En el seno de Europol se encuentra el

cve: BOCG-12-CG-A-276

Centro de Lucha contra la Ciberdelincuencia que se organiza en tres áreas: una dedicada a los fraudes online, otra a los ciberdelitos y una tercera a los abusos sexuales de menores online. Señala también que recientemente se ha creado un equipo específico para perseguir la criminalidad dentro de la dark web.

Por otra parte, señala que entre las principales dificultades a la hora de perseguir el delito en el ciberespacio se encuentra la diversidad de marcos legales nacionales que supone, por ejemplo, que la figura del agente on line no es común a todos los países de nuestro entorno. También cita la lentitud de las comisiones rogatorias como otra dificultad para llevar a buen puerto las investigaciones judiciales.

Asimismo, indica que una de las principales dificultades reside en la mutabilidad de los delitos en la red que supone por ejemplo la existencia de servicios criminales que se prestan a otros delincuentes que pagan por ellos, como si fuese un servicio más al uso. Además de las acciones operativas Europol insiste en la necesidad de campañas de prevención.

Continúa describiendo dos operaciones contra el uso criminal de la dark web, en concreto Alphabay y Hansa, mercados ilegales cerrados el pasado año mediante una operación coordinada de Europol, en ese mismo ámbito de la dark web sitúa la lucha contra la pornografía infantil y el abuso sexual de menores que ha permitido identificar y rescatar a 241 víctimas de estas prácticas en todo el mundo. A este respecto, señala que resulta fundamental la colaboración del público en general mediante la técnica de extraer imágenes de objetos o lugares que se encuentran en esos vídeos y se pide al público en general que ayude a reconocerlos. El compareciente indica que esta práctica ha dado unos notables resultados a la hora de perseguir este delito. Concluye en definitiva indicando que la continua colaboración de todos los sectores involucrados es la clave del éxito.

COMPARECENCIA DEL **GLOBAL CISO, CHIEF INFORMATION SECURITY OFFICER AND TECHNOLOGY RISK, DEL GRUPO SANTANDER, DON DANIEL BARRIUSO ROJO,** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 715/000599 (S) y núm. expte. 219/001523 (CD)]. Sesión de 13 de diciembre de 2018.

El compareciente comienza afirmando que las amenazas sobre la ciberseguridad no pueden ser eliminadas; pueden ser gestionadas pero muy difícilmente eliminadas ya que se tratan de riesgos muy dinámicos y tiene ventaja siempre el que ataca. Continúa afirmando que la privacidad de los datos de los clientes del Banco Santander son la prioridad y que, por ello, el componente de la seguridad se sitúa al principio en el mismo diseño de los nuevos servicios. Describe, a continuación, cómo se concibe la seguridad informática en tres niveles: un primer muro que ayuda a proteger, un segundo muro que ayuda a detectar y un tercer muro que supone responder.

A este respecto, indica que el Grupo Santander está a punto de inaugurar un nuevo centro en España con más de 300 profesionales en esta materia. Incide en que es muy importante formar de manera continua a los empleados para que protejan la información que manejan. Esa concienciación considera que es necesario extenderla a toda la sociedad comenzando con los más pequeños, los niños, utilizando los medios de comunicación al alcance de todos. Por ello, propone crear una organización que coordine esas campañas de concienciación aunando esfuerzos público-privados.

Otro aspecto que destaca es la formación del talento ya que la demanda va a ser creciente en los próximos años. A este respecto, indica que si bien es cierto que la mayor parte de esta demanda consistirá en profesionales técnicos del mundo de las ingenierías, la ciberseguridad, cada vez más, es un elemento que necesita de otras profesiones, como el derecho, la criminología o la psicología. Para satisfacer esta demanda considera importante generar interés en edades tempranas en esta materia, tanto en la educación primaria como secundaria.

Respecto de la universidad, resalta que sería positivo desarrollar un currículum específico de ciberseguridad con una estrecha colaboración público-privada. En este esfuerzo es importante conseguir una mayor participación de las mujeres en las profesiones técnicas ya que en el ámbito de la ciberseguridad sólo el 11 por ciento de los profesionales son mujeres. En este sentido, el Banco Santander tiene un programa de becas dirigidas a mujeres relacionadas con el mundo de las tecnologías denominadas STEM.

Concluye afirmando que hemos de posicionar a España como un lugar seguro en el ciberespacio para atraer inversión y negocio online, en este sentido considera que la ciberseguridad no sólo es una amenaza sino una oportunidad.

cve: BOCG-12-CG-A-276

COMPARECENCIA DEL **SEÑOR DE LA CUEVA GONZÁLEZ-COTERA (ABOGADO Y DOCTOR EN FILOSOFÍA, PROFESOR ASOCIADO DE LA UNIVERSIDAD COMPLUTENSE DE MADRID),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001552 (CD) y núm. expte. 715/000616 (S)]. Sesión de 23 de enero de 2019.

El compareciente comienza señalando la importancia del código fuente e indica que su comparecencia se va a referir casi exclusivamente a esta cuestión. Comienza por resaltar la vinculación entre el código fuente y las normas jurídicas. Indica que no tener acceso al código fuente no es sólo una cuestión que afecta a la seguridad nacional sino que ni siquiera como ciudadano se tiene acceso para poder discutir una resolución que se hubiera podido fundamentar en la aplicación de un determinado tipo de software. En este sentido indica que la tecnología no es un imponderable al cual los ciudadanos tenemos que someternos sino que es la tecnología la que permite la actividad humana y si como ciudadanos podemos disponer de ese código fuente podremos ser sujetos conscientes y participar en el proceso de participación de la norma.

