XXXII SEMINARIO INTERNACIONAL
DE SEGURIDAD Y DEFENSA

AMENAZAS DESDE EL CIBERESPACIO

XXXII SEMINARIO INTERNACIONAL
DE SEGURIDAD Y DEFENSA

AMENAZAS DESDE EL CIBERESPACIO

Madrid, 17 y 18 de septiembre de 2020

Edición a cargo de
Miguel Ángel Aguilar y Juan de Oñate

Asociación de Periodistas Europeos

Coordinación
Juan de Oñate

Transcripción de textos
Antonio Carrasco

Fotografías
Fernando Sánchez

Diseño y producción editorial
Exilio Gráfico

Impresión
Gracel

Impreso en España

Depósito legal: M-3586-2021

ÍNDICE

Si nos viéramos obligados a señalar un rasgo que describiera la época actual en su totalidad, haríamos como Luciano Concheiro (*Contra el tiempo*. *Filosofía práctica del instante*, 2016) y, sin dudarlo un segundo, elegiríamos la aceleración. Porque cada etapa histórica se distingue por una determinada manera de experimentar el tiempo y la que estamos viviendo es la de la aceleración. Es el incremento de la velocidad lo que explica en buena medida cómo funcionan hoy en día la economía, la política y las relaciones sociales y lo que permite que entendamos un poco mejor este mundo y a quienes lo habitamos. Percibimos una sucesión de eventos que se superponen y reclamamos que esa serie continúe. Como en la viñeta de El Roto de un primero de año donde se leía en la pancarta que encabezaba la multitud: «¡Queremos mentiras nuevas!».

El sociólogo Harmut Rosa distingue tres planos de aceleración: el de los desarrollos tecnológicos, el de los cambios sociales y el del ritmo de vida diaria. Explorar la aceleración nos lleva a comprender cómo ha sido utilizada para la obtención de ganancias, en línea con el denominado «capitalismo de la vigilancia» (Shoshana Zuboff, 2020), que desvía la atención y confunde a la opinión pública mezclando imperativos comerciales con la inevitabilidad tecnológica. En cuanto al efecto amnésico de la velocidad, su mejor descripción se encuentra en *La lentitud*, la novela de Milan Kundera donde se recupera nuestra experiencia de viandantes que se detienen para gozar al sobrevenirles un recuerdo agradable y aceleran el paso para disipar la memoria de algo que nos apena.

De modo que los acontecimientos se suceden de modo acelerado con velocidad creciente, desbordando nuestra capacidad para asimilarlos, mientras la tecnología, que favorece grandes logros y avances para la sociedad, provoca también nuevos riesgos y amenazas en distintos ámbitos, incluido el de la seguridad y la defensa. Veníamos de las denominadas guerras limpias donde, como precisó Salomé Zuravichvilli en nuestro seminario de junio de 2001, éramos capaces de causar daños insoportables al enemigo sin sufrir bajas propias. Pero estas asimetrías tuvieron como respuestas el más sucio de los terrorismos y, enseguida, ese panorama se vio alterado, por una revolución tecnológica que cambió el escenario y el desarrollo de los conflictos.

El campo de batalla se desplazó al ciberespacio y a los ejércitos tradicionales se sumaron nuevos agentes convencionales, hasta ahora ajenos. El objetivo último de doblegar la voluntad del adversario permaneció inalterable pero los medios para alcanzarlo pasaron a gravitar sobre las infraestructuras críticas con el objetivo de alterar suministros imprescindibles o de percutir de manera indirecta a través de empresas, bancos o instituciones teóricamente ajenas al conflicto. La presión sobre los no combatientes con objeto de alterar la moral del enemigo es un clásico, bajo distintas modalidades, desde la más remota antigüedad.

Las ciberagresiones son relativamente anónimas –su autoría resulta difícil de adjudicar– y para contrarrestarlas se utiliza una gradación de contrataques que pretenden salvaguardar la seguridad propia al tiempo que inducen temor en el adversario, creando una espiral de antagonismo, una suerte de «ciberguerra fría» que guarda algunas analogías con la carrera armamentística y la escalada de misiles nucleares en la que compitieron Estados Unidos y la Unión Soviética en los años ochenta y que, por virtud de la MDA (Mutua Destrucción Asegurada), tuvo el efecto de disuadir a ambas superpotencias del empleo del arma nuclear.

Los ciberataques permanentes, multidireccionales y maliciosos tienen el propósito final de alterar el modo de vida de los

ciudadanos y de desintegrar las democracias. Entre las distintas maneras de las que se sirven estos ciberataques para erosionar los cimientos de las sociedades enemigas destaca el recurso a la desinformación, la mentira y la manipulación informativa. La pandemia que ha asolado el mundo en el año 2020 ratifica que la diseminación de la falsedad en dosis masivas puede resultar un arma altamente peligrosa. Como subrayó el Alto Representante para la Política Exterior y de Seguridad y vicepresidente de la Comisión de la Unión Europea, Josep Borrell: «En el mundo actual, impulsado por la tecnología, los guerreros empuñan teclados en lugar de espadas y las operaciones de influencia y campañas de desinformación constituyen un arma reconocida de los agentes estatales y no estatales».

La proliferación de mensajes e informaciones falsas, orquestadas estratégicamente, puede desestabilizar un país, polarizando su sociedad o fomentando el aumento de populismos cainitas en su seno. Estos abusos resultan corrosivos para los valores democráticos y son susceptibles de debilitar instituciones u organismos nacionales e internacionales. Para combatir la mentira interesada de nada sirven los escudos antimisiles ni los cortafuegos informáticos, sino el periodismo que una ciudadanía crítica ha de exigir. El periodismo de la verdad, el periodismo de la contextualización y el rigor, el periodismo que, frente a la inundación informativa que nos asola, hace de planta potabilizadora y nos proporciona el agua potable de la verificación.

Estas «Amenazas desde el ciberespacio» fueron abordadas en el XXXII Seminario de Seguridad y Defensa que la Asociación de Periodistas Europeos convocó en el mes de septiembre, superada la primera ola de la pandemia y a punto de iniciarse la segunda. Nos habíamos visto obligados a posponer el encuentro previsto para junio y adaptarlo a las nuevas circunstancias dotándolo de un carácter semipresencial, con un aforo muy reducido y su emisión por *streaming* a través de distintas redes sociales. También tuvimos que cambiar la sede de su celebración y, por se-

gunda vez desde que se iniciara la serie en 1983, el encuentro salió de Toledo trasladándose a un lugar impregnado de historia y de defensa de las libertades, donde estuvo la redacción del periódico *El Sol*, que ahora da asiento a la Fundación Diario *Madrid*.

Ésa es la patera que acoge a los náufragos de aquel periódico *Madrid*, que como trabajadores dieron ejemplo admirable anteponiendo la lucha por las libertades a la mera preservación de sus puestos de trabajo, actitud de la que les sobrevino el despido y el cierre del periódico, que anduvo falto de calor en el elogio a Franco. La Fundación Diario Madrid heredera de aquel naufragio es la que acogió la edición XXXII del Seminario Internacional de Seguridad y Defensa, centrado en la idea de que, en el nuevo panorama internacional, en la guerra híbrida, en la geopolítica de la desinformación, la mentira mata.

Vaya nuestro agradecimiento a todos los participantes en el encuentro: el Almirante Juan Francisco Martínez Núñez, Secretario General de Política de Defensa (SEGENPOL); Paz Esteban, directora del Centro Nacional de Inteligencia (CNI); el General Miguel Ángel Ballesteros, director del Departamento de Seguridad Nacional (DSN): el General Félix Sanz Roldán, ex JEMAD y exdirector del CNI; el General Rafael García Hernández, Comandante del Mando Conjunto del Ciberespacio (MCCE); Rosa Díaz, directora general del Instituto Nacional de Ciberseguridad (INCIBE); Luis Jiménez, subdirector general del Centro Criptológico Nacional (CCN-CERT); Madeline Mortelmans, directora principal para Política de Ciberseguridad del Departamento de Defensa de Estados Unidos; Mario Esteban, investigador principal del Real Instituto Elcano; Ignacio Ramos, profesor de Relaciones Internacionales y delegado para Asuntos Chinos de la Universidad Pontificia Comillas; el Coronel Carlos Javier Frías, doctor en Paz y Seguridad Internacional y colaborador del Instituto Español de Estudios Estratégicos (IEEE); María Elena Gómez Castro, Directora General de Política de Defensa (DIGENPOL); Carmen Romero, subsecretaria general adjunta de Diplomacia Pública de la OTAN; el General Francisco José Dacoba, director del Instituto Español de Estudios Estratégicos (IEEE); y la ministra de Defensa, Margarita Robles.

Gracias también a los periodistas encargados de moderar y activar las sesiones. Fueron Montserrat Domínguez, subdirectora de *El País;* Javier García Vila, director de Europa Press; Ángel Gonzalo, jefe de Internacional de Onda Cero; Javier Fernández Arribas, director de *Atalayar*; Georgina Higueras, excorresponsal de *El País* en Asia-Pacífico; y Rafael Panadero, jefe de Internacional de la Cadena SER.

Es obligado también expresar nuestro reconocimiento a la Secretaría General de Política de Defensa del Ministerio de Defensa, a la Junta de Comunidades de Castilla-La Mancha, a El Corte Inglés y a Indra por su patrocinio para que el XXXII Seminario Internacional de Seguridad y Defensa fuera posible, con la esperanza de seguir mereciendo su confianza.

MIGUEL ÁNGEL AGUILAR Y JUAN DE OÑATE
Madrid, diciembre de 2020

ALMIRANTE JUAN FRANCISCO
MARTÍNEZ NÚÑEZ
Secretario General de Política de Defensa
(SEGENPOL)

MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación
de Periodistas Europeos (APE)

MONTSERRAT DOMÍNGUEZ
Vicepresidenta de la Asociación de
Periodistas Europeos y subdirectora de *El País*

Miguel Ángel Aguilar, Montserrat Domínguez
y el Almirante Juan Francisco Martínez Núñez

MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación de Periodistas Europeos

Vamos a dar comienzo a este trigésimo segundo Seminario de Seguridad y Defensa, bajo el título «Amenazas desde el ciberespacio». Antes, quiero explicar brevemente la constancia del seminario y su punto de ignición, que se remonta al año 1983. Veníamos entonces tratando de atenuar o reconvertir con el General Gutiérrez Mellado la pésima relación que existía entre las Fuerzas Armadas y la prensa, entre los militares y los periodistas. La idea generalizada entre los periodistas era que los militares –todos los militares– eran golpistas, y la idea generalizada entre los militares era que todos los periodistas eran unos hijos de puta. Entonces, conversando con el General, pensamos que hacía falta establecer un ámbito de proximidad para intentar desactivar esos recelos tan fuertes. Y así empezó este seminario, que siempre se ha desarrollado en el Parador de Toledo. Hasta hoy, la única excepción fue una edición que se celebró en Segovia y que recuerdo trataba de «Euromisiles y pacifismo». Desde entonces, hemos ido abordando en cada seminario asuntos de mayor temperatura y cada uno de ellos ha sido grabado y posteriormente transcrito, editado y publicado, dando lugar a una colección que permite seguir cuáles han sido los principales asuntos que han ido jalonando esos años, siempre procurando convocar y tener como ponentes a personalidades relevantes del mundo de las Fuerzas Armadas, de la universidad, del mundo de los *think tanks* y del mundo de los periodistas.

Nadie nos lo ha puesto fácil, pero ahí está la trayectoria de estos seminarios. Digo que no ha sido fácil porque para hablar de estos asuntos no basta con tener una idea, no basta con trazar un proyecto, no basta con hacer un presupuesto, sino que también hay que conseguir que alguien lo pague. No quiero engañarles a ustedes. Sepan que las asociaciones de periodistas no son exactamente como la CEOE o el Círculo de Empresarios. O sea,

que las cuotas de los miembros no dan para mucho. Por eso, cada vez que se hace algo hay que buscar quien lo sostenga. Por eso, quiero agradecer el apoyo del Ministerio de Defensa y agradecérselo personalmente al Almirante Juan Francisco Martínez Núñez, Secretario General de Política de Defensa, el SEGENPOL, que está aquí con nosotros. Ha sido extremadamente grato trabajar junto a él estos últimos años, encontrando los temas, encontrando los ponentes, alentándonos en esta tarea...

También quiero agradecer su apoyo a Indra y El Corte Inglés. Aunque este año estamos sometidos a las limitaciones que todos conocen, éstas han sido un incentivo para que se interese mucha más gente. En los últimos años hemos estado bastante desbordados pero éste, si cabe, lo estamos aun más. Al saberse que el número de participantes presenciales iba a ser muy limitado, la avalancha de gente que ha querido incorporarse ha sido enorme. Para todos ellos se ha generado este sistema de *streaming* que les va a permitir seguir en directo lo que aquí se celebre.

Aprovecho para decir que tienen ustedes a su disposición el volumen que corresponde al anterior seminario, que celebramos en el mes de junio del 2019. Yo creo que fue muy acertado el título y la orientación que le dimos: «OTAN. El vértigo de la retirada americana». Un vértigo en el que todavía estamos y no sabemos por cuánto tiempo, porque todo esto tiene que ver con las elecciones a la presidencia de Estados Unidos, que como saben serán en noviembre. La descripción de ese escenario que aparecería después de la retirada americana fue un ejercicio de extraordinario interés y en el que participaron ponentes de máximo relieve, como también ocurrió en el seminario anterior, «La guerra híbrida. La mentira como arma y la verdad, como víctima», que también estuvo muy en la línea de las preocupaciones que todavía permanecen en primerísimo plano.

En esta convocatoria nos vamos a ocupar de las amenazas que nos llegan desde el ciberespacio, que se ha convertido en un nuevo ámbito de confrontación.

En la actualidad, entre las gentes que compiten en este espacio, el objetivo sigue siendo doblegar la voluntad del adversario, aunque ahora con otros medios, que gravitan sobre infraestructuras críticas o la alteración de suministros imprescindibles y que buscan incidir en el modo de vida de las sociedades para desintegrar la democracia. Llegados aquí, debemos hacer una referencia a esta plaga de la COVID-19, que ha ratificado que la diseminación de la falsedad en dosis masivas puede resultar una de las armas más peligrosas: falsedades de destrucción masiva. Como subrayó Borrell: «En el mundo actual, impulsado por la tecnología, los guerreros empuñan teclados en lugar de espadas y las operaciones de influencia y campañas de desinformación constituyen un arma reconocida por agentes estatales y no estatales».