En este sentido, cita a Wittgenstein al afirmar que «los límites de mi lenguaje son los límites de mi mundo.» A continuación se refiere a los términos y condiciones de las aplicaciones informáticas que hacen que escapemos a los mecanismos de garantía jurisdiccional que sí disfrutamos offline.

Concluye afirmando que debe existir una regulación jurídica que determine la posibilidad de que los ciudadanos puedan tener acceso a la escritura del código fuente y de los algoritmos y ello porque el artículo 23 de la Constitución Española establece el derecho de participación de todos los ciudadanos.

Además, señala que es necesario que los códigos fuente y los algoritmos se publiquen en repositorios oficiales para que puedan ser leídos, de tal forma que el poder sea transparente para que evitemos la arbitrariedad, ya que como decía Kant cuando el Estado es transparente evita las guerras con otros Estados. En este sentido, concluye afirmando que la soberanía tecnológica de un Estado depende precisamente de su capacidad para ser transparente con respecto al código fuente de los programas que realizan las labores de gestión y control.

COMPARECENCIA DEL **SEÑOR CAVANILLAS DE SAN SEGUNDO (CHIEF BIG DATA & SECURITY OFFICER, RESPONSABLE DE CIBERSEGURIDAD DE LA EMPRESA ATOS),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 219/001553 (CD) y núm. expte. 715/000617 (S)]. Sesión de 23 de enero de 2019.

El compareciente inicia su exposición centrándose en las personas que pueden tener distintas motivaciones para actuar en el ciberespacio, que pueden ser políticas, económicas o incluso de actitud vandálica y de hacer daño por sí mismo. En cuanto al perfil social, puede ir desde el delincuente profesional hasta el insider que pretende hacer daño a la empresa u organización dentro de la que está. A continuación, el compareciente se centra en la seguridad de las pymes y autónomos que están totalmente desprotegidos por su incapacidad para invertir sumas de dinero en ciberseguridad. Señala que las pymes son un ámbito crítico para el funcionamiento de la economía española ya que el 99,8 por ciento son pymes y generan el 66 por ciento de los empleos.

Por otra parte, señala lo complicado que es gestionar equipos de personas con alta capacidad para frenar ataques y que en un momento dado pueden decidir acabar atacando a la misma empresa u organización para la que trabajan, por todo lo anterior propone como solución para mejorar la seguridad en las pymes que existe una serie de copago por esos servicios de ciberseguridad entre las comunidades autónomas y los propios interesados que permite a esas empresas acceder a esos servicios. Asimismo, señala la necesidad de crear un cuarto ejército, el ejército en la red, de tal forma que este nuevo ejército forme profesionales que defiendan a España en el ciberespacio y que tengan por delante una carrera militar.

Por otra parte, afirma que el ciberriesgo es tan reciente que la mayor parte de la gente todavía no ha aprendido a gestionarlo ya que sólo han pasado 31 años desde el primer delito informático, el gusano de Morris. Por último, concluye afirmando que es necesario crear centros de formación de alto rendimiento de profesionales en esta materia al estilo de una academia militar o de policía tal y como ya está haciendo China, que va a crear seis academias de este tipo.

cve: BOCG-12-CG-A-276

COMPARECENCIA DEL **SEÑOR BERMÚDEZ GONZÁLEZ (FISCAL DELEGADO ADSCRITO AL SERVICIO DE CRIMINALIDAD INFORMÁTICA DE LA FISCALÍA GENERAL DEL ESTADO),** PARA INFORMAR CON CARÁCTER GENERAL SOBRE LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/001895 (CD) y núm. expte. 713/001135 (S)]. Sesión de 23 de enero de 2019.

El compareciente señala que la ciberseguridad es una disciplina transversal que abarca una gran cantidad de campos, desde la psicología al derecho pasando por supuesto por la propia informática y las comunicaciones. Resalta la importancia del activo del talento, que según él, es fácil de encontrar siempre que se busque en los ámbitos adecuados.

Seguidamente, incide en la necesidad de aclarar el marco regulatorio que se establece a partir de la transposición de la Directiva NIS mediante el Real Decreto Ley 12/2018. A este respecto, solicita a la mayor brevedad posible la aprobación de su normativa de desarrollo. Tras otras consideraciones, se refiere al internet de las cosas como un factor importante de vulnerabilidad: cámaras de videovigilancia, electrodomésticos, etc.

También incide en que la nueva normativa debería tener en cuenta la Fiscalía como canal seguro de notificaciones de particulares que no quieran aprovecharse de las vulnerabilidades que descubren sino simplemente notificarlas. De esta forma, podría protegerles como denunciantes. En definitiva, solicita un mayor protagonismo de la Fiscalía en todo lo que tiene que ver en la protección de los datos de los ciudadanos. Concluye afirmando que la ciberseguridad es la gran amenaza no del futuro sino del presente cuando se transforma en ciberdelincuencia.

COMPARECENCIA DEL **SEÑOR SECRETARIO DE ESTADO DIRECTOR DEL CENTRO NACIONAL DE INTELIGENCIA (DON FÉLIX SANZ ROLDÁN),** PARA INFORMAR CON CARÁCTER GENERAL SOBRE LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/002361 (CD) y núm. expte. 713/001147 (S)]. Sesión de 14 de febrero de 2019.

El compareciente comienza indicando que si bien Internet ha traído consigo grandes avances para la humanidad también ha traído consigo importantes riesgos y amenazas, por lo cual, considera absolutamente adecuado que la Comisión Mixta de Seguridad Nacional estudie cuestiones relativas a la ciberseguridad dado que es uno de los grandes retos que los Estados tienen ahora mismo planteados.

Seguidamente, expone que según calculan los expertos, cerca de un 60 % del tráfico en Internet no está producido por personas sino por cosas, por ello el Internet de las cosas es una cuestión fundamental ya que se calcula que son ya 35 000 millones los dispositivos interconectados. Seguidamente, expone que en España se están haciendo a este respecto las cosas bien como demuestra la rápida gestión y solución durante los ataques del virus WannaCry. Así, expone que desde que se detecta el virus a las 13:30 horas de un viernes se tardaron apenas 5 horas en tener preparada la vacuna contra el virus que se colgó de la página web del CCN a las 17:40 horas de ese mismo día. Una hora después 600 000 personas se habían descargado la vacuna. Por otra parte, señala que también la Red sirve para otras muchas cosas que realizan actores maliciosos y pone como ejemplo de ello la intensa utilización de Internet como sistema de mando y control por parte del Daesh.

A continuación, enuncia cuáles son las prioridades del CNI-CCN en esta materia. La primera es proteger a las Administraciones Públicas, estatal, autonómica y local, pero también hay que proteger las infraestructuras críticas, la ciberseguridad de la defensa y la ciberseguridad de empresas y ciudadanos, tareas que corresponden a otros centros de la Administración. Por otra parte, señala que de la enorme cantidad de incidentes que se producen todos los años, solo algunos son realmente críticos. Se puede decir que se produce uno de estos ataques críticos cada 3 o 4 días. Insiste en el necesidad de que todos los elementos conectados a Internet deben contar con la ciberseguridad desde el momento de su diseño y fabricación solicitando incluso que se apruebe legislación al respecto impidiendo que elementos de software que no sean ciberseguros lleguen al mercado. Por otra parte, señala la importancia de instalar sondas que permitan hacer un seguimiento del tráfico de Internet y destaca las redes sondas instaladas por el CCN en la Administración española. A continuación, señala la importancia de que todos aquellos que reciben ataques importantes a pesar del coste reputacional, los notifiquen para que de esa forma se puedan tomar medidas al respecto.

Seguidamente, resalta la importancia de que exista algún tipo de normativa de carácter internacional que permita regular incluso los enfrentamientos entre Estados en el ciberespacio, siendo el ámbito de

cve: BOCG-12-CG-A-276

Naciones Unidas el más adecuado para llevar a cabo este esfuerzo del mismo modo que se ha conseguido una normativa internacional que regula la utilización de armas nucleares, bacteriológicas o químicas. A este respecto, señala que la gran dificultad es la atribución de los ataques, una atribución en la cual ni siquiera tenemos el 100 % de seguridad sobre esa atribución.

Concluye señalando que el éxito absoluto a la hora de proteger los intereses españoles en el ciberespacio no se puede garantizar ni en España ni en ningún otro país. Una ciberseguridad total es imposible pero también pone de manifiesto que de momento en España hemos sido capaces de afrontar con éxito los grandes ciberataques que se han producido en los últimos tiempos, dado que disponemos de un marco de gobernanza maduro y en funcionamiento y coordinado. También señala que es imprescindible que todas las instituciones confíen en el CCN a la hora de mejorar su ciberseguridad. Insiste en la necesidad de legislar con más intensidad sobre esta materia.

Termina indicando algunas de las principales cuestiones que deben ser tenidas en cuenta a la hora de incrementar la seguridad en el ciberespacio: el uso de los datos, el espionaje industrial y la inteligencia artificial, con los grandes desafíos éticos que supone. A este respecto, señala que la inteligencia artificial puede ser una herramienta importante a la hora de resolver el problema de las fake news. También indica que es necesario un mayor compromiso presupuestario por parte de los poderes públicos y mejorar la formación, clave en todo este proceso.

COMPARECENCIA DE **DON JAVIER LESACA ESQUIROZ (DOCTOR EN HISTORIA CONTEMPORÁNEA E INVESTIGADOR VISITANTE EN LA UNIVERSIDAD DE COLUMBIA),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA MEDIANTE EL SISTEMA DE VIDEOCONFERENCIA. [Núm. expte. 219/001551 (CD) y núm. expte. 715/000625 (S)] . Sesión de 14 de febrero de 2019.

El compareciente señala que su comparecencia se va a centrar en las metodologías de las campañas de desinformación que en estos momentos afectan a los sistemas de democracia liberal. Indica que la piedra angular de estos sistemas es una opinión pública libre y bien informada que tradicionalmente ha pivotado sobre instituciones públicas, medios de comunicación y ciudadanos. A principios del S. XXI ese esquema se fractura por la falta de confianza de los ciudadanos en las instituciones públicas, como indican las encuestas, y por la crisis de los medios de comunicación tradicionales. En este sentido, afirma que los algoritmos de las plataformas de comunicación no están favoreciendo un debate transparente sobre temas clave de la sociedad, lo que supone la polarización de los ciudadanos sobre esos temas clave. En este contexto, se produce un momento propicio para utilizar la desinformación como herramienta de enfrentamiento.

La comunicación se concibe así como un arma más en el conflicto cuyo objetivo es desestabilizar otros Estados. Por esa razón, algunos Estados están reconociendo que las campañas de comunicación forman parte de sus herramientas de guerra híbrida. El propio Gobierno de España en su propio sistema de seguridad nacional en el año 2017 ha reconocido como amenaza las operaciones de manipulación informativa.

A este respecto, indica que las guerras de desinformación tienen 4 pasos. El primero consiste en analizar y detectar las vulnerabilidades de un país considerado adversario. El segundo, la creación de narrativas que potencien esas debilidades. El tercero, creación de una red de medios propios ajena a los medios de comunicación tradicionales y que permitan actuar de manera directa en la audiencia. Y por último, el uso automatizado en las redes sociales para potenciar ese mensaje y que llegue a más audiencia.