A lo largo de las sesiones que se celebrarán estos dos días, y que concluirán con la intervención de la ministra, van a ir sucediéndose conferencias, mesas redondas y conversaciones con ponentes de primerísimo nivel de nuestro país y con algunas aportaciones excepcionales procedentes de otros países.

Eso es básicamente lo que quería decir antes de dar paso a nuestra vicepresidenta, Montserrat Domínguez.

MONTSERRAT DOMÍNGUEZ
Vicepresidenta de la Asociación de Periodistas Europeos
y subdirectora de *El País*

Yo solamente quería agradeceros vuestra presencia a todos los que estáis aquí y a los que nos estáis siguiendo *online*, porque es verdad que éste ha sido un éxito de convocatoria increíble teniendo en cuenta las circunstancias. Volveremos a Toledo pronto, entre otras cosas porque buena parte del éxito de este seminario no solamente es la calidad de los intervinientes, de los debates y de los coloquios, sino también el microclima que se crea durante la convivencia. Además de lo que podemos luego consultar en los vídeos y en las publicaciones del seminario, ese cli-

ma que se crea es el que nos permite profundizar en estos asuntos que nos preocupan.

Me gustaría insistir en que todos los que nos están siguiendo *online* también pueden participar enviando sus preguntas, que trataremos de recoger al final de cada coloquio. Sin duda constituye un éxito de adaptación poder hacer este seminario de forma semivirtual, semipresencial, lo cual demuestra eso que se dice en biología, que lo importante no es ser el más fuerte sino el que más rápidamente o mejor se adapta a las circunstancias hostiles. La que estamos viviendo es una situación claramente hostil y este seminario, como tantas otras cosas, demuestra nuestra capacidad de adaptación. Sin más dilación, le cedo la palabra al Almirante Juan Francisco Martínez.

ALMIRANTE JUAN FRANCISCO MARTÍNEZ NÚÑEZ
Secretario General de Política de Defensa (SEGENPOL)

Buenos días, secretaria de Estado. Buenos días a todos los presentes y a los que nos siguen por *streaming* y, si me lo permiten, un saludo especial los amigos que nos siguen desde el otro lado del océano Atlántico. En primer lugar quiero agradecer a la Asociación de Periodistas Europeos, en las personas de Miguel Ángel Aguilar y Montserrat Domínguez, su compromiso y tesón a lo largo de treinta y dos ediciones de un seminario que acerca la defensa al ciudadano y a los hacedores de opinión tratando los temas más relevantes del momento –a veces cáusticos, como muy bien dice Miguel Ángel– relacionados con la seguridad y la defensa. Creo que haber conseguido hacer esta edición muestra que ese tesón es capaz de vencer las rigideces y dificultades del momento y encontrar la flexibilidad necesaria para poder dar continuidad al seminario, en este caso con una gran parte de los asistentes presentes de forma virtual.

El ciberespacio es el nuevo mundo del siglo XXI. Es un nuevo mundo que, al contrario que el que se descubrió en una empresa de hace ya 530 años, no se descubre de repente, sino que se descubre cada día. Cada día vemos que las nuevas tecnologías dejan rápidamente de ser nuevas y cada día tenemos que reflexionar sobre dónde estamos y a dónde nos conducen. Cada vez que renovamos un móvil, una tableta o un ordenador nos parece que nos ofrece unos productos maravillosos, sorprendentes; eso sí, a veces no con todos los valores humanos que desearíamos. Hace un año, paseaba yo por Cádiz y de repente vi un jaleo en una terraza. Estaban transmitiendo un partido de fútbol y la gente estaba protestando. Un chiquillo con un móvil chino les había cambiado el canal y el sonido, pues ese móvil chino traía de serie un instrumento para cambiar el canal de cualquier televisión. Personalmente, no creo que eso sea precisamente un espejo de valores humanos asociados a la tecnología. Hoy la tecnología nos inunda de una forma ubicua, casi imperceptible y a la vez imprescindible. Porque, como decía, cuando adquirimos un nuevo aparato, el de última moda, al día siguiente nos acostumbramos a trabajar con él y deja de sorprendernos, pasando a estar presente en nuestras vidas sin que casi nos demos cuenta de ello. Todo parece *business as usual*.

Una de las experiencias más impresionantes derivadas de la COVID-19 fue ver cómo nuestro país continuó trabajando. Es verdad que muchos sectores sufrieron dramáticamente; aquellos que necesitan de la presencia y el intercambio, como por ejemplo la hostelería y todo el ámbito turístico, pero una gran parte del país siguió tele-trabajando, tele-estudiando, tele-aprendiendo, tele-conferenciando y tele-relacionándose, venciendo de una forma sorprendente lo que de otra forma hubiera sido una pandemia mucho menos llevadera, mucho más dramática.

Al mismo tiempo, muchos organismos y empresas, incluidos centros sanitarios, sufrían ataques cibernéticos, en lo que son las dos caras de una misma moneda. Hoy se nos abre un mundo lleno de oportunidades, una realidad en la que podemos seguir trabajando aunque estemos confinados, pero, a la vez, un mundo lle-

no de riesgos y amenazas, que es sobre los que vamos a tratar en estas dos jornadas. En el ciberespacio se encuentran nuestros datos. Tal como lo define la Directiva de Defensa Nacional 2020, es «el nuevo recurso crítico de la economía mundial». Nuestros datos, la inteligencia artificial, las simples plataformas sociales, etcétera, son objeto de competición, incluso geoestratégica; a veces entre actores estatales, grandes o pequeños, y otras no.

Desde la defensa, tampoco podemos dejar de contemplar cómo avanza la economía digital, la moneda digital, internet y su impacto tremendo en el mercado laboral. Para bien o para mal, vivimos en un mundo híbrido, real y virtual, al que necesitamos dotar de una nueva gobernanza. Como marino, siempre he visto como la historia de la humanidad trataba de hacer de la altamar un espacio libre, un espacio para todos, mientras cada vez había más pequeñas parcelas, que eran las aguas interiores, el mar territorial, la zona contigua, la zona económica exclusiva… Cada vez vamos parcelando más lo que era un espacio libre. Posiblemente en internet hemos alcanzado unas cotas de libertad tremendas, aunque no hayamos alcanzado, ni mucho menos, igualdad en el acceso y hayamos creado un nuevo mundo en el que todavía la seguridad, nuestros valores, las reglas, no han permeado lo suficiente. Debemos dotar pues al mundo cibernético de una gobernanza más eficaz. El derecho que rige las relaciones humanas en el mundo físico tiene agujeros enormes en el mundo virtual, tal como veremos estos días.

También en el ámbito de la defensa, el ciberespacio nos plantea problemas antes totalmente desconocidos. Voy a poner dos o tres ejemplos, aunque hay muchos más. Uno de ellos es la dificultad a la hora de establecer una atribución clara a los ataques. Hay forenses de gran calidad, gente muy joven y muy buena; algunos de los mejores son españoles, incluso en la OTAN. Pero aun así hay una dificultad tremenda a la hora de atribuir los ataques, lo cual nos crea una dificultad en el funcionamiento de un instrumento tradicional de la defensa, como es la disuasión.

Otro ejemplo es que el enorme potencial destructivo de determinadas capacidades en internet puede permanecer totalmente oculto y latente, sin que nadie lo observe, al contrario de lo que ocurre con las compañías de carros de combate, submarinos, silos de misiles, formaciones de aviones... En cambio, estas formaciones de servidores permanecen ocultas, latentes, lo que nos lleva a un cambio muy profundo en el paradigma de cómo tratar a un competidor estratégico. Ya tenemos la disuasión y diálogo, y ahora hay que forjar una tercera vía; quizá, disuasión, diálogo y corresponsabilidad. Si no llamamos a las grandes potencias a que se sientan plenamente dueñas del futuro, no de su propio futuro ensimismado, sino del futuro de todos, ese potencial latente, capaz de destruir el comercio, la seguridad energética, la seguridad sanitaria, etcétera, estará ahí y podrá ser utilizado.

Un último ejemplo. Es muy posible que en esta destrucción, en esta situación fractal de las relaciones internacionales, con un desprecio al orden internacional basado en reglas creadas en las postrimerías de las dos guerras mundiales, todo un acervo cultural, como es la sociedad de naciones, termine convirtiéndose en un mero reflejo de lo que vemos si paseamos por las calles de nuestra ciudad, es decir, a todo el mundo ensimismado mirando la pantalla de su aparato digital. En las terrazas hay grupos de chicas –antes eran de chicos y chicas– en alegre conversación cada una con su móvil. Si nos montáramos en un globo y fuéramos ascendiendo y dejáramos de ver a esas personas, veríamos ese mismo ensimismamiento entre los países. Pues los países acuden cada vez más a la escena internacional mirándose su propio ombligo y esto también es una consecuencia de internet; posiblemente una consecuencia sociológica de internet.

Por otro lado, la revolución digital lleva muchos años alterando nuestros sistemas de mando y control. Por eso, mucha de nuestra inteligencia se basa o apoya ahora en los sistemas digitales. Y, por eso, desde hace muchos años, estamos tan preocupados en el mundo de la defensa. Todavía recuerdo –estaba en el

gabinete del secretario de Estado– cuando a todos nos preocupaban las consecuencias que tendría el «Efecto 2000», aunque todos sabíamos que aquello realmente no nos iba afectar, porque si en el ordenador no metíamos el año en el que vivíamos, si, por ejemplo, en la fragata *Extremadura* no metían en el año, sino solo el día, el célebre Y2K no podía afectarnos. Aun así pasamos una noche de fin memorable con aquello del Y2K.

Podríamos decir que la importancia militar del ciberespacio es casi residual. El impacto en lo no militar supera con mucho el impacto en lo militar, pero, lógicamente, ése es un capítulo más del libro de los impactos del ciberespacio. Porque concebimos la ciberdefensa como un conjunto de capas sucesivas que, como cualquier otra ciberseguridad, comienzan en el individuo. Un individuo que debe comportarse de acuerdo con unos protocolos frente a las máquinas que utiliza. Esto se extiende también a las complejísimas redes de datos de las empresas. Por poner un ejemplo, hace casi un año, en una visita a Telefónica, un gurú de la telefonía me pidió el móvil. Cuando se lo dejé me dijo que no me preocupara que no me iba a hacer ningún daño. Al devolvérmelo me dijo que había estado conduciendo por la autopista de Extremadura a un promedio de 138 kilómetros por hora. Yo le dije que de eso hacía ya bastante tiempo y él me dijo que en el teléfono eso quedaba para siempre. Es tremendo todo lo que se llega a acumular si tú le das acceso al móvil. Mantener la responsabilidad en la red, ya sea civil o militar, en las múltiples redes que tenemos, es responsabilidad de todos porque todos somos actores; más aun, todos somos nodos, nodos de recepción y de emisión.

También conviene, como en todo problema, aplicar un poco de realismo al mirar el problema de la seguridad en el ciberespacio y evitar la mitología que suele acompañar la aparición de algo que parece tremendamente destructivo. La tecnología está cambiando dramáticamente el mundo pero la tecnología es simplemente una herramienta que alguien diseña y que está en mano de

seres humanos. El ciberespacio es un producto de la humanidad y será siempre lo que nosotros queramos que sea.

En cuanto al ámbito concreto de la defensa, el componente humano no pierde su importancia. Ni a pesar de los avances tecnológicos ni, precisamente, gracias a ellos. Estamos en esta dicotomía en la que nos beneficiamos del avance tecnológico y vivimos con sus riesgos, pero ninguno de ellos –la operación Balmis creo que lo ha visualizado muy bien– puede sustituir la empatía, el espíritu de sacrificio, el espíritu de servicio a los demás y el sentido del deber. Eso va a estar ahí para siempre.

Cuando la Directiva de Política de Defensa que publicamos el 6 de agosto habla de soberanía nacional, incluye, por supuesto, la soberanía en el ciberespacio. ¿Qué es la soberanía en el ciberespacio? Es un concepto distinto del habitual. El ciberespacio es un bien común de la humanidad. Ahí la soberanía tiene mucho más que ver con el grado de conocimiento y con la autonomía tecnológica que tenga cada país, aquélla que le permita garantizar a sus ciudadanos un acceso seguro, libre de amenazas y que contribuya a su innovación y progreso. Tanto la OTAN como la Unión Europea tienen programas –estos días veremos alguno en concreto– de respuesta a estos retos. La primera respuesta colectiva de la OTAN data del año 2002. La OTAN no sólo ha hecho del ciberespacio un dominio operacional del mismo nivel que los tradicionales de tierra, mar y aire, o el nuevo del espacio, sino que ha asumido que un ataque cibernético podría llegar incluso a superar el umbral que llevaría a la invocación del Artículo 5 del Tratado del Atlántico Norte, con todo lo que eso conlleva. Y una de las cosas que ha conllevado es que todos los aliados nos hemos incorporado al compromiso de ciberdefensa de 2016. La trascendencia de estas cuestiones no es sólo filosófica, sino que estamos bajando rápidamente de las musas al teatro.

Igual ocurre en la Unión Europea, que reconoce que la cadena de ciberdefensa es tan fuerte como el eslabón más débil. La Unión Europea ha desarrollado algunos tipos de respuestas muy

interesantes, además de las doctrinales, las técnicas, etcétera. Por ejemplo, por primera vez, en la diplomacia cibernética se ha sancionado a empresas e individuos por un comportamiento inadecuado o delictivo en las redes. También hay otras medidas interesantes, como la Unidad Conjunta de Ciberseguridad, o una muy novedosa plataforma europea, que esperamos se asiente, para el conocimiento del entorno cibernético.

El ciberespacio está ya plenamente aceptado como un ámbito de las operaciones militares, pero sería un error considerarlo un ámbito aislado. Precisamente, desde el principio de los tiempos los ejércitos han basado sus operaciones en la capacidad de integración de elementos muy distintos. Lo digital impregna ya la mayoría de las operaciones militares. Miguel Ángel aludió a las palabras de Josep Borrell, nuestro Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, que realmente son tan acertadas como preocupantes.

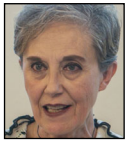
Para terminar como un tono optimista, no debemos olvidar que aunque lo digital nos puede ayudar mucho a gestionar el mundo real, no lo sustituye. Nuestras vidas, nuestros valores y nuestras necesidades siguen teniendo mucho más que ver con el carbono que con el silicio. Y esperemos que siga siendo así. Espero que disfruten del seminario y les deseo nuevamente, como en las anteriores ediciones, muchos éxitos. Gracias.