En este sentido, señala el importantísimo papel que las redes de bots juegan en esta última fase. Para ello, pone el ejemplo del papel que ciertas cuentas en redes sociales están teniendo en el caso de los chalecos amarillos en Francia. Indica que en algunos de estos perfiles, se están produciendo 752 mensajes por día, lo cual indica un comportamiento no humano. Señala también el caso de varios perfiles denominados Iván226622, Rick888 o Bobbit, que fueron especialmente activos en la crisis de Cataluña, y que actuaron coordinadamente de forma tal que se puede deducir que en realidad, estaban siendo gestionadas por una sola persona real, ya que compartían constantemente los mismos contenidos manifiestamente falsos. Esos indicios permiten asegurar que esas cuentas que aparentaban ser humanas estaban al servicio de una institución u organización cuyo único afán era generar desinformación. El autor

cve: BOCG-12-CG-A-276

pone a continuación otros ejemplos de este tipo de operativa relacionados con el Estado Islámico o con asuntos de inmigración en Italia.

Concluye afirmando que la metodología de la disrupción o campañas de desinformación es un fenómeno más complejo que el de las noticias falsas.

COMPARECENCIA DE LA **SEÑORA SUBSECRETARIA DEL MINISTERIO DEL INTERIOR (DOÑA ISABEL GOICOECHEA ARANGUREN),** PARA INFORMAR SOBRE DIVERSAS CUESTIONES RELATIVAS A LA CIBERSEGURIDAD EN ESPAÑA. [Núm. expte. 212/002362 (CD) y núm. expte. 713/001148 (S)]. Sesión de 14 de febrero de 2019.

Comienza la compareciente señalando que se va a referir a las materias competencia del Ministerio del Interior en materia de procesos electorales. En este sentido, afirma que al asumir las responsabilidades ministeriales esta preocupación se puso en el centro de las actuaciones del Departamento. Por ello, se analizaron los antecedentes de los años 2015 y 2016 que habían sido analizados por el CCN detectando múltiples vulnerabilidades en todo el procedimiento. Sobre esta base, se aprobó el acuerdo marco utilizado como herramienta para la contratación de toda la infraestructura en materia electoral del Ministerio del Interior. En este acuerdo marco, la ciberseguridad es un componente fundamental.

En este sentido, afirma que para que las elecciones transcurran sin incidentes y con la máxima transparencia es necesario una acción coordinada de todos los órganos competentes en la Administración General del Estado. En este esquema será fundamental asegurar en materia de ciberseguridad una detección precoz y una capacidad inmediata de actuación. Estas necesidades ya se han contemplado en los pliegos de contratación siguiendo las sugerencias aportadas por el CCN, incluyendo la obligación de una auditoría de seguridad de las empresas que se han presentado a este procedimiento de contratación con carácter previo a la adjudicación. Este procedimiento culminó con la adjudicación del contrato el pasado 31 de enero a una UTE formada por las empresas Scytl y Vector.

Asimismo, señala que por parte del CNPIC se va a poner en marcha un dispositivo extraordinario de ciberseguridad que afecta a las infraestructuras críticas. Asimismo, se pretende apoyar a la Junta Electoral Central y a los demás actores que forman parte del proceso para tener conocimiento instantáneo de cualquier posible incidente. En definitiva, se trata de sumar todas las capacidades que aportan tanto el INCIBE como el Mando Conjunto de Ciberdefensa y el CCN así como las Fuerzas y Cuerpos de Seguridad del Estado. Por otra parte, señala que la Unión Europea está especialmente preocupada por estas cuestiones con ocasión de la aceleración de las elecciones al Parlamento Europeo, por lo cual ha creado una red nacional en materia de elecciones. Por último, señala que todas estas actuaciones y organismos de coordinación se pretende que se mantengan estables en el tiempo de forma tal que su activación sea inmediata en caso de convocatoria de procedimientos electorales.

Concluye afirmando que sobre el Ministerio del Interior se coloca una enorme responsabilidad por los sucesivos procesos electorales a punto de producirse pero que dicha responsabilidad se está abordando con un esfuerzo coordinado profesional y eficaz por parte de diversos organismos de la Administración General del Estado que están actuando al unísono.

V.2. **Documentación aportada por los comparecientes.**

Sesión del 23 de noviembre de 2017.

— De D.ª Mira Milosevich Juaristi, investigadora principal del Real Instituto Elcano y profesora asociada de Historia de Relaciones Internacionales del Instituto de Empresa (IE University) (núm. expte. 219/000906):

• La injerencia de Rusia en el referéndum ilegal de Cataluña (presentación powerpoint).

— Del General de División, Excmo. Sr. D. Carlos Gómez López de Medina, Jefe del Mando Conjunto de Ciberdefensa (MCCD) (núm. expte. 219/001048):

• Estrategia de seguridad nacional; estrategia de ciberseguridad nacional; el Mando conjunto de ciberdefensa (presentación de powerpoint).

cve: BOCG-12-CG-A-276

Sesión del 28 de febrero de 2018.

— De D. Xabier Mitxelena Ruiz, Security Iberia Lead en Accenture (núm. expte. 219/001044):

• Grow confidently (presentación powerpoint).

— De D. Jesús Romero Bartolomé, Socio responsable de soluciones de seguridad de PwC (núm. expte. 219/001045):

• Presentación powerpoint: Ciberseguridad en España. Retos y oportunidades.

Sesión del 12 de abril de 2018.

— De D. Fernando Picatoste, Socio Risk Advisory (Deloitte) (núm. expte. 219/001131):

• Presentación de powerpoint.

— Del General de División D. José Luis Goberna Caride, Subdirector general del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) (núm. expte. 212/001203):

• Presentación de powerpoint: Centro de sistemas de tecnologías de información y comunicaciones del Ministerio de Defensa.

Sesión del 24 de mayo de 2018.

— De D. Miguel Rego Fernández, Socio de iHackLabs (núm. expte. 219/001246):

• Presentación powerpoint: Talento y Emprendimiento en Ciberseguridad. Oportunidades y Riesgos.

Sesión del 28 de junio de 2018.

— De D. Carlos León de Mora, Director de la Cátedra Telefónica Inteligencia en la Red y Director del Grupo de Investigación Tecnología Electrónica e Informática Industrial (TIC-150) de la Universidad de Sevilla, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001289):

• Presentación powerpoint: Formación del Talento y el Impacto de la Inteligencia Artificial.

Sesión del 18 de septiembre de 2018.

De D. Javier Candau, Jefe del Departamento de Ciberseguridad del Centro de Criptológico Nacional, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/001726).

Sesión del 9 de octubre de 2018.

— De D. Luis Fernando Hernández García, Coronel del Área Técnica de la Jefatura de Información de la Guardia Civil, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/001760).

• Estado de la Ciberseguridad, visión de la Guardia Civil.

Sesión del 13 de diciembre de 2018.

— D. Fernando Ruiz Pérez, Responsable de Operaciones del Centro Europeo del Cibercrimen (EC3) de Europol, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 219/001522).

• Centro Europeo de Ciberdelincuencia (EC3).

cve: BOCG-12-CG-A-276

Sesión del 14 de febrero de 2019.

— Subsecretaria del Ministerio del Interior, para informar sobre diversas cuestiones relativas a la ciberseguridad en España (núm. expte. 212/002362).

• Presentación de Powerpoint.

VI. CONCLUSIONES.

Durante el desarrollo de los trabajos de la Ponencia, se han puesto de manifiesto una serie de hechos objetivamente contrastados que van a constituir la base de estas conclusiones y recomendaciones.

1. La profundidad y relevancia de los cambios que la disrupción digital está produciendo en los sistemas económicos, los sistemas políticos, los modelos comerciales y, en general, en las relaciones sociales, supone una transformación integral de la realidad que conocemos. Se trata de un fenómeno cuya característica más destacada es precisamente la transversalidad. Dada la ubicuidad de este cambio de paradigma civilizatorio se puede concluir que el modo en que los estados afronten los retos que plantea esta nueva situación van a ser decisivos a la hora de asegurar un futuro de estabilidad y progreso económico y social para los ciudadanos de esos países.

2. En este horizonte de cambios la preocupación por la seguridad en la red se ha convertido en una amenaza que debe ser tratada con la misma relevancia que otros riesgos que anteriormente se han planteado en situaciones de cambio como la actual. Por esta razón, lograr un adecuado nivel de ciberseguridad es una tarea prioritaria para las autoridades públicas y para la sociedad en general. En este contexto, la ciberseguridad se convierte en uno de los pilares de cualquier política de Seguridad Nacional que pretenda proteger los derechos fundamentales y libertades públicas, así como el bienestar económico de los ciudadanos. En este sentido, fenómenos tales como la criminalidad en la red, el ciberterrorismo o las amenazas a la estabilidad económica o a los sistemas políticos son cuestiones que necesitan ser abordadas desde un punto de vista legislativo, normativo, presupuestario y, en general, de organización administrativa. Ahora bien, esta tarea no solo corresponde a los poderes públicos; hace falta un enfoque holístico que implique a toda la sociedad para lograr que el increíble caudal de oportunidades, de desarrollo y generación de talento que ofrece la red no se malogre por aquellos actores que utilizan el ciberespacio para cometer crímenes, desestabilizar o desinformar.

3. Si bien en los últimos años se han llevado a cabo iniciativas que permiten hablar de un modelo de gobernanza de ciberseguridad que satisfactoriamente ha cubierto los objetivos en nuestro país, es necesario seguir avanzando. Según el organismo de Naciones Unidades para las tecnologías de la información y la comunicación (ITU), España ocupa el puesto 19.º del mundo por su compromiso con la ciberseguridad, y el 9.º dentro de la Unión Europea. Destaca especialmente, en este sentido, los esfuerzos que desde 2010 se llevan a cabo para la aplicación completa del Esquema Nacional de Seguridad así como la Ley de Protección de Infraestructuras Críticas del año 2011. A este respecto, también va a ser muy relevante el pleno desarrollo de la normativa relacionada con la transposición de la Directiva NIS. No obstante, en este sentido el entramada institucional constituido por CCN (Centro Criptológico Nacional), INCIBE (Instituto Nacional de Ciberseguridad), CNPIC (Centro Nacional de Protección de Infraestructuras Críticas), y Mando Conjunto de Ciberdefensa (MCCD) constituyen un conjunto coordinado de instituciones públicas cuyo objeto es velar por la ciberseguridad. A esto hay que añadir la acción operativa del Cuerpo Nacional de Policía y Guardia Civil en apoyo de la Fiscalía Especial de Delitos Informáticos que han visto incrementadas sus capacidades de investigación con la reforma de la Ley de Enjuiciamiento Criminal y del Código Penal en 2015.

4. No obstante, otra de las características del nuevo entorno cibernético son los cambios acelerados que producen en consecuencia la mutabilidad de las amenazas. Constituyen un hecho insoslayable que las normas jurídicas van por detrás de esos cambios acelerados, con la dificultad añadida que supone la ausencia de fronteras, marco en el cual se aplican las leyes, y otros aspectos centrales que configuran internet tales como el anonimato.