MONTSERRAT DOMÍNGUEZ
Vicepresidenta de la Asociación de Periodistas Europeos
y subdirectora de *El País*

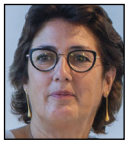
Gracias Almirante. A continuación daremos comienzo al seminario en sí, con la intervención de la directora del Centro Nacional de Inteligencia.

3. INTELIGENCIA EN EL CIBERESPACIO

PAZ ESTEBAN
Directora del Centro Nacional
de Inteligencia (CNI)



Moderadora
MONTSERRAT DOMÍNGUEZ
Subdirectora de *El País*



Paz Esteban y Montserrat Domínguez

MONTSERRAT DOMÍNGUEZ
Moderadora

Vamos a dar comienzo a la primera sesión del Seminario Internacional de Seguridad y Defensa. Paz Esteban es la actual directora del Centro Nacional de Inteligencia, pero también del Centro Criptológico Nacional, de la Autoridad Nacional de Inteligencia y Contrainteligencia y de la Autoridad Delegada para la Seguridad de la Información Clasificada, así como presidenta del Consejo Nacional de Ciberseguridad.

En suma, es la primera mujer en estar al frente de nuestros servicios de inteligencia, así como la primera que proviene de las filas de estos servicios, donde ha desarrollado toda su carrera profesional tras incorporarse al CESID en 1983, no mucho después de licenciarse en Filosofía y Letras por la Universidad Autónoma de Madrid. Una de sus pasiones es la historia antigua y medieval, aunque a lo largo de estos 37 años que lleva en el servicio ha tenido la oportunidad de profundizar más en historia contemporánea porque, directora, te ha tocado vivir un cambio profundo en todo nuestro entorno, además de estar en un observatorio realmente excepcional desde el que ser testigo de los últimos coletazos de la Guerra Fría, con la caída del muro de Berlín, la desaparición de la Unión Soviética, el auge del yihadismo, la emergencia de China como una potencia no exclusivamente económica y todo el desafío que suponen las nuevas tecnologías, no tanto en si mismas como por su uso perverso por parte de determinados Estados o de otros actores con intereses opacos. Eso es algo que nos preocupa especialmente aquí, en la Asociación de Periodistas Europeos: el uso indiscriminado de armas de confusión masiva, que son capaces de desestabilizar y de hacer crecer la desconfianza hacia nuestras instituciones y hacia nuestro modo de vida.

Sin más dilación, le cedo la palabra a Paz Esteban, directora del Centro Nacional de Inteligencia, que debemos añadir no se

prodiga mucho en los medios ni en intervenciones públicas, por lo que es un extraordinario y raro privilegio poder tenerla aquí con nosotros.

PAZ ESTEBAN
Directora del Centro Nacional de Inteligencia

Buenos días a todos, a quienes están aquí y a quienes nos están siguiendo *online*, y muchas gracias, Montserrat por tu presentación y por poner en valor lo que representa trabajar y servir a España desde el Centro Nacional de Inteligencia, al que tengo el honor de representar y dirigir.

En primer lugar, quiero agradecer a la Asociación de Periodistas Europeos, y especialmente a su secretario general, Miguel Ángel Aguilar, la invitación a participar en este Seminario Internacional de Seguridad y Defensa. Lo ha dicho el SEGENPOL y yo me sumo a sus palabras en cuanto al tesón que demostráis en la celebración, año tras año, de este encuentro. Treinta y dos ediciones es tiempo más que suficiente para que valoremos muy positivamente el interés de estas convocatorias, siempre tan bien y cuidadosamente organizadas, por la Asociación de Periodistas Europeos. En este caso, tengo que añadir que ha sido una magnífica idea por vuestra parte dedicar esta trigésimo segunda edición a las «Amenazas desde el ciberespacio», que es uno de los espacios globales recogidos en la Estrategia de Seguridad Nacional de 2017 y, sin duda, uno de los ámbitos que más se ha visto afectado por la crisis de la COVID. Desde mi experiencia de mucho tiempo como miembro del Servicio de Inteligencia de España y, ahora, como su directora, he podido comprobar la evolución de estas amenazas y su muy significativo incremento en los últimos años y, sobre todo, cómo la actual pandemia está acelerando esta tendencia, al haberse ampliado el radio de acción de los ciberatacantes, su agresividad y el carácter crítico de los incidentes que protagonizan.

Estoy convencida de que, durante las dos jornadas en las que se desarrollará este seminario, vamos a tener la oportunidad de reflexionar y sacar conclusiones sobre estos riesgos cibernéticos, que tocan de lleno la seguridad nacional, la soberanía, el funcionamiento de las infraestructuras críticas, el patrimonio científico y tecnológico, la competitividad de nuestras empresas, la imagen exterior de España y la privacidad de los datos de nuestros conciudadanos.

Vivimos un tiempo nuevo que nos exigirá a todos un gran esfuerzo para estar en condiciones de aprovechar las enormes oportunidades que la tecnología nos ofrece y, a la vez, para hacer frente a los considerables desafíos que la revolución tecnológica está generando. El CNI, como ya hiciera su antecesor, el CESID, ha desarrollado una intensa actividad en este campo. Más adelante me referiré a cuando, a principios de los años ochenta, un pequeño grupo de expertos del servicio, verdaderos pioneros en la materia, comenzaron a estudiar y a prever las vulnerabilidades y los riesgos asociados al uso y aplicación de la tecnología de aquellos momentos. De ahí venimos. Ahí empezamos nuestra andadura en lo que ahora conocemos como «ciberespacio». Es evidente que lo que hace cuatro décadas nos parecía a casi todos ciencia-ficción hoy forma parte de nuestra vida cotidiana y se ha convertido, desde el punto de vista de la seguridad, en una de las principales preocupaciones de las administraciones, de las empresas y de los propios ciudadanos; unas preocupaciones a abordar desde diferentes planos y con la colaboración de muchos y muy distintos actores. Por esa razón, el CNI es plenamente consciente de la necesidad de compartir encuentros como éste con profesionales de los medios de comunicación, pues ustedes constituyen un muy buen vehículo para trasladar y hacer entender a la sociedad los riesgos a los que nos enfrentamos y para concienciarla sobre lo que cada uno de nosotros podemos evitar mediante el uso responsable de las redes y sistemas de información y comunicaciones.

La relevancia de este asunto ya está siendo reconocida por los medios y plataformas a las que ustedes representan, en los que cada vez es más frecuente encontrar secciones que comenzaron dedicadas a la tecnología, en general, y en las que progresivamente todo lo relacionado con la ciberseguridad ha ido ganando mayor espacio. Oportunidades y desafíos son la cara y la cruz de una realidad innegable, que ya es presente y no un futurible; una realidad cambiante como pocas y que, además, avanza a una velocidad que nos obliga a una actualización permanente que, en el caso de los servicios de inteligencia, se traduce en términos de recursos y, en concreto, de mejora de nuestras capacidades de prevención, detección, análisis y respuesta a las amenazas. Una realidad, insisto, que nos impone una profunda revisión de nuestros modelos de trabajo y de nuestras herramientas con el fin de adecuarnos a ese «tiempo nuevo» al que antes me refería, que no es sino el entorno digital en el que ahora todos nos movemos.

Déjenme decirles que, a pesar de que en este foro nos vamos a centrar en las amenazas, es necesario empezar recordando que el desarrollo tecnológico ha favorecido un período de auge económico y social sin precedentes y que ofrece posibilidades de crecimiento al conjunto de la sociedad. Es éste un cambio que tiene impacto desde todos los ángulos y que está modificando nuestro modo de vida, nuestra cultura, nuestras costumbres en general y nuestras estructuras sociales, que actualmente se desarrollan de manera paralela tanto en el mundo físico como en el mundo virtual.

Desde el punto de vista de los servicios de inteligencia, las nuevas tecnologías han creado un entorno diferente que puede favorecer la consecución de los objetivos que perseguimos pero, eso sí, a cambio de que adaptemos, como les acabo de señalar, nuestro modelo de trabajo y los medios de los que nos servimos para realizarlo. Nos enfrentamos a una verdadera sobreabundancia de información que nos obliga a aumentar y modernizar nuestra capacidad para procesarla, tratarla, almacenarla, hacerla accesible, distribuirla y explotarla. En otras palabras, el mundo digital en el que ya nos movemos nos exige enfoques novedosos, métodos distintos, instrumentos y técnicas más avanzados y, en definitiva, nuevas formas de hacer inteligencia, porque estamos determinados a que el CNI siga siéndole útil a los destinatarios del producto que elaboramos y a que éstos continúen necesitándonos. Aunque aún nos encontramos en el camino de esa renovación técnica, metodológica y procedimental, el horizonte que nos hemos marcado en cuanto a la integración de fuentes de datos, la fusión de información, la implantación de herramientas colaborativas y de sistemas de búsqueda global, la inteligencia artificial, etcétera, está suponiendo ya el inicio de un cambio de mentalidad en el CNI. Se trata de un proceso similar al que han emprendido nuestros homólogos del entorno europeo y que nos está llevando a pasar de un modelo basado tradicionalmente en la «necesidad de conocer» a otro en el que prima la «cultura de compartir», dentro del mantenimiento de los estándares de seguridad inherentes al trabajo de inteligencia. Hablamos pues de un cambio tecnológico y de cultura corporativa que afecta a todos los sectores de actividad del servicio y, por tanto, es perfectamente aplicable a cuanto hacemos en materia de ciberseguridad.

Antes de centrarme en el ámbito cíber, que es el que hoy nos ocupa, he creído oportuno hacerles partícipes de la transformación a la que nos impulsan los avances tecnológicos, de los que en el CNI somos usuarios y que, en este caso concreto, nos facilitan la tarea de identificar y tratar de neutralizar las amenazas procedentes del ciberespacio contra los intereses nacionales y la seguridad de los sectores tanto público como privado, así como de los ciudadanos.

Porque no debemos olvidar que esa revolución digital que tanto nos favorece, porque nos abre nuevas y mejores posibilidades de actuación, es la misma de la que se valen quienes crecientemente nos ciberatacan, ya se trate de actores estatales, grupos organizados, colectivos de diversa índole o individuos aislados.

Unos «enemigos sin rostro», como tantas veces les hemos definido, con capacidad para desarrollar acciones hostiles que, en cuestión de minutos, pueden comprometer los activos de cualquier organismo de una administración, corporación, empresa, infraestructura, etcétera; unos atacantes que disponen de los medios y de la voluntad de agredir los sistemas y las redes de cualquier objetivo público, privado o individual que haya suscitado su interés para la consecución de sus fines maliciosos: el espionaje, la desestabilización, el robo, la extorsión o la suplantación de la identidad de personas físicas o jurídicas.

Para responder a este tipo de amenaza, que era todavía emergente, pues su plasmación y sus efectos no se manifestaban aún con la virulencia actual, en 2004 se creó el Centro Criptológico Nacional, el CCN, que como ustedes saben está adscrito al CNI y cuyo personal se encuentra integrado orgánica y funcionalmente en el Centro Nacional de Inteligencia. Como les decía al inicio de mi intervención, el CCN tiene sus orígenes en una pequeña sección de nuestro antecesor, el CESID, que, a principios de la década de 1980, logró alcanzar un profundo conocimiento de las amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicación de la época. Antes he calificado a aquellos profesionales de pioneros, y lo fueron, pero lo cierto es que también tuvieron mucho de visionarios pues trabajaron para hacernos comprender que la información que circulaba por medios electrónicos también debía ser protegida con medios *ad hoc* para impedir el acceso no autorizado de terceros, como tradicionalmente veníamos haciendo con la documentación en soporte papel, en este caso con medidas de seguridad física.

El paso del tiempo demostró que las amenazas eran reales, que teníamos que estar preparados para hacerles frente y que la seguridad de redes y sistemas de información y, por lo tanto, del ciberespacio eran un reto que cada vez adquiría mayor prioridad. Y así quedó recogido en 2002, en la ley reguladora del CNI, que incorporó esta materia entre las funciones asignadas al servicio

que entonces se creaba. Pero poco después dimos un paso más, o mejor dicho, el legislador dio un paso más, y en 2004, como acabo de comentarles, mediante un Real Decreto se creó el CCN, corroborando de esta forma la necesidad de contar con un organismo específicamente encargado de la seguridad de los sistemas de información de la administración, así como de garantizar la confidencialidad, la disponibilidad y la integridad de la información, incluida la información clasificada, que dichos sistemas procesan, almacenan o transmiten. Después han venido otros, pero me van a permitir que señale, porque es un dato objetivo, que el CCN fue el primer organismo constituido en España para ocuparse de la amenaza cibernética y de la protección frente a ella.

En 2019 hemos celebrado el decimoquinto aniversario de su creación. Durante estos años, el Centro Criptológico Nacional se ha convertido en un referente en su ámbito de actuación, respetado y considerado dentro y fuera de nuestras fronteras. Así nos lo reconocen nuestros interlocutores nacionales y extranjeros y así lo confirma el hecho de que, por su experiencia, sus conocimientos técnicos y su eficacia, la intervención del CCN, su presencia y su colaboración son permanentemente solicitadas. Les pongo un ejemplo: el CCN organiza anualmente las llamadas Jornadas STIC, que este año, en su decimocuarta edición, se celebrarán del 30 de noviembre al 4 de diciembre. Estas jornadas se han convertido en el principal encuentro de expertos de la ciberseguridad en lengua española y en un referente en el panorama internacional. Congregan a toda la comunidad que interviene en la salvaguarda de nuestro ciberespacio: Gobierno, administraciones e instituciones públicas, empresas, universidades y ciudadanos. En 2019, las Jornadas STIC contaron con 130 ponentes, 60 empresas representadas y 3.500 asistentes. Es decir, el aumento del prestigio del CCN ha crecido en la misma proporción que el interés por la ciberseguridad. A título anecdótico, pero ilustrativo, les confesaré que a las primeras Jornadas STIC, celebradas en 2007, acudieron veinte personas.