5. Todo ello lleva aparejada la conclusión de que, en estos momentos, la defensa de los derechos fundamentales y libertades públicas de los ciudadanos y de la estabilidad económica de los Estados, en gran parte, se pone en juego en el ciberespacio. Por esa razón, la ciberseguridad se convierte en uno de los pilares más importantes para garantizar la Seguridad Nacional de los países. Prueba de ello es que las recientes estrategias de Seguridad Nacional publicadas en los países de nuestro entorno, y en nuestro

cve: BOCG-12-CG-A-276

caso, la Estrategia de Seguridad Nacional de 2017 recogen ya la ciberseguridad como un ámbito preferente de actuación junto a otros ámbitos más tradicionales tales como los conflictos armados, el terrorismo, el crimen organizado, el espionaje, la inestabilidad económica, la vulnerabilidad energética y el cambio climático. A este respeto, durante los trabajos de la Ponencia se han identificado diferentes ámbitos en los cuales hay que incidir si se quieren afrontar con éxito los retos que plantea la seguridad en la red.

6. El primero de ellos es el de la regulación. Se ha planteado por parte de muchos de los comparecientes la necesidad de regular aspectos concretos aun no cubiertos por normas jurídicas. En concreto se ha apelado a la necesidad de aunar esfuerzos para lograr algún tipo de normativa internacional que regule el conflicto en el ciberespacio, adaptando las normas de Derecho internacional público a los nuevos escenarios de conflicto así como a las nuevas formas de transgresión del principio de no injerencia de la Carta de Naciones Unidas. Así mismo se ha insistido en que es importante la participación de España de forma proactiva en todos los foros internacionales a los que pertenece para lograr una gobernanza de la red que permita proteger el modelo de sociedad democrática y plural que tenemos como propio, todo ello de forma coordinada con los países de nuestro entorno. En este sentido se considera imprescindible que junto a los países de la Unión Europea juguemos un papel líder en lo que significa la defensa de una ciberespacio libre en el cual se garanticen los derechos fundamentales y en el que también se garantice la existencia de normas internacionales que permitan una gobernanza global de la red bajo los principios de cooperación y relaciones pacíficas entre Estados. Se considera prioritario alcanzar algún tipo de acuerdo en materia de Derecho Internacional Humanitario adaptando el Ius ad Bellum a las peculiaridades del conflicto en el ciberespacio.

7. Por ello es necesario que en el ámbito de Naciones Unidas, la Unión Europea, la OSCE, la OTAN y otras organizaciones internacionales en las cuales España participa, seamos capaces como país de generar consensos y aunar esfuerzos para asegurar la prevalecía de los principios que presiden en el ámbito físico las relaciones entre Estados también en el ámbito del ciberespacio. A este respecto, es especialmente relevante continuar desarrollando todas las potencialidades que el Convenio de Budapest del Consejo de Europa de 2001 ofrece.

8. Por otra parte, también se ha solicitado de forma reiterada por los comparecientes que se complete en la medida de lo posible el ordenamiento jurídico nacional con normas que doten de seguridad jurídica a las actuaciones en el ciberespacio. Especialmente se ha insistido en la necesidad de llevar a cabo un adecuado proceso de transposición de la Directiva 2016/1148 de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión conocida como Directiva NIS. Dicha transposición se produjo mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y en estos momentos se está tramitando como Proyecto de Ley en el Congreso de los Diputados. se ha puesto de relieve la importancia de completar cuanto antes esta tramitación y sobre todo la necesidad de aprobar seguidamente a esta ley ya a la mayor brevedad el reglamento de desarrollo de esta ley para aclarar alguna de las dudas de procedimiento que se plantean.

9. Asimismo, se considera conveniente la modificación del Código Penal para tipificar la figura de la suplantación de identidad en la Red. Asimismo, también se sugiere la necesidad de modificar la tipificación de los delitos de injurias y calumnias para permitir ejercer la acción penal una vez que el ofendido ha fallecido para que puedan ejercitarla herederos o familiares del mismo. Asimismo, podría estudiarse la procedencia de sancionar con pena de privación de utilización de Internet o de administrar páginas web para prevenir la reiteración de los comportamientos más graves a aquellos sujetos que han sido condenados por delitos, por ejemplo, el acoso a menores a través de Internet.

10. También ocupó un lugar destacado entre las recomendaciones de los comparecientes la necesidad de alcanzar acuerdos al más alto nivel político que permitan articular políticas públicas a corto y medio plazo para lograr una marco estable de actuación pública que además impliquen de forma coordinada al mayor número posible de Administraciones Públicas. Se cree adecuado alcanzar un cierto nivel de compromiso a los responsables políticos de las distintas fuerzas parlamentarias para alcanzar consensos en esta materia que necesita de acuerdos amplios que aúnen a la mayor cantidad de actores posibles.

11. En este sentido también fue destacable la casi unanimidad de todos los comparecientes a la hora de señalar la importancia que la disrupción digital va a tener en el mercado de trabajo. Se señaló de forma reiterada que se va a destruir empleo por la digitalización y robotización del modelo productivo, pero al

cve: BOCG-12-CG-A-276

mismo tiempo se pusieron de manifiesto las enormes posibilidades que se van a producir en cuanto a la generación de nuevas oportunidades de empleo en ámbitos laborales emergentes. Uno de estos vectores de crecimiento de nuevos empleos es precisamente la ciberseguridad ya que según diversas estimaciones la demanda de empleos en este sector se cifra en 3,5 millones en los próximos años dentro de la Unión Europea.