Durante sus dieciséis años de existencia, el CCN ha contribuido al fortalecimiento de la ciberseguridad nacional de diferentes maneras. Por un lado, protegiendo las redes y sistemas de organismos públicos y de entidades estratégicas, gestionando incidentes y elaborando planes específicos para mitigar sus efectos. Por otro, diseñando soluciones y herramientas de ciberseguridad, formando conjuntamente al personal de la administración pública y de las empresas y redactando guías, consejos y recomendaciones para difundir la cultura de ciberseguridad, contribuyendo así a la generación de iniciativas tan relevantes como la creación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado o la implantación del Esquema Nacional de Seguridad. Y, finalmente, promoviendo, en su calidad de organismo de certificación, el uso de productos y sistemas seguros, y colaborando en el desarrollo de nuevas estrategias y legislación intercambiando información y técnicas con organismos homólogos de otros países, así como representando a nuestro país en los foros y organizaciones multilaterales, en los que la ciberseguridad ha adquirido cada vez un mayor protagonismo. Este abanico de cuestiones relacionadas con la actuación del CCN está recogido en la Memoria de Actividades y en el Informe sobre Ciberamenazas y Tendencias que en estos próximos días haremos públicos. Les animo a que consulten ambos documentos si desean ampliar la información que les he proporcionado, ya que no voy a extenderme más hablando del CCN; primero, porque no quiero interferir en la posterior intervención de su subdirector y, también, porque quiero centrarme en el valor añadido que aporta el CNI en su conjunto y en el tratamiento integral e integrado que hacemos de la ciberseguridad.

En el Servicio de Inteligencia español, bajo un mismo paraguas y con un mismo objetivo, se coordinan los diferentes enfoques complementarios desde los que abordar la ciberseguridad. El trabajo del centro en este ámbito incluye la perspectiva técnica, encomendada principalmente al CCN –pero no sólo a éste,

como luego veremos–, y la dedicada al análisis de inteligencia o contrainteligencia tradicional, que se ocupa de las agresiones con origen en actores estatales dirigidas contra intereses españoles. Podemos distinguir tres planos. Por un lado, está la labor que desempeña el CCN de la que acabo de hablarles, por lo que no voy a insistir en ello. Por otro –y éste es el enfoque puramente de inteligencia–, el CNI desarrolla una serie de líneas de acción que se resumen en la investigación, el seguimiento y la valoración de las capacidades, las motivaciones y los objetivos de los agresores, que se complementan con el análisis cualitativo de cada incidente para determinar qué tipo de información ha sido sustraída y qué consecuencias puede tener para la víctima. Además, se lleva a cabo una labor de sensibilización sobre la amenaza que supone el ciberespionaje a cargo o patrocinado por potencias extranjeras y sobre la necesidad de adoptar medidas para prevenir y neutralizar esos ataques. Esto se está haciendo tanto de manera proactiva, en organismos o en empresas que se considera que pueden ser de interés para terceros, como aquellos que ya han sido objeto de agresión. Y, por último, el centro tiene también el recurso de la Inteligencia de Señales (SIGINT), que es un elemento diferencial de nuestra actividad en general y, en este caso concreto, de nuestra contribución a la ciberseguridad, dado que ningún otro organismo dispone ni de las capacidades técnicas ni de las facultades legales para obtener, evaluar e interpretar el tráfico de señales de carácter estratégico derivado de las comunicaciones internacionales, tal y como establece nuestra ley reguladora. Este acceso SIGINT a señales internacionales permite detectar agresiones y completa la labor técnica que realiza el CCN en cuanto a análisis e investigación de ciberincidentes.

Esta combinación de enfoques y capacidades de la que dispone el CNI constituye su mayor y más importante activo. Nuestro conocimiento del mundo cíber es profundo, porque lo trabajamos desde ángulos distintos. Por eso, representa una potente herramienta para conseguir el mayor grado de certidumbre posi-

ble en la siempre complicada atribución de los ataques. Como les decía, el tratamiento integral de las ciberagresiones, gracias a la amplitud de competencias asignadas legalmente que nos confiere el hecho de ser el único Servicio de Inteligencia a nivel nacional, es lo que convierte en singular la aportación del CNI en este amplio mundo de la ciberseguridad en el que hoy, en este seminario, nos hemos sumergido de la mano de la Asociación de Periodistas Europeos.

A ninguno se nos oculta que el ciberespacio permite operar, desde no importa dónde y con un alto grado de impunidad y de anonimato, sobre todo tipo de objetivos, situados en cualquier lugar del mundo. También todos somos conscientes de que tanto la relación coste-eficacia de las agresiones en ese entorno como sus resultados son difícilmente alcanzables en comparación con el uso de otros medios. Si a ello unimos el hecho de que el mundo digital se caracteriza por la ausencia de fronteras físicas y que esto hace que su ordenación normativa y jurisdiccional sea difícil de articular, tendremos el contexto casi perfecto para la ejecución de los ciberataques. Con estas condiciones, la ganancia de un agresor es enorme, y más aun si se compara con el riesgo mínimo que corre. Quiero insistir en que los ciberatacantes, estatales o no, mientras sólo teman al fracaso, carecerán de motivos para dejar de intentarlo, porque no tienen nada que perder, porque prácticamente nunca sufren las consecuencias de sus actos. Además, la utilización de los avances tecnológicos hace más efectivas y complejas las agresiones desde el ciberespacio, lo que incrementa el coste de las herramientas a usar en su contra.

Desde luego que no es mi intención pintar deliberadamente un panorama sombrío, pero esto es lo que tenemos, ésta es la realidad a la que nos enfrentamos. No es un problema que podamos minimizar. Buena prueba de ello son las denominadas Amenazas Persistentes Avanzadas, o APT por sus siglas en inglés (Advanced Persistent Threat), que agrupan las principales acciones ciberofensivas. Detrás de cada APT existen grupos de trabajo estables formados por equipos multidisciplinares con altos conocimientos y gran cantidad de recursos materiales y económicos a su disposición, por lo que suelen estar patrocinadas por Estados o por grandes grupos de carácter cibercriminal. En el caso de los Estados, éstos cuentan con unidades cíber especializadas dentro de sus estructuras de inteligencia militares y civiles, o con *proxies*, tales como empresas tecnológicas, *hackers* o ciberdelincuentes, de los que se valen para ocultarse y ejecutar acciones ofensivas que no puedan ser fácilmente atribuidas. De hecho, la atribución de los ciberataques es cada vez más difícil debido a los grandes recursos técnicos y económicos que se destinan a la ocultación de su origen real.

España, tanto *per se* como por su pertenencia a organizaciones internacionales –especialmente la OTAN y la Unión Europea– con las que comparte intereses de todo tipo, continúa siendo objeto de constantes intentos de ciberataques por parte de actores estatales o de grupos esponsorizados por éstos, y no es previsible que esta tendencia deje de crecer en el futuro. En nuestro país, los objetivos prioritarios continúan siendo, por un lado, la administración pública, buscando información sensible que facilite posiciones de ventaja al agresor; y, por otro lado, las empresas de los sectores estratégicos (energético, aeroespacial y defensa). Además, se ha observado un incremento de los ataques a las cadenas de suministro de las víctimas (intermediarios, proveedores, distribuidores, etcétera), con redes habitualmente menos protegidas, como forma de acceso al objetivo final. No hay duda de que el caso del ciberespionaje económico supone un grave y creciente riesgo para los intereses nacionales puesto que su objetivo es el robo de la propiedad intelectual e industrial de empresas y organizaciones. Se trata de una actividad muy rentable, porque, de tener éxito, le permite al agresor ahorrar tiempo y recursos en investigación científica y desarrollo tecnológico.

Si hablamos de crecimiento de los ciberataques y de las actividades de ciberespionaje, no podemos obviar el hecho de que

precisamente ése ha sido uno de los efectos inmediatos de la COVID-19 pues, en líneas generales, la pandemia no ha sido un generador de nuevos riesgos o amenazas, sino un acelerador de tendencias existentes con anterioridad. Se trata de un elemento indudablemente disruptivo e inesperado, un «cisne negro», según la terminología que hace años acuñaron los expertos para referirse a un suceso improbable, que ocurre por sorpresa y que termina teniendo gran impacto. La COVID ha recuperado esta teoría, porque reúne todas las características que definen un «cisne negro», aplicado en esta ocasión a la esfera política, económica, social, sanitaria, de seguridad…

Pero volvamos a nuestro ámbito y veamos cuáles han sido los efectos de la pandemia en el panorama de la ciberseguridad global, porque es evidente que ha influido desde el momento en que la situación ha sido aprovechada por actores hostiles para potenciar sus ataques: desde las operaciones de robo de información hasta las campañas de *ransomware* o secuestro de datos.

Hace unos días, leía en una publicación especializada que «alentados por la crisis sanitaria, el teletrabajo y el uso masivo de herramientas de colaboración digital (como la videoconferencia) han permitido a muchas empresas continuar su actividad». Aquí tenemos una de las claves para explicar el crecimiento de los ciberataques. El hecho cierto es que el uso obligado del teletrabajo ha aumentado el área de exposición de los sistemas de información y de las redes, y el insuficiente nivel de seguridad en unos y en otras ha facilitado la entrada de los atacantes más agresivos y la actividad de grupos cibercriminales. La exposición no controlada de muchas organizaciones a internet tiene este riesgo. Una tendencia que va a continuar al alza pues es previsible que los ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales se incrementen. El objetivo será acceder a la infraestructura de la institución o de la empresa del empleado que teletrabaja para conseguir distintos fines, entre los que el ciberespionaje será uno de los principales.

En general, la COVID-19 ha incrementado el riesgo de ciberataques pero, sobre todo, lo ha hecho contra objetivos especialmente vulnerables y sensibles en estas circunstancias, como son el sector sanitario, la industria farmacéutica y los centros de investigación. La pugna por obtener la vacuna contra el virus y todo lo que implica su comercialización constituyen alicientes más que sobrados para que algunos actores, estatales o no, hayan emprendido una campaña de ataques especialmente virulenta. Y claro está que no sólo en España se ha producido este fenómeno. Con nuestros colegas de otros países occidentales hemos intercambiado información sobre las actividades de ciberespionaje que todos hemos sufrido sobre los organismos nacionales e instituciones involucradas en las investigaciones para desarrollar una vacuna contra la COVID-19. El CNI, declarado por el Gobierno «servicio esencial» durante el estado de alarma, no ha bajado la guardia durante estos meses. Desde marzo, hemos centrado nuestro esfuerzo en garantizar la ciberseguridad del sector público español, y especialmente el sanitario, precisamente en los momentos de mayor tensión de los servicios de salud, así como en detectar las actividades que pudieran afectar al tejido industrial y productivo. Hemos observado un incremento cuantitativo de los ciberataques y un aumento cualitativo de su gravedad y agresividad en la actuación de quienes utilizan el ciberespacio con fines maliciosos e ilícitos. Pero, sobre todo, hemos empezado a ver cómo se va consolidando una tendencia que apunta a una previsible disminución de las actividades «tradicionales» de espionaje, en favor de las «alternativas tecnológicas» representadas por el ciberespionaje.

Pero las posibilidades de utilización maliciosa del ciberespacio no se agotan con los ciberataques. Las oportunidades de actuación que ofrece el ciberespacio han favorecido que adquiera una relevancia inusitada un fenómeno tan antiguo como la desinformación. En este caso, el ciberespacio es usado, no para ejecutar una agresión en sentido estricto, sino para diseminar conte-

nidos con una finalidad concreta, recurriendo para ello a redes sociales, a medios de comunicación digitales y a programas informáticos, como es el caso de los *bots*, que automatizan y multiplican los mensajes. Cuando la desinformación está dirigida a una determinada audiencia, durante un tiempo también determinado y con un objetivo definido, podemos hablar de «campañas de desinformación». Y no se nos puede olvidar que lo que se encuentra detrás de todo esto es una distorsión deliberada de la realidad (lo que ahora llamamos «posverdad») diseñada para modificar la opinión pública e influir a favor de los intereses del promotor de la campaña en cuestión, que normalmente es una potencia extranjera que se vale de ese instrumento para la consecución de objetivos poco o nada confesables. Ahí está el peligro, en la voluntad de quien orquesta este tipo de acciones y lo hace para desestabilizar, menoscabar la credibilidad de las instituciones, dañar el prestigio de un país, polarizar a la sociedad o imponer relatos sesgados; y siempre, como en el caso de los ciberataques, desde el anonimato. Aunque no sean una variante de las ciberagresiones, estas campañas comparten con ellas el aprovechamiento de las posibilidades que ofrecen el mundo virtual y los avances tecnológicos para ejecutarlas, además de su eficiencia y la dificultad de su atribución. Pero, sobre todo –y por eso me interesa subrayar esta correlación– porque ciberataques y desinformación son dos de las principales herramientas que se utilizan en el marco de las denominadas operaciones híbridas.

Durante los últimos años, los procesos electorales habían sido uno de los objetivos principales de las campañas de desinformación. Sin embargo, a raíz de la crisis de la COVID-19, algunos actores estatales han desarrollado una intensa actividad de desinformación a través del ciberespacio, poniendo de manifiesto el poder disruptivo de la difusión de información manipulada y sus posibles consecuencias para la seguridad de los Estados. Por ello, a lo largo de estos meses, el CNI ha trabajado en la detección y el análisis de las campañas de desinformación originadas

en el exterior y difundidas a través de aparatos de propaganda controlados o patrocinados por actores estatales, algunas de ellas muy agresivas en el planteamiento de narrativas antieuropeas. En este período y en este contexto, el CCN ha elaborado y publicado una Guía de Buenas Prácticas frente a la desinformación; una guía que tiene como principal destinatario al ciudadano, porque él es el objetivo, el receptor primordial del mensaje que trasladan estas campañas. Además, hemos puesto en marcha el denominado Observatorio ELISA, que es una herramienta diseñada por el propio CCN para analizar narrativas maliciosas y catalogar los medios que las difunden, y que entendemos que puede ser de utilidad para que nuestros conciudadanos conozcan la fiabilidad del origen de la información que reciben en las distintas plataformas.

Quisiera concluir con una última reflexión sobre este asunto, porque sé que mañana habrá una mesa dedicada monográficamente a él. Con relación al fenómeno de la desinformación, se podría decir que los Estados democráticos somos más vulnerables que los que no lo son. Lo somos porque no censuramos los contenidos que circulan por redes sociales o difunden los medios de comunicación ni controlamos el acceso a ellos y porque no contamos con aparatos de propaganda que lancen campañas de esa naturaleza contra terceros. A cambio, eso sí, tenemos libertad de expresión y de prensa.

Podía haber subtitulado mi intervención de hoy con la frase «oportunidades y desafíos», porque resulta una buena descripción de lo que representan la tecnología y el ciberespacio desde la perspectiva de la inteligencia. Hasta ahora les he hablado fundamentalmente de desafíos. Ahora quiero centrarme en las oportunidades, que son, principalmente, la sensibilización de la sociedad, la conjunción de esfuerzos a nivel nacional de cuantos organismos tenemos competencias en el ámbito cíber, tanto en el sector público como en el privado, la colaboración internacional y la acción concertada de los organismos multilaterales.

Uno de los elementos esenciales a la hora de garantizar la seguridad en el ciberespacio es el ciudadano. Las personas pueden ser el motor que impulse la confianza en la tecnología, promoviendo procesos que la garanticen. Se trata de que el ciudadano sea consciente de los riesgos asociados al uso de la tecnología y pueda exigir que se incorpore la seguridad como un elemento de serie en los dispositivos y servicios que utiliza. Para ello, empresas, fabricantes y proveedores de servicios, así como los responsables públicos y las administraciones, incluido el CNI, debemos implicarnos, dando un salto cualitativo en la labor de concienciación de los usuarios, comprometiéndonos con la idea de que todos somos corresponsables de la ciberseguridad nacional y debemos hacer un uso responsable de las tecnologías.

Al hablar de los diferentes actores implicados en la sensibilización de la sociedad no he citado a los medios de comunicación. No es porque me haya olvidado de ellos, de ustedes, sino porque quiero hacer una mención especial al importante papel que juegan en ese empeño. Y nada mejor que hacerlo en este foro, bajo el patrocinio de la Asociación de Periodistas Europeos.

No tengo ninguna duda de que la participación activa de los medios en la concienciación de los ciudadanos es una baza de primer orden para elevar los niveles de ciberseguridad. Ustedes, los profesionales de la comunicación, representan una verdadera oportunidad en ese sentido porque tienen una capacidad de llegar a la opinión pública mayor que la que tenemos otras instancias. Contar con ustedes para esta labor es pues una apuesta ganadora.

El resto de oportunidades que he mencionado tienen todas ellas un denominador común, que es la constatación de que, frente a amenazas globales como las procedentes del ciberespacio, las respuestas deben ser también globales y basarse en la coordinación. En la constatación de esa realidad, que nos conduce a una dinámica de cooperación entre organismos dentro y fuera de España y a la concertación de políticas y de normativa a nivel multilateral, reside una nada desdeñable oportunidad de éxito frente a quienes nos agreden. Es éste un problema al que nadie puede enfrentarse de forma aislada. Por eso, la colaboración constituye un activo imprescindible al que sería un error sustraernos. La conjunción de esfuerzos es la mejor oportunidad para afrontar los desafíos que nos plantea el uso malicioso del ciberespacio y no duden de que el CNI participará activamente en ese esfuerzo para construir, entre todos, un entorno virtual seguro y confiable.

Muchas gracias de nuevo a la Asociación de Periodistas Europeos por su invitación y muchas gracias a todos ustedes por su atención. Ésta ha sido mi primera visita a este seminario y confío en que no sea la última. Les deseo a los organizadores, a los ponentes y a los asistentes que estos dos días les sean fructíferos. Cuídense de los ciberataques y de los virus, de los informáticos y de los otros.

MONTSERRAT DOMÍNGUEZ
Moderadora

Muchísimas gracias, directora. Ha dicho muchísimas cosas que nos van a obligar a reflexionar. No sé hasta qué punto somos conscientes de la desigualdad de las fuerzas en esta batalla contra este enemigo enmascarado.

4. APROXIMACIÓN A LA CIBERDEFENSA

GENERAL FÉLIX SANZ ROLDÁN
Jefe del Estado Mayor de la Defensa (JEMAD) entre 2004 y 2008 y director del Centro Nacional de Inteligencia (CNI) entre 2009 y 2019

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Moderador
JAVIER GARCÍA VILA
Director de Europa Press

Javier García Vila, el General Miguel Ángel Ballesteros
y el General Félix Sanz Roldán

La necesidad de protegerse de amenazas indetectables, asintomáticas, procedentes de la red está asumida de manera generalizada por organismos, instituciones y empresas de todo el mundo. Prevenir los ataques cibernéticos que amenazan directamente los pilares de un país y a sus ciudadanos requiere el despliegue de un sistema de ciberdefensa capaz de neutralizarlos. La respuesta puede incluir una gradación de ataques que salvaguarden la seguridad al tiempo que retroalimenten los temores del adversario, creando una espiral de antagonismo.

¿Estamos ante una militarización del ciberespacio? ¿Cuándo acaba la ciberseguridad y empieza la ciberdefensa? ¿A qué nuevos retos nos enfrentamos? ¿Cómo pueden defenderse nuestras democracias de estas nuevas amenazas a sus valores?

JAVIER GARCÍA VILA
Moderador

Vamos a dar comienzo a la primera mesa de debate del seminario, que se titula «Aproximación a la ciberdefensa». Antes que nada, quería dar las gracias a la Asociación de Periodistas Europeos por contar conmigo para esta ocasión, porque soy un apasionado de estos temas. Creo que es el gran reto que tenemos por delante, como recordaba antes la directora del CNI. Estamos hablando de unas amenazas que se producen en un mundo sin fronteras, sin regulación jurídica alguna, más allá de alguna práctica de buenas conductas que no sirven para gran cosa; con prácticamente una imposibilidad física de seguir la pista de los malos; y con ataques que vienen tanto desde Estados como desde actores no estatales. Es decir, un paraíso para el malo y un infierno para el bueno. Pero para eso están las instituciones: para defendernos. Y eso es lo que vamos a intentar precisar a continuación con dos personas que de esto saben muchísimo.

Tenemos con nosotros al General Miguel Ángel Ballesteros, que es nada menos que el director del Departamento de Seguri-

dad Nacional, y al General Félix Sanz Roldan, que fue JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019. Voy a dar el un turno de intervención primero al General Sanz Roldán. A continuación intervendrá el General Ballesteros y, después, abriremos un turno de diálogo en el que todos podréis participar con vuestras preguntas. Quienes nos estáis siguiendo por Zoom, que por cierto sois muchísimos, también podéis mandar preguntas; me las harán llegar y después trataré de plantear las más interesantes. Por favor, General.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Antes que nada quiero dar las gracias a la Asociación de Periodistas Europeos en los mismos términos que los he hecho en las veintidós ocasiones anteriores. Me gusta decirlo porque en esto, al menos, sí que soy el más antiguo. Y esto tiene mucho que ver con la contumacia de la propia Asociación de Periodistas Europeos, que no deja de cometer el error de llamarme para que venga a hablar de lo que toca cada año, siempre, claro está, en relación con la seguridad y la defensa. Pero todo ello tiene un valor añadido, pues yo conservo los textos que se editan con posterioridad a cada edición de este seminario y es curioso cómo, veinte años después, hay ideas en esos textos que mantienen una vigencia casi absoluta. Por tanto, las reflexiones que realizamos aquí, las mías y las de todos, regidas siempre por los límites que nos marca cada tema a tratar, siempre han dado buenos frutos. Yo les invito a que, cuando quieran saber el futuro que se preveía para la OTAN en el año 2000, vayan y analicen aquello que se discutió aquí, en la Asociación de Periodistas Europeos, hace dieciocho años.

Una de las cosas que siempre me ha sorprendido para bien ha sido la manera de titular estos seminarios y cada una de las sesiones que los conforman. Recuerdo un título singularmente interesante: «Los dioses. Manual de empleo». Era cuando empezaba a surgir el asunto del fundamentalismo yihadista. En esta ocasión, me parece muy acertada, muy conseguida, la gráfica y el texto que nos animan a compartir reflexiones. En este caso, yo las voy a compartir con una persona con la que he estado destinado muchos años en el mismo regimiento y con quien recibí la misma educación, hace también muchísimos años, en el Real Colegio de Segovia. Creo que hubiéramos estado mejor de uniforme, porque venimos a hablar de defensa y siempre es interesante que se sepa que somos dos militares, aunque también es verdad que, en el asunto «cíber», a mí todavía me gusta matizar si estamos hablando realmente de defensa o de seguridad.

Hace ya mucho tiempo que usamos el termino «ciberseguridad». A mí me da la sensación de que es un término más apropiado que ciberdefensa pero, naturalmente, también podemos tratarlo desde ese punto de vista. Yo tuve un magnífico profesor en la escuela de Estado Mayor, Miguel Alonso Baquer, que definía claramente la diferencia entre seguridad y defensa. Él decía algo así como que seguridad es ese estado del que no conviene salir y defensa es el estado que hay que abandonar cuanto antes. Hablaba en aquellos momentos del concepto normal de defensa, en el que se ponen todos los recursos del Estado para parar una agresión, pero la realidad es que las palabras y los conceptos van cambiando y ya no está tan mal hablar de ciberdefensa. No estamos pensando exactamente en el uso de la fuerza, pero sí estamos hablando de muchas otras cuestiones, como limitar los daños que nos puede hacer un adversario, responder a una agresión y, si se han producido daños, ver la forma de resolverlos cuanto antes.

Hoy me voy a ocupar pues del concepto de ciberdefensa, que es sobre lo que me preguntan, siguiendo el método que he empleado durante toda mi vida, que es hacerlo desde diferentes niveles; así es cómo tratamos los problemas los militares, especialmente antes de tratar una estrategia. Se empieza definiendo el problema, algo que estoy seguro de que se hará aquí veinticinco

veces entre hoy y mañana, además de las otras veinticinco o cincuenta veces que ya se ha definido con anterioridad. Por tanto, yo no lo voy a hacer. No voy a decirles a ustedes que el 40% del tráfico es malicioso ni que recibimos 18.000 ataques, de los que tres son críticos. Sé que lo saben de sobra. Pero sí que les voy a exponer alguna de las conclusiones que permiten aplicar el término defensa a la ciberseguridad.

En primer lugar, quiero abordar lo político y las relaciones entre Estados. Emilio Lamo de Espinosa, presidente del Real Instituto Elcano, que con frecuencia aparece en las páginas de pensamiento de los periódicos, nos dice que nos encontramos en un mundo digital y que, por tanto, en este mundo desaparecen todos los conceptos que se volcaron en Westfalia. Puede parecer raro empezar hablando de algo ocurrido en 1648, pero el mundo que hemos vivido hasta hace nada era el de Westfalia. Era el de las fronteras y el del derecho a responder a las invasiones. Pero, como dice Emilio, esto se ha acabado. Ya no hay fronteras que defender. Y es verdad, en muy escasas ocasiones, hay fronteras que se están definiendo con el convencimiento de todos de que lo son. El orden que presidió en Westfalia murió y ahora estamos en otro. Y creo que no exagero si digo que ese otro orden viene de la mano de la red. La red es una y única. Aunque hablemos de la red corporativa del periódico o de la red corporativa de lo que sea, la red es una y única. Todos estamos en la red. Además, no se circunscribe a Estado alguno. Es más, creo que es muy claro que precisamente la red nos ha obligado a concebir nuevos Estados que no tienen fronteras. Podríamos poner, por ejemplo, el caso de Facebook. Facebook es un Estado digital que no tiene fronteras. No podemos considerarlo una nación, pero la cantidad de cosas que puede hacer son de la misma trascendencia, o incluso más, que las que puede hacer un Estado. Pero mucho más importante que eso es la cantidad de ciudadanos que tiene ese Estado. Incluso Estados Unidos, a través de su Congreso, se dice: «Ojo, tenemos que ver qué hace Facebook, qué hacen Google, Apple, etcétera». Y se encuentra con que no dispone de muchos elementos para abordar lo que hacen; la única herramienta que tiene a mano es la ley antitrust. De ahí que los Estados tradicionales tengan que seguir trabajando con estos nuevos Estados con las mismas leyes que tenían antes, desarrollando a matacaballo otras disposiciones que puedan hacer que el mundo de no-Westfalia en el que vimos hoy se parezca un poco al mundo en el que hemos vivido durante los últimos cuatrocientos años.

Me gustaría compartir lo que decía el director del Instituto de Internet de Oxford respecto a que Facebook no es lo suficientemente poderoso como para decidir quién va a ser el presidente de Estados Unidos, pero tampoco es posible ser elegido presidente de Estados Unidos sin una estrategia seria y coherente en Facebook. Esto es un ejemplo de lo que dice Emilio Lamo de Espinosa: las normas que teníamos para un orden internacional ya no nos sirven. Incluido, por supuesto, todo el derecho de la guerra que hemos desarrollado durante siglos. Es curioso como el propio derecho de la guerra y su elemento básico, la Carta de Naciones Unidas, han ido evolucionando con las situaciones que hemos ido viviendo y según hemos ido desarrollando nuestra capacidad de hacernos daño. Cuando aparece la guerra química, la Carta de Naciones Unidas la recoge como un nuevo tipo de agresión y le muestra a las naciones cómo pueden defenderse, cómo pueden realizar el proceso de identificación del agresor, volver a agredirlo en su justa medida, etcétera. Ocurrió lo mismo cuando aparecieron las armas nucleares. En ese momento España era miembro no permanente del Consejo de Seguridad de Naciones Unidas y la Carta de Naciones Unidas debía prever con qué elementos contaríamos para su definición cuando hubiera una agresión de este tipo y cómo podríamos hacerle frente. Pero ese caso no se ha dado.

Estamos en un mundo nuevo, con un orden nuevo, con naciones que no son naciones, pero nos falta legislación, nos falta poner orden en el orden. Y eso es lo que tendríamos que hacer.

Los Estados, que sí que tienen fronteras y que sí tienen capacidad de actuar dentro de esas fronteras, son uninacionales, tienen fronteras y no pueden legislar por sí mismos nada que exceda su territorio. Por tanto, es importante utilizar para todas estas cosas las organizaciones internacionales, además de las organizaciones regionales. Si verdaderamente estamos hablando de algo parecido a la guerra, entre las soluciones que casi de forma inmediata se nos ocurren está, primero, la regulación; una regulación específica y nueva y un derecho internacional específico y nuevo adaptado a este problema. Si, desde las instituciones que conforman la comunidad internacional o desde las organizaciones regionales de las que hemos hablado, hemos sido capaces de llegar a los diferentes acuerdos START, si hemos sido capaces de llegar a una situación en la que todos hemos estado de acuerdo a la hora de retirar las armas nucleares tácticas de Europa, cómo no vamos a llegar a acuerdos en la comunidad internacional sobre cómo tratar estos asuntos que nos atañen ahora, si es que queremos tratarlos como una agresión superior a la del ámbito de la seguridad. Lo primero que se requiere es la educación. Con educación me refiero a convencernos y convencer a los demás de que la gestión de lo privado es un derecho humano y no es un activo comercializable. Y no solo estoy hablando de los datos. Los datos son mi derecho pero mi vida lo es más aun. Habrá que hacer algo para que ese derecho no se vea amenazado.