12. Para dar satisfacción a esta demanda de empleo de calidad es necesario poner en marcha diversas adaptaciones del modelo educativo que posibiliten la especialización en diversos niveles educativos tanto profesional como universitario. Es imprescindible en esta materia homologar las diversas titulaciones ahora existentes en materia de ciberseguridad para permitir la certificación de estándares comunes de formación. Todo ello conjugado con la necesaria flexibilidad que la dinámica de los avances vertiginosos en este ámbito impone. Esta iniciativa se entiende sin perjuicio del establecimiento de modelos de colaboración público-privada que permita la convergencia de demanda y oferta laboral, otorgando a las empresas especializadas del sector un papel cooperativo en estos esfuerzos. En este sentido se insiste en que el papel de las universidades será esencial en este proceso de transformación del que depende la generación una parte de los empleos del futuro. Y todo ello de forma transversal a todas las disciplinas de conocimiento, ya que si bien el esfuerzo más importante en esta materia corresponde a las disciplinas académicas técnicas y científicas, fue una constante a lo largo de las comparecencias el aserto de que la complejidad de la disrupción digital es de tal envergadura que hace falta incorporar conocimiento de otras disciplinas del saber como la psicología, la sociología o el derecho. Es necesario incorporar un enfoque integral para poder comprender y encauzar este nuevo paradigma digital que al final se dirige a servir a las personas, ya que la tecnología está a su servicio.

13. Por otra parte, se ha puesto de manifiesto en reiteradas ocasiones la necesidad de conseguir una mayor participación de las mujeres en este sector de actividad tecnológica, ya que ahora existe una muy baja representación de mujeres en actividades relacionadas con la ciberseguridad. Es necesario atraer todo el talento posible hacia esta área y por ello se considera fundamental fomentar la formación, participación y emprendimiento de la mujer en el ámbito de la ciberseguridad. En este sentido se considera imprescindible poner en marcha políticas públicas que favorezcan todas las iniciativas que en esta dirección se pongan marcha ya sean formativas, educativas o de investigación, para lograr mayores cotas de participación desde la perspectiva de género en el sector de la ciberseguridad.

14. También ha sido constante la apelación a la creación de mecanismos adecuados de gestión del talento. En el sector de la ciberseguridad el elemento más relevante es el talento de los profesionales. Como se puso de manifiesto en diversas comparecencias España es un país que genera mucho talento en este sector pero es necesario mejorar las herramientas de detección del mismo y asegurar el desarrollo de carreras profesionales acordes con esas capacidades. Por ello se propuso crear sistemas de detección de talento en todos los niveles educativos pero especialmente en la educación secundaria. Sería muy positivo poder orientar a aquellos escolares especialmente dotados en estas materias a que encaminen sus estudios universitarios o profesionales hacia el sector de las tecnologías de la información como garantía de generación de la necesaria masa crítica de capacidades y aptitudes que permitan situar a España entre los países en cabeza en materia de investigación y desarrollo en este sector.

15. Por otra parte, también se hizo referencia a la necesidad de articular políticas públicas en materia de ciberseguridad dirigidas específicamente a las pequeñas y medianas empresas y a los autónomos. La inmensa mayoría de las empresas españolas son PYMES y una parte importante del empleo es generado por estas. Por sus características, este tipo de empresas en muchas ocasiones no pueden permitirse ni el asesoramiento ni los equipos ni los sistemas necesarios para evitar intrusiones que en algunos casos pueden suponer un grave golpe para la viabilidad de esos negocios. Si bien ya existen actuaciones en esta materia a cargo de INCIBE, se estima necesario incrementar esas actuaciones para llegar al máximo número posible de estos pequeños empresarios y autónomos. Para ello habría que articular mecanismos de apoyo en los que participen también las Comunidades Autónomas junto con la Administración General del Estado en un esfuerzo de cooperación y coordinación que genere sinergias.

16. Otro ámbito de actuación que se ha destacado por todos los comparecientes es la necesidad de llevar a cabo políticas públicas que generen una cultura de ciberseguridad en toda la sociedad; desde los directivos de empresas hasta los ciudadanos de a pie. Este tema se asocia íntimamente con el de la alfabetización digital. La disrupción digital ha sido tan intensa y en tan poco tiempo que en cierto sentido y con carácter general no hemos podido adquirir las herramientas intelectuales y habilidades necesarias para desenvolvernos en este ámbito con las garantías precisas de libertad de criterio y de conocimiento

cve: BOCG-12-CG-A-276

del entorno que ya disfrutamos en el mundo físico. Esto es especialmente cierto cuando nos referimos a los colectivos sociales más vulnerables; infancia y personas mayores, especialmente estos últimos que carecen de la soltura necesaria en este nuevo entorno de la que sí disfrutan los nativos digitales. Por ello, se considera prioritario emprender acciones por parte de los poderes públicos que incentiven la concienciación sobre los peligros que se esconden en la red, así como la adquisición de un conocimiento más profundo de la realidad digital que nos rodea pero que en ocasiones no sabemos cómo se configura. En este sentido habría que emprender acciones formativas y de difusión pública a varios niveles; desde lo más sencillo y elemental, hasta los niveles más complejos. En este último caso sería recomendable que también los usuarios intermedios, la gran mayoría de los ciudadanos, tuviesen acceso a la comprensión de cuestiones más complejas tales como el código, los algoritmos o la inteligencia artificial.