Hay algo más que también debíamos considerar, aunque es difícil usar un término concreto. A mí no se me ha ocurrido otro mejor que nacionalismo digital, pero lo voy a explicar y espero que entre todos acuñemos un término nuevo. Ningún Estado debería llegar al punto de tener que decidir quién quiere que ocupe nuestra red. Es decir, ¿queremos que el 5G que va a ocupar nuestras redes venga de Estados Unidos o venga de China? ¿Quién queremos que nos colonice a este respecto? ¿Estados Unidos o China? El presidente de Unisys decía que no se nos reconocerá capacidad de protegernos si no se nos reconoce que poseemos

suficiente tecnología como para podr asegurar nuestra seguridad, nuestro crecimiento económico y la protección de nuestras infraestructuras. Y esto es válido también en el ámbito internacional. Pero nosotros, para poder participar en ese juego de crear estructuras, de crear un derecho que nos ampare de este tipo de acciones, primero debemos tener alguna fuerza, debemos tener algo con lo que jugar.

Así llegamos al siguiente asunto que, también desde el punto de vista de lo militar, es nuestro día a día, la táctica, algo en lo que España ha hecho bastantes cosas. Aquí se puede ser triunfalista o no, pero o poco le interesamos a los malos o realmente en nuestro país se ha conseguido que no haya habido grandes desastres derivados de sus acciones en la red. Por tanto, vamos a pensar que algo estamos haciendo bien. Desde el año 2013 tenemos en España una Estrategia Nacional de Ciberseguridad con unos objetivos muy claros que posiblemente todos ustedes conozcan, pues están recogidos y ampliados en la Estrategia de Ciberseguridad del año 2019. Pero no sólo eso. También creamos el Consejo de Ciberseguridad., que fue el punto focal en el que se discutían todas las actividades relacionadas con lo cíber: las militares y las que no lo eran; las de infraestructuras críticas y las de ataques en la red; la comisión de delitos en la red o el mero hecho de molestar para hacerse notar. También se creó el Mando de Ciberdefensa, que tiene mucho que ver con una organización regional que se dedica a la defensa y que también quiere estar segura en su ámbito. Tenemos un documento reciente, singularmente importante, que se llama «España Digital 2025». Yo les invito a que lo miren. Hay un resumen ejecutivo bastante corto en internet que incluye dos de los elementos fundamentales. El primero es la importancia de la propia ciberseguridad y, el segundo, todavía más tangible es la creación del Centro Nacional de Ciberseguridad, algo con lo que llevamos algún tiempo pero que, por determinadas razones que yo no voy a juzgar hoy aquí, hasta ahora no ha sido posible. Pero ya ha llegado el mo-

mento de conseguirlo, especialmente por su conexión con la defensa. Porque crear un centro de operaciones supone tener un puesto de mando y un puesto de mando es un lugar con analistas de todo tipo que son capaces de definir qué tipo de amenazas se reciben en tiempo real. Pero, mucho más importante que eso, son capaces de reaccionar de forma inmediata para contrarrestar una amenaza.

Si nos tuviéramos que quedar con una sola cosa de esta breve reflexión que he hecho sobre ciberdefensa, huyendo de los términos que generalmente se han barajado, debería ser eso: nos falta un Centro de Operaciones de Ciberseguridad que, en los ataques cíber, tenga la capacidad de interpretar una agresión y de dar una reacción sólida, contribuyendo, dentro de esta terminología dual de los elementos de defensa, a que España también esté más segura en este ámbito.

JAVIER GARCÍA VILA
Moderador

Gracias, General. Has abierto algunos temas muy interesantes que luego, si tenemos tiempo, intentaremos precisar un poco más y poner negro sobre blanco. General Ballesteros, por favor, su turno.

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Muchas gracias. En primer lugar, quisiera agradecer a la Asociación de Periodistas Europeos su invitación. Yo no llevo veintidós años como el General pero sí que he venido ya unas cuantas veces. Todavía recuerdo que, en 2003, tuvimos que interrupción una sesión porque entraron unos manifestantes en el Parador de Toledo. Sin duda, éste es un seminario sumamente interesante, con el añadido de que luego, además, lo tienes por escrito. En esta ocasión tengo un doble agradecimiento: el agradecimiento por haber sido invitado a participar en él y por compartir sesión con el General Félix Sanz Roldán, que para mí es un referente profesional. Por ello, compartir con él esta tarima no deja de ser un doble honor. También les diré que no me siento muy cómodo teniendo que hablar aquí sobre la aproximación a la ciberdefensa teniendo entre el público al General del Mando del Ciberespacio; quizás yo hubiera estado mejor ahí y él aquí. Dicho esto, como director del Departamento de Seguridad Nacional, un puesto privilegiado que permea todo el sistema, voy a orientar mi intervención desde el enfoque de la seguridad. Es decir, les voy hablar de la ciberdefensa dentro del sistema de seguridad nacional.

Permítanme dos obviedades. Estamos en un mundo globalizado, sí. Acaba de empezar la segunda globalización, también. Ayer mismo leí un artículo sobre este tema que decía que la globalización nació en los años ochenta –aunque Marshall McLuhan ya vislumbra en los sesenta esa aldea global– pero que es de la mano de las tecnologías de la información y de la comunicación, de la mano de internet a finales de la década de los ochenta, cuando llega realmente la globalización. La globalización se caracteriza por la velocidad de cambio, por la aparición de riesgos y amenazas poliédricas que, si no sabemos ver que son poliédricas, nos pueden conducir a errores.

Ahora estamos viviendo la primera gran amenaza global, que ha forzado al confinamiento de más de un tercio de la comunidad mundial, de los habitantes de este planeta. En principio, para mucha gente, la crisis de la COVID-19 es una crisis sanitaria. Hoy ya sabemos que no es una crisis sólo sanitaria. Es una crisis económica, una crisis social, una crisis comercial... En definitiva, es una crisis endemoniadamente poliédrica. Si enfocamos el tema sólo desde un punto de vista, lo enfocaremos mal. Estos riesgos y amenazas son difíciles de evaluar. Llevamos seis meses de pandemia y todavía no somos capaces de vislumbrar lo que va a venir, lo que queda por delante. Y tampoco somos capaces

de saber bien cómo se comporta el virus. La pandemia resulta difícil de predecir. Se hacen continuamente previsiones y continuamente hay que rehacerlas porque no se cumplen.

En este mundo tan cambiante, aparece un espacio nuevo: a tierra, mar y aire hay que añadir ahora el ciberespacio. Un ciberespacio que ha dado lugar a las llamadas estrategias híbridas, que a su vez han dado lugar a los conflictos híbridos, que se caracterizan por dos elementos claves. Un elemento clave de los conflictos híbridos, de las estrategias híbridas, es la desinformación y, el otro, la ciberdefensa. El General Sanz Roldán ha sido el presidente del Consejo Nacional de Ciberseguridad. Como el bien sabe, en un momento determinado nos encontramos con que había que situar las amenazas híbridas dentro del sistema de seguridad nacional. ¿Dónde las colocamos? Todavía recuerdo una intervención suya en el consejo donde dijo que si algo tienen en común las estrategias híbridas es que siempre está presente la ciberseguridad. Yo añadiría que lo mismo ocurre con la desinformación. Así que, mientras no se acuerde un comité de amenazas híbridas, tendremos que encajarlas en el Consejo Nacional de Ciberseguridad, ya que la ciberseguridad siempre aparece en las estrategias híbridas.

Respecto a la desinformación, también aparece la necesidad de diseñar buenas estrategias de comunicación. Traigo esto a colación porque estamos en un seminario organizado por la Asociación de Periodistas Europeos. El periodismo que hacen los miembros de la APE no es el periodismo de las redes sociales, ése en el que no se sabe de dónde viene la noticia y en el que, además, ésta está sin contrastar, sino ese periodismo que es una pieza clave para la lucha contra una desinformación que es capaz de producir unos daños enormes.

Si a algo nos conduce el uso del ciberespacio, de esas amenazas poliédricas, es a la necesidad de tener un sistema de análisis geopolítico. La geopolítica nos da esa visión poliédrica de los problemas que nos permite ver venir las crisis con un poquito

de antelación, ya que con mucha antelación es imposible en las circunstancias en las que vivimos. Pero eso exige un análisis permanente. Y exige también una integración de la información. Todo ello conduce, inevitablemente, a la creación de un sistema de seguridad nacional que integre esa información y proporcione información integrada al Gobierno –que es el que tiene que tomar las decisiones– para que sea capaz de tomar las decisiones adecuadas. Ese enfoque integral es fundamental. Esto lo descubrimos todos el 11 de septiembre de 2001 con el ataque terrorista de Al Qaeda contra las Torres Gemelas, contra el Pentágono… Entonces se llegó a la conclusión de que la información de las quince agencias de investigación de inteligencia que había en ese momento en Estados Unidos no estaba integrada. Por eso no habían sido capaces de detectar el ataque, no habían sido capaces de predecir la posibilidad de un ataque. En segundo lugar, las estrategias, que en Estados Unidos ya se llamaban de seguridad nacional, usaban una única herramienta, que eran las Fuerzas Armadas. Y las Fuerzas Armadas solas no habían sido capaces de evitar un ataque en el que murieron en una mañana casi tres mil personas y quince mil resultaron con daños permanentes. No habían sido capaces de evitar un ataque en el corazón financiero del país, ni tampoco en el militar y en el político, si contamos el avión que se derribó antes de alcanzar su objetivo. Fue entonces cuando se llegó a la conclusión de que las estrategias de seguridad nacional deben tener un enfoque integral, poliédrico. Y si hay algo transversal a todas las amenazas, a las ciberamenazas, son las Fuerzas Armadas, que tienen que proteger sus propias redes, diseñar operaciones que se solapan con las operaciones militares y ser capaces de llegar donde no pueden llegar otros instrumentos del Estado. Este enfoque integral lo da el Sistema de Seguridad Nacional. Me van a permitir que lo enfoque muy rápidamente.

Vayamos a la Estrategia de Seguridad Nacional 2017, que es la que está en vigor y la que se va a revisar ahora; aunque estas

estrategias se revisan más o menos cada cinco años, la COVID-19 ha demostrado que hay que mejorar el enfoque. En esta estrategia, cuando se habla de amenazas y desafíos –no conozco las razones por las que se cambió la palabra riesgos por desafíos, aunque probablemente sea más asumible políticamente–, aparecen cosas como cambio climático, epidemias y pandemias, migración, etcétera. En cambio, si preguntáramos al común de los españoles cuál de los riesgos y de las amenazas son actualmente los más afectados, obviamente la gran mayoría hablaría de la vulnerabilidad del ciberespacio, que es uno de los tres espacios comunes y que se caracteriza por una bajísima regulación. El espacio aéreo, por ejemplo, está regulado, pero el ultraterrestre no lo está; el espacio marítimo también está regulado aunque no lo suficiente teniendo en cuenta que es muy difícil controlar los grandes océanos. Así que ahí estaríamos todos de acuerdo: el ciberespacio es una de las amenazas que enfrentamos.

La directora del CNI hablaba de como, con la COVID-19, se ha acelerado todo lo relativo al ciberespionaje, que busca entrar en los laboratorios. En este momento hay doscientos y pico proyectos de vacuna y hay muchos Estados, y no Estados, a los que les gustaría saber hasta dónde y en qué se basan los avances científicos de cada uno de esos laboratorios. Y en algunos casos lo han logrado. Sin duda, los ciudadanos también habrían identificado el espionaje como una amenaza. ¿Habrían identificado también la protección de las infraestructuras críticas? Yo creo que sí, al menos el de aquellas empresas claves que están recibiendo ataques. El año pasado hubo treinta y cinco ataques críticos –si no recuerdo mal–, la mayoría contra infraestructuras críticas, a las que también les afecta la ciberseguridad. ¿Y el terrorismo? Todo el mundo sabe que el Daesh se ha apoyado en dos grandes pilares: uno, la comunicación y el reclutamiento a través del ciberespacio, y, dos, el dominio del territorio facilitado por la inmigración de combatientes al califato. Ese control del territorio también le permitió movilizar, de una población total de ocho millones de personas, a unos cuantos miles, al igual que lo hacen los Estados.

¿Y si nos hubieran dicho que los conflictos armados tienen también un componente de ciberseguridad? Pues posiblemente ahí el ciudadano de a pie nos hubiera dicho que ahí no, pero yo les digo que sí, que la ciberseguridad llega ahí, que está ahí permanentemente. Como dice el General Guerásimov, el JEMAD ruso, hoy los conflictos armados empiezan en el ciberespacio. Según su doctrina, las Fuerzas Armadas, aunque siguen teniendo un papel muy relevante, hoy tienen otro papel, pues se pueden hacer muchas cosas previas que evitan tener que llegar al uso de la fuerza. Esto es así por dos razones. Primero, por la seguridad enorme que da la dificultad de atribución, saber quién está detrás de un ciberataque. Es muy difícil tener pruebas de quién está detrás porque se utilizan *proxies* y *bots*, como mencionaba la directora del CNI. Es más, incluso se utilizan actores involuntarios. Un ordenador de un ciudadano no protegido es susceptible de ser empleado como un atacante contra un tercero, lo cual hace que sea muy difícil atribuir el origen de cada ciberataque. La segunda característica, según Guerásimov, es la difícil relación entre causa y efecto. Detrás de la desinformación en las elecciones norteamericanas de 2016 han estado organismos rusos. Y digo organismos rusos, que no es lo mismo que el Gobierno ruso. Eso está probado según un informe que se hizo en Estados Unidos. Pero ¿eso ha logrado cambiar el Gobierno, consiguiendo que en vez de Hillary Clinton saliera el presidente Trump? Eso es imposible de demostrar. No hay posibilidad de establecer una relación de causa-efecto. Y eso es una gran ventaja para los agresores.

Entonces, ¿cómo nos defendemos los países? Pues con una estrategia clásica de defensa; la represalia. La represalia consiste en mandar un mensaje al adversario, a aquel otro país con el que tienes un conflicto, diciéndole: «Oye, no te metas conmigo porque tengo la misma capacidad militar que tú y si te decidieras a lanzarme un ataque, lo cual es absolutamente ilegal, pues está

prohibido por la Carta de Naciones Unidas, yo tendría derecho a la legítima defensa según el Artículo 51 y saldrías muy dañado». Por ejemplo, en el tema nuclear la represalia, el «*si vis pacem, para bellum*», ha dado resultado al 100%; ahí nunca ha fracasado. En el tema convencional sí ha habido muchos fracasos con esta estrategia pero, aun así, es una estrategia que se sigue utilizando y sigue siendo una estrategia de éxito. Pero, en el caso de las ciberamenazas, la única herramienta para aplicar esa estrategia de la represalia es la ciberdefensa, que es una pieza clave.

¿Y la migración? ¿Tiene algo que ver la migración con las ciberamenazas? No con las ciberamenazas exactamente, pero hay que tener en cuenta que las redes sociales son el cauce que utilizan las mafias de tráfico de personas para alentar, cuando les viene bien, el tráfico de personas para cruzar con patera.

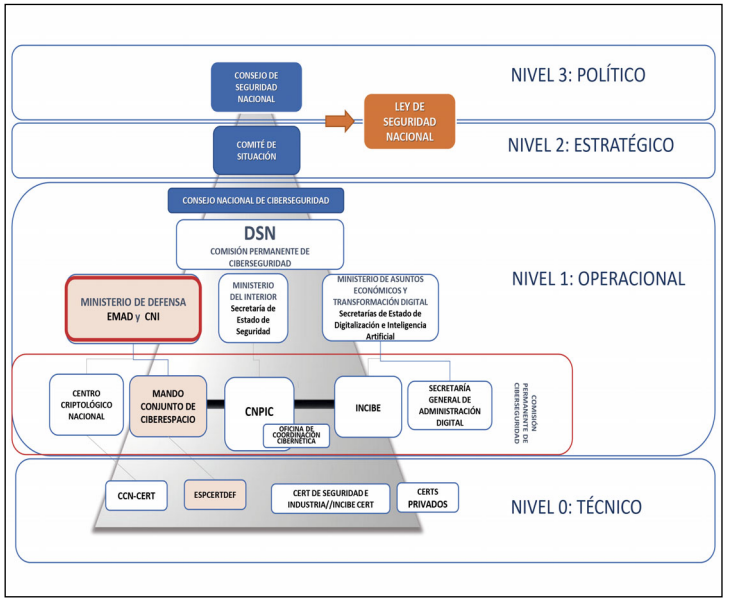
Con todo esto, lo que quiero decir es que estamos ante un problema cada día más importante. Ahí tienen los datos del Informe Anual de Seguridad Nacional correspondiente a 2019 y del Centro Criptológico Nacional; y no entro en los datos del INCIBE ni de los ataques a empresas. Se contabilizaron 42.997 ciberataques, mayoritariamente dirigidos a la administración, de los cuales 3.172 fueron muy importantes y 37 fueron críticos, entendiendo por críticos que el daño se traslada al ciudadano directamente y que no es fácil resolverlo de forma automática. En la estrategia de 2017 se habla de cinco dinámicas de transformación y una de ellas se refiere a la dimensión tecnológica. Precisamente esa dimensión tecnológica hace que esto no sea estable nunca sino que esté en continua transformación. El 5G es algo que se está empezando ya a implantar en España y que requiere adoptar medidas de seguridad nacional, medidas para las redes que afectan a la seguridad nacional, muy especialmente a la ciberdefensa. La ciberdefensa hoy es una defensa mayoritariamente compartida en la OTAN y en la Unión Europea, que tiene una cláusula de defensa mutua. Para que las organizaciones internacionales alimenten con información a sus países miembros, es necesario disponer de redes seguras. Y esas redes seguras pasan porque, a la hora de dar el salto al 5G, las redes de defensa sean especialmente seguras. Hay que adoptar medidas especialmente seguras para esas redes, pues afectan a todo el sistema de seguridad nacional. La Unión Europea ya ha dictado unos criterios, en lo que se llama la *tool box*, la caja de herramientas de lo que recomienda. Y recomienda tener cuidado con el *vendor risk*, con los proveedores de riesgo, y no incluirlos en zonas sensibles. también recomienda no tener un único proveedor en una red, porque al final estás en manos de una empresa. También habla de las amenazas híbridas, algo que ya ha mencionado el General y que es un tema importantísimo en el que todos estamos implicados; especialmente en defensa.

Entendemos por amenaza híbrida, como dice el Teniente Coronel Frank G. Hoffmann, «cualquier adversario, actor estatal o no estatal, que de manera simultánea y adaptativa, emplea una mezcla de armas convencionales, tácticas irregulares, terrorismo y comportamiento criminal en el espacio de batalla para alcanzar sus objetivos políticos». La alta tecnología que hay que emplear para actuar contra un Estado va disminuyendo las posibilidades de que sea un *hacker* quien lance una guerra híbrida. Es imposible que lo haga. Las guerras híbridas las lanzan los Estados. Lamentablemente, las guerras convencionales son palmarias, tienen lugar a la luz de los ojos del mundo. De ahí que estén condenadas y que ahora los Estados se agarren a las guerras híbridas, que no están a la vista y resultan pues mucho más tentadoras. Guerra híbrida es aquella que emplea una combinación de instrumentos convencionales y no convencionales, como el ciberataque, la desinformación, la presión económica, la presión energética, etcétera. Ejemplos de guerras híbridas son la que en 2006 se produjo entre Hezbolá e Israel o el conflicto de Ucrania, con el triunfo de la estrategia híbrida rusa; y digo triunfo porque se ha quedado con la península de Crimea y porque el valle del Donbás, toda la zona de Donetsk, Lugansk, etcétera, ya no está

bajo el control del Gobierno de Kiev. Es ésta una cuestión sin resolver y de difícil solución.

¿Dónde está el sistema de seguridad nacional? ¿Qué hace la ciberdefensa? Debajo de la política nacional aparece la Estrategia de Seguridad Nacional y su principal instrumento, el Consejo de Seguridad Nacional. Éste, además del presidente, lo preside también –al menos una vez al año– Su Majestad el Rey, y están implicados los ministerios afectados –aunque también pueden participar otros ministerios cuando es necesario– y cinco secretarios de Estado, de los cuales uno es el director del CNI, otro el director del Gabinete del Presidente, otro el JEMAD, otro el secretario de Estado de Política Exterior –una pieza fundamental– y, por último, el secretario de Estado de Seguridad. También asiste el director de Seguridad Nacional; aunque no participa en las decisiones, sí está en las discusiones. Los comités, o consejos, que asesoran al Consejo de Seguridad Nacional están en el segundo nivel. Y en este segundo nivel está también el Comité de Situación, que en principio está presidido por la vicepresidenta Primera, que se encarga de la gestión de crisis. Debo decirles que durante la crisis de la COVID-19 se activó este comité, recopilando información de ciberseguridad cuando ha sido necesario. Y, debajo, están las estrategias de segundo nivel. Una de esas estrategias es la Estrategia Nacional de Ciberseguridad. En el tercer nivel es donde están los planes, además de una estrategia, que es la estrategia militar. Y dentro de la estrategia militar están los planes de ciberdefensa, que se encargan de la protección de sus propias redes, de las operaciones propias de ciberdefensa y de la disuasión cibernética, un instrumento propio de la ciberdefensa. Y ya debajo estaría el cuarto nivel, que son las operaciones, que es donde encaja todo este sistema.

El General Sanz Roldán también ha hablado de la nueva estrategia, que es muy diferente a la de 2013, que puso en marcha todo el sistema de seguridad nacional, mientras que la de 2019 intenta ser una estrategia mucho más práctica y adaptada a la ini-



ciativa de protección de las redes que establece la Unión Europea. Si miramos el esquema del interior del sistema, vemos que debajo de ese Comité de Situación está el Consejo Nacional de Ciberseguridad, que ha presidido el General, y también un Comité Permanente de Ciberseguridad que incluye el Mando Conjunto del Ciberespacio. Están también el Centro Criptológico Nacional, el Centro Nacional de Protección de Infraestructuras Críticas, el secretaria está entre el público–, la Secretaría de Estado de Avance Digital e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones. Debajo están los centros de respuesta. Aquí es donde aparece ese Centro de Operaciones de Ciberseguridad, ese centro de inteligencia que falta por implementar, aunque ya está aprobado y creo que la principal causa de que aún no esté en funcionamiento es que no ha habido unos presupuestos que lo doten económicamente. Hasta ahora ha sido imposible montarlo pero su creación es urgente.

Aquí voy a hacer un inciso para explicar cómo funciona esto en otros países. Por ejemplo, el Reino Unido tiene un centro de respuesta para todo el Estado; para la administración, para las empresas, para todo. Lo único que no está incluido dentro de ese centro es el Mando de Ciberdefensa británico. Lógicamente, lo militar está al margen, por todo lo que les decía y por sus peculiaridades: protegen sus redes, diseñan operaciones y tienen la capacidad de ejercer la disuasión, lo cual no está dentro de los centros de respuesta, que se limitan a actuar cuando se produce un ataque, a desarrollar la capacidad de pararlo y de ser resiliente en el menor tiempo posible. Como decía, los británicos tienen todo eso aglutinado en un único centro en el que trabajan cerca de mil personas, de las cuales aproximadamente ochocientas son funcionarios o personal laboral; el resto son de empresas que diseñan, que trabajan en la investigación, etcétera.

En España, en cambio, tenemos el Centro de Respuesta para la administración, el Centro Criptológico Nacional, el Centro de Respuesta de apoyo a las empresas, que es INCIBE. Y también

tenemos centros de respuesta en comunidades autónomas, aunque no en todas; en algunas hay centros de mucho peso, como es el caso del CESICAT, el Centro de Ciberseguridad de la Generalitat. Así es como funcionan las cosas ahora. Convendría, de vez en cuando, hacer una reflexión sobre esto, aunque siempre habrá que acomodarlo a las peculiaridades de España y a su sistema administrativo, que desde luego no es el que tiene Francia, un país jacobino que tiene a la ANSSI, que es una agencia también de ciberseguridad que lo abraca prácticamente todo; siempre dejando lo militar al margen. Ése es el sistema.

En la nueva Estrategia de Seguridad Nacional se ha dado mucha importancia a la colaboración público-privada, pues no podemos aspirar a estar en lo último en este campo si sólo contamos con la administración. Lo que se ha creado es un foro nacional de ciberseguridad, que ya está trabajando, compuesto por organizaciones que no son de la administración. Hay representación de las grandes organizaciones y de medios de comunicación especializados. Ese foro, con personal ajeno, lo que hace es proporcionar una colaboración a la administración con ideas, con trabajos, etcétera. En este momento se están montando tres grupos de trabajo en su seno. El primero es un grupo de trabajo para estudiar la cultura de ciberseguridad en España. El segundo es un grupo de trabajo para gestionar el conocimiento, para ver si tenemos cubiertas todas las necesidades en las universidades y si somos capaces de retener el talento. Y el tercero es el de I+D+i. Y aquí vuelve a aparecer la ciberdefensa.

En el ámbito convencional, la defensa se ha caracterizado por el I+D. En todos los sistemas de comunicación, satélites, barcos, aviones, vehículos, etcétera, si uno quiere ver lo último en tecnología tiene que ir a las industrias que trabajan en materias de defensa. Y en ciberseguridad tiene que ocurrir lo mismo. Tenemos que poner el foco en esa forma de trabajar porque, cuando se diseñan los planes estratégicos y se determina qué capacidades se necesitan, los barcos, los aviones…, ahí tiene que

estar lo último de lo último. La capacidad es mucho más que el aparato. Es la organización, el saber manejarlo, la formación del personal, etcétera. Debemos ver cómo tiene que ser el barco que se diseñe, que va a entrar en funcionamiento dentro de cuatro años y tiene que seguir dando servicio dentro de veinticinco. Hay que hacer un esfuerzo por analizar esas capacidades, para ver cómo cumplimos con todas esas expectativas. En ciberdefensa, lo de los veinticinco años es imposible, pues cambia todo muy rápidamente, pero hay que hacer –y seguro que se está haciendo– ese esfuerzo por estar en la punta de la tecnología a nivel mundial. Ésa es la única forma de tener unas capacidades adecuadas y poder ejercer la disuasión frente a actores externos.

JAVIER GARCÍA VILA
Moderador

Muchas gracias, General. Ha sido interesantísimo escucharte. Tengo muchísimas preguntas de los asistentes que han acudido al encuentro, así como de los que nos siguen *online*. Pero antes permitidme que intentemos concretar algunas de las cosas que habéis comentado. Ha habido una coincidencia muy clara en los dos sobre la demanda de un Centro de Operaciones de Ciberseguridad, que yo me permito calificar como un CNI del ciberseguridad. El General Ballesteros ha dicho que se trata de un mero problema presupuestario, luego deduzco que si hay presupuestos se pondría en marcha este CNI de ciberseguridad. ¿Es así?

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Yo quiero pensar que sí porque cuando estaba al frente del CNI el General Sanz Roldán, que fue uno de sus principales impulsores, tampoco fue posible. La única resistencia es que en España se funciona con un presupuesto aprobado por las Cortes y,

mientras no tengamos ese presupuesto, no se puede crear un órgano que no está dotado económicamente.

JAVIER GARCÍA VILA
Moderador

Precisamente sobre este asunto incide el compañero Miguel González, de *El País*. Pregunta si ese Centro Nacional de Ciberseguridad del que ha hablado el General Sanz Roldán podría ser la fusión del CCN y del INCIBE.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

No. El elemento de partida es que no es un CNI de cíber. Podríamos hasta haber usado un término militar, como puesto de mando contra los ataques cibernéticos o algo así. El término debería ser militar porque las normas de funcionamiento son militares. Es como un puesto de mando, aunque de otro tipo. En ese puesto de mando se recibe la información de que se está generando un ataque y esa información la estudian los expertos del mismo puesto de mando e, inmediatamente, le hacen frente, con los medios que tengan a su disposición. Por tanto, no es sólo inteligencia o información. Es información en tiempo real. Se ve lo que está ocurriendo en tiempo real en la red en España, se analiza quiénes son, qué hacen, si son fuertes o son débiles, si es limitado o amplio, etcétera, y a continuación se decide cual es el instrumento más importante o adecuado que se tiene a mano para hacerle frente. Entonces viene la segunda parte. Pero ambas se hacen en un único puesto de mando con dos elementos, uno dedicado a saber lo que pasa y otro a actuar contra lo que pasa. Estaba hasta pensado el edificio que alojaría el puesto de mando. De hecho, yo llegué a preguntar por qué no poníamos el letrero y la bandera. Eso ya de por sí tendría un efecto para el ciudadano.

JAVIER GARCÍA VILA
Moderador

¿Dónde estaba el edificio?