17. Solo un adecuado nivel de desarrollo de esta cultura de la ciberseguridad nos dará las herramientas necesarias para hacer a la sociedad en su conjunto mucho más resiliente ante los ataques malintencionados de aquellos que quieren usar la red para cometer delitos o llevar a cabo campañas de desinformación. El elemento más vulnerable de un sistema en estos casos siempre es el elemento humano y la mejor forma de proteger es educar y concienciar. Por esta razón el pilar de la cultura de ciberseguridad se considera clave en la Estrategia de Seguridad Nacional y permite por otro lado asegurar la protección de una ciudadanía informada y consciente de las amenazas. Es prioritario potenciar el sentido crítico y la responsabilidad, como herramientas eficaces para enfrentarse a la complejidad que supone el dominio digital, logrando así que los ciudadanos titulares de derechos y libertades fundamentales sean también protagonistas en el dominio virtual, como no puede ser de otra forma, en un Estado social y democrático de Derecho.

18. Por todo ello, se propone elaborar un plan de difusión de la cultura de ciberseguridad que abarque todos los canales formativos e informativos posibles y que llegue a todas las capas sociales. En cuanto a niños y jóvenes los centros educativos deberían introducir espacios de formación en esta materia del mismo modo que ya se llevan a cabo esfuerzos en materia de seguridad vial. En cuanto a otras capas de población, la implicación de los medios de comunicación, especialmente las televisiones públicas, deberían formar parte de este esfuerzo combinado. Asimismo, también las redes sociales podrían tener una participación relevante en este esfuerzo formativo, ya que es el canal primario de comunicación e información de las generaciones más jóvenes.

19. También se puso de manifiesto con reiteración que en todos los esfuerzos que se lleven a cabo para mejorar el nivel de ciberseguridad en España la colaboración Público-privada será decisiva. La cooperación entre ambas esferas será crucial dada la necesidad de actuar en red y de forma muy rápida en la gestión de ataques graves como se ha visto recientemente. Especialmente clave en este sentido es la cooperación público-privada en el ámbito de la gestión de las infraestructuras críticas, ya que el 80 % de estas son propiedad de empresas privadas. Es también esencial esa colaboración en lo que se refiere a la necesidad del desarrollo de herramientas informáticas para el sector público. En este sentido es también importante aunar esfuerzos para lograr el objetivo de reducir la dependencia exterior en esta materia, en la medida de lo posible, tanto para fomentar la investigación y producción española, como para incrementar el nivel de ciberseguridad de los sistemas redes y equipos desplegados en España.

20. Por otra parte, también se ha insistido en la necesidad de implantar unas obligaciones de ciberseguridad en el internet de las cosas (IoT) que contemple la obligatoriedad de homologaciones o certificaciones de productos antes de ser puestos a la venta en el mercado. Solo así será posible lograr que fabricantes y productores contemplen la ciberseguridad no como algo añadido con posterioridad al proceso productivo sino como una parte decisiva en las fases iniciales de diseño de productos. De esta manera se podrían mitigar en gran parte las numerosas vulnerabilidades que hoy afectan a una parte importante de los dispositivos conectados en lo que se denomina el internet de las cosas. Una buena forma de comenzar a potenciar esta línea de actuación sería introducir estándares de homologación y certificación de ciberseguridad en las políticas de compras públicas.

21. Se puso de manifiesto también la necesidad de complementar la Estrategia de Seguridad Nacional con un Plan operativo sobre mejora de la ciberseguridad que articulase en un solo documento una gran cantidad de actuaciones en todos los ámbitos que se han ido describiendo anteriormente. Dicho Plan debería contar con el más amplio apoyo institucional posible y debería contar con un cuantioso apoyo presupuestario. El compromiso con la ciberseguridad se plasmaría así en líneas concretas de actuación dotadas cada una de ellas con fondos suficientes para alcanzar objetivos concretos y medibles con un horizonte temporal fijo. Junto a este Plan de actuación debería contemplarse la posibilidad de asociar a

cve: BOCG-12-CG-A-276

esas líneas de acción concreta a otros actores que coadyuven a alcanzar los objetivos marcados tales como medios de comunicación, redes sociales, empresas informáticas, prestadores de servicios digitales, universidades, centros de pensamientos, centros educativos o asociaciones empresariales o sindicales. En definitiva, aunar esfuerzos colectivos que tengan como meta situar a España en el puesto que le corresponde entre los países de nuestro entorno en materia de ciberseguridad y que al mismo tiempo se pueda convertir en referencia en este ámbito para otros países especialmente en el contexto Iberoamericano.

22. Por último, también se puso de manifiesto la necesidad de que en el nuevo ámbito digital mantengamos como ciudadanos las mismas libertades y derechos que disfrutamos *offline*. En un Estado social y democrático de Derecho como el ciudadano y sus libertades deben estar en el centro mismo de todas las actuaciones de los poderes públicos. La libertad de expresión y de información constituyen el núcleo de un Estado democrático, e internet ha demostrado ser un eficaz medio de difusión y expresión de ideas. Esa libertad debe ser preservada contra los intentos de limitarla. Un ciberespacio libre de intervenciones abusivas por los Estados es la razón misma del éxito de la red como medio para expresar la creatividad y el talento que reside en el espíritu humano. Internet es el medio más poderoso para permitir el desarrollo de todas esas potencialidades de un modo democrático y equitativo posibilitando el progreso de la Humanidad a todos los niveles. Ahora bien, todas esas potencialidades se podrían ver malogradas si no conseguimos un adecuado nivel de seguridad en la red del mismo modo que necesitamos un adecuado nivel de seguridad en la vida real fuera de la red. Si bien es cierto como se ha afirmado constantemente a los largo de los trabajos de esta Ponencia que hoy por hoy es imposible garantizar por ningún actor o ningún Estado, una ciberseguridad total, lo cierto es que deberemos alcanzar un equilibrio, un compromiso, entre la libertad que ahora disfrutamos en internet y la seguridad que ahora exige este fenómeno global del ciberespacio que ha cambiado nuestras vidas.

cve: BOCG-12-CG-A-276