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Cerca del cine Palafox de Madrid. Era un edificio antiguo, pero realmente nunca hubiera sido el emplazamiento definitivo porque para esto se necesita algo mucho más sólido. La idea era arrancar ahí y que no fuera de nadie, porque allí estaríamos sentadas personas del Centro Nacional de Inteligencia, de la Guardia Civil, de la Policía, de los especialistas en redes… En el puesto de mando habría todo tipo de personas; incluso podría haber oficiales de enlace de otros mandos de ciberseguridad. Tendría ese sentido de puesto de mando. Y también tendría una función adicional, además de actuar contra quienes nos atacan, que sería poder presentar posturas únicas a la vista del análisis que allí se haría de una determinada emergencia. En una ocasión, un responsable político me dijo que había habido un problema cíber y que tenía cinco papeles de cinco organizaciones, que todas tienen sus responsabilidades. Posiblemente los cinco estaban bien pero ese responsable político lo que quería era un solo papel. El puesto de mando también tendría esa virtud: la de aportar datos unificados desde el campo táctico, que es donde estamos, no desde las grandes estrategias.

Como ha dicho el General Ballesteros, hasta ahí llegamos. ¿El problema es de dinero? Para empezar sí, es un problema de dinero. Después, cuando se cree, surgirán otras aristas que también habrá que tratar, que pueden ser más complejas, como integrar culturas tan diferentes en un solo sitio para hacer frente a esos problemas. Pero inicialmente, para poner la bandera y el letrero, es lo que hay.

JAVIER GARCÍA VILA
Moderador

Para terminar con este asunto, ¿sería razonable salir de aquí con la idea de que en los próximos meses, no años –porque esto va muy rápido–, tendremos ese centro operativo?

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Yo no estoy en condiciones de poder asegurar eso porque se presupuestó la creación de este centro a finales de 2018 o principios de 2019, cuando la circunstancia presupuestaria era distinta a la de hoy. Por eso yo no me atrevería asegurar nada.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Hay un documento importantísimo que ha lanzado el Gobierno. Se titula es «España digital 2025» y está en la red, donde todos podemos consultarlo. Uno de los puntos que abarca es el de la ciberseguridad. Desarrolla cada uno de los puntos y además dice que va a estar vestida toda esa estrategia con una cantidad de dinero que está citada en el plan. Y una de las cosas que dice es: «Despliegue y operación del Centro de Operaciones de Ciberseguridad». Es verdad que luego el presupuesto es lo que te gastas cada año, pero en la Estrategia Nacional vuelve a estar. Y en «España Digital» se dice de cuánto dinero va a estar dotado.

JAVIER GARCÍA VILA
Moderador

Otro asunto importante. En su intervención, el General Ballesteros ha hablado de 37 ataques críticos en 2019 y ha definido lo

que es un ataque crítico: que tenga repercusión sobre la gente y sea muy difícil de neutralizar. Al hilo de esto, pregunta Ana Alonso, de *El Independiente*: «¿Qué ciberataques se han detectado desde que empezó la crisis de la COVID-19 y cómo se han neutralizado?».

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

En la crisis de la COVID-19 no ha habido mucha actividad. Esperábamos que, como todo el mundo estaba teletrabajando, hubiera un incremento de la actividad de ciberamenazas. ¿Hay amenazas ahora? Sí, hay algunas empresas muy importantes, cuyos nombres no puedo daros, que en este momento están sufriendo ciberataques, pero no hemos detectado un incremento respecto al período anterior. Incluso se han atacado hospitales, aunque parezca mentira. Pero es que se ataca todo. 42.000 ataques dan para mucho. Los menos preocupantes son los ataques de denegación de servicio que, por ejemplo, hacen que durante equis horas no puedas acceder a la página web si tienes que hacer una cita para una consulta médica. Otra cosa son los *ransomware*, los secuestros de ficheros, que se han convertido en un negocio y que son un problema muy grave.

JAVIER GARCÍA VILA
Moderador

Al hilo de una pregunta que nos plantea Jaime por Zoom y de lo que ha dicho la directora del CNI quisiera preguntaros sobre el peligro de que un ordenador personal civil sea utilizado para un ataque más grande, algo que está ahora muy de actualidad por lo del teletrabajo, ya que hay mucha gente teletrabajando en todo el mundo. ¿Cuál sería vuestra recomendación al respecto? Y, por otro lado, ¿se podría crear una legislación parecida a la que tiene Corea del Sur sobre la creación de un documento nacional de identidad virtual?

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Lo que es importante es que el ciudadano y las empresas tomen conciencia de la importancia de la ciberseguridad. En España hay personas que creen que eso de la protección del ordenador es una cosa que te dan gratis. Y, si no te lo dan gratis, no lo pones. Y no es así. Esto es algo que hay que poner. No sólo hay que poner los antivirus. También hay que poner los *firewalls*, las barreras para que no entren. Alguno de los ataques que ha habido últimamente han tenido lugar en los accesos remotos a las empresas, que van securizados. El que se conecta sabe que hay algunas empresas potentes en las que está habiendo algunos problemas. Es importante que todos los ciudadanos tomen conciencia de que, igual que pones una cerradura en la puerta de tu casa, debes poner cerraduras en tus ordenadores. Y lo mismo con el móvil, porque el móvil es un ordenador. Esa falta de cultura es lo que permite que los malos cojan tu ordenador y lo utilicen como un *bot*, como un ordenador remoto, de tal forma que es tú ordenador el que está atacando a un tercero. Y eso provoca que, al final, estemos atacando a nuestras empresas desde nuestros propios ordenadores.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Cuando compramos un frigorífico, ese frigorífico llega a nuestra cocina después de haber pasado muchísimas pruebas de seguridad, como por ejemplo que no tenga fugas de gas. En cambio, cuando compramos un ordenador o una tableta el único instrumento que ha pasado una prueba de seguridad es el cargador. Por

tanto, ¿no deberíamos hacer con los ordenadores y con las tabletas exactamente lo mismo que hacemos con las neveras? Debería haber un centro, sea nacional o multinacional, en el que se diga a las empresas que si quieren vender ordenadores tienen que llevar todo esto puesto. Y, si no lo lleva, no pueden venderlo. Ése es el asunto que, para mí, nos queda por cubrir. ¿Cómo es posible que la tableta que compré ayer sólo tenga un certificado de seguridad y que sea el del cargador?

Paso al segundo asunto. ¿Cuándo están las empresas propiciando la seguridad y cuándo no? Aquí hablarían los más técnicos de los fallos del día cero de cada uno de los elementos que se ponen a la venta. Hay muchos elementos que, el mismo día que se ponen a la venta, alguien ya ha pagado para saber todos los fallos que tiene su sistema, en el día cero. Y con esos fallos del día cero se han hecho unas maniobras de ataque terribles. Un caso es el WannaCry, que paró la mayor parte de la sanidad del Reino Unido y que en España también atacó a mucha gente. Se trataba de un fallo de día cero de un teléfono móvil. Por tanto, estoy de acuerdo en que hay que ser cuidadosos, pero vamos también a lo básico: antes de vender un ordenador con un determinado *software*, usted tiene que reunir todas las condiciones necesarias para hacerlo con seguridad. Y si ese ordenador va a hacer una determinada acción que está fuera de lo normal, debe haber alguien que lo pare en la puerta.

Y otra reflexión muy breve. El hecho de que desde un ordenador personal de alguien que está en zapatillas en su casa, porque está con el coronavirus, se pueda atacar los ordenadores de la administración de España no quiere decir que vayamos a dejar de hacer ordenadores personales cada vez más pequeños y más potentes. Lo que hay que hacer es regular. Hay que dotar a la administración de herramientas, de normas complementarias, de leyes, que permitan vivir dentro del progreso. Como ha dicho el General Ballesteros, también hicimos las bombas atómicas, que son terribles, y hemos sido capaces de regularlas. Pues con esto

tiene que ser un poco igual. Este esfuerzo sí que es imprescindible. Si todos los instrumentos que utilizamos en nuestra vida vienen con certificaciones de seguridad, si hay agencias, empresas y organizaciones internacionales que dan esas certificaciones para otras cosas, para los ordenadores también debe haberlas. Basta ya de que el único elemento seguro de un ordenador sea el enchufe.

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Las cosas cambian tan rápidamente... Hace cinco años los parches que se le ponían al *software* estaban probados y se sabía que iban a funcionar bien. Pero hoy cambia tan rápidamente todo que los parches que carga Microsoft, día sí y día no, muchas veces no han sido sometidos a suficientes pruebas. ¿Por qué? Porque si esperan el tiempo necesario para probarlos el agujero de seguridad está demasiado tiempo abierto. Así que lo que se hace es parchear ese agujero y ya se parcheará sobre ese parche para ir tapando nuevos agujeros.

Otro problema es que habría que conseguir que la comunidad internacional llegue a acuerdos en materia de seguridad en el ciberespacio. En el caso de las bombas nucleares, en paralelo a los acuerdos START está la verificación: un sistema por el que luego los países van y comprueban cuántas cabezas nucleares tiene cada país. Como el Tratado FACE, que era una maravilla pues te permitía contabilizar cuántos carros de combate había en toda Europa. Tú declarabas una cifra de carros de combate y te venía un checoslovaco o un ruso y te decía: «Quiero ver lo que hay dentro de ese almacén». Y si la puerta tenía más de dos metros tenías que abrirle la puerta y dejar que entrara. Si tenía menos de un metro no hacía falta, porque por ahí no podía salir un carro de combate. El problema del ciberespacio es cómo verificar. Aquí vuelvo a la represalia. Como todavía no hay acuerdos

internacionales, cualquier acuerdo va a tener que estar basado en la represalia. Si se detecta que el Gobierno equis ha lanzado un ciberataque, la comunidad internacional le tiene que imponer sanciones. Eso es lo único que tenemos, porque no se puede verificar qué está haciendo cada uno en el ciberespacio.

JAVIER GARCÍA VILA
Moderador

Quería plantearos a los dos un tema que es muy importante y que entiendo daría para una conferencia muy larga, pero quiero conocer vuestra opinión. Es un tema que plantea por Zoom Ana Georgina Guerrero, quien nos dice que las medidas que adopten las administraciones públicas para asegurar la ciberseguridad en muchas ocasiones podrían colisionar con derechos fundamentales como la libertad de expresión, la intimidad, los datos, el derecho al secreto de las comunicaciones, etcétera. ¿Cómo se pueden planificar estas medidas para asegurar el equilibrio entre defensa y seguridad y derechos fundamentales?

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

El General Sanz Roldán ha dicho antes que Facebook es un Estado y es verdad que lo es. Facebook ahora va a cifrar las conversaciones y lo que le pedimos desde el mundo occidental es que dé acceso a los jueces o a la policía con un mandato judicial. Si no fuera así, estaremos como en el caso de Telegram, donde todo está cifrado. Ahí el Daesh, todos los terroristas en general, se mueven a sus anchas. Recientemente se publicó en prensa que Facebook había dado de baja cientos de miles de *bots* que se habían dedicado a darle *likes* al Ministerio de Sanidad con señoritas de buen ver para desgastar la imagen de dicho ministerio durante la pandemia, cuando más importante es que mantenga su

crédito. ¿Quién ha sido capaz de montar eso? Porque eso se hace con máquinas y exige tiempo y dinero. Facebook al final cerró todos los *bots* pero tienes que pelear con ellos para que lo cierren. Facebook tiene su negocio montado y no le interesa dar de baja cosas.

Sobre libertad de expresión y la seguridad, sabemos que ése siempre ha sido un equilibrio delicado. Hay que dar un mensaje de tranquilidad. Todos somos conscientes, y más en este foro, de que uno de los pilares en los que se sustenta la democracia es la libertad de prensa, la libertad de expresión. Dicho esto, si hay una campaña que busca, por ejemplo, que se quite todo el mundo la mascarilla, porque todo esto de la pandemia es un invento, algo habrá que hacer para intentar evitar el daño que se provocaría a la salud pública si los ciudadanos dejan de atender a los requerimientos de las autoridades sanitarias. Eso no va a atentar nunca contra la libertad de expresión. En España, cuando se ha llevado un tema ante los tribunales, normalmente el juez, ante la duda, aplica el «*in dubio pro reo*»; en este caso, «*in dubio pro* libertad de expresión». Por tanto, yo creo que en España no hay un control que implique una merma de calidad democrática o de calidad en la libertad de expresión.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Este mismo debate lo vamos a tener en este seminario dentro de tres o cuatro años como mucho. Porque, en ese progreso que no se detiene, tampoco se está deteniendo la inteligencia artificial y tampoco se están deteniendo los medios de transmisión entre ordenadores. Aquí hay algo que debemos tener muy claro cuando hablamos de la red 5G. La red 5G no es más que la forma de conectar un ordenador con otro de forma más rápida, sin latencia. Es decir, que vamos a tener una red muy rápida, de tal manera que todo va a ser prácticamente simultáneo, gracias a unas má-

quinas que van a ser capaces de entenderse y de discernir la verdad por ellas mismas. Dentro de cuatro años, con la inteligencia artificial, ya veremos cómo va a repercutir en la libertad de expresión. Porque cuando a alguien se le ocurra decir una mentira, por ejemplo que las mascarillas no sirven para nada, las propias máquinas van a saber en un tiempo infinitesimal quién lo dice y la credibilidad que tiene. Después, cuando nos lo presenten a nosotros, nos lo van a dar con una valoración, con un «aquí le mando este mensaje pero que sepa que esto es mentira». Porque, si hablamos de libertad de expresión, usted podrá decir lo que quiera, pero los instrumentos que todos tendremos comprobarán lo que es verdad y lo que no lo es y pondrán esa información en nuestras manos. Ése es el camino por el que vamos. Por eso digo que estas disquisiciones de hoy se van a quedar viejas muy pronto. Mientras tanto, siempre que regulamos algo para evitar un riesgo, decimos lo que no se puede hacer: para evitar los incendios forestales se prohíben las barbacoas. Y, en estos casos, hay que entender que la libertad de expresión es un bien fundamental y que tiene que quedar salvaguardada. Pero eso no quiere decir que no haya que regular este mundo; hasta que se regule por su propia capacidad de regularse, lo cual no va a tardar.

JAVIER GARCÍA VILA
Moderador

Quiero plantearos dos asuntos que preguntan algunos asistentes sobre la posición de España. El primer asunto lo plantean de forma muy parecida Javier Fernández Arribas, de *Atalayar*, y Alberto Suárez. España, por su posición geográfica en el flanco sur de la Unión Europea, por su cercanía con el continente africano, es un objetivo relevante para los ciberataques tanto de actores estatales, como puede ser Rusia, como no estatales, como Daesh. La pregunta es si tanto el Estado como el público en general somos conscientes de esto.

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

En lo que se refiere a la opinión pública, creo que España tiene un déficit de cultura de seguridad nacional, aunque éste cada vez sea menor. Poco a poco vamos avanzando. Precisamente ahora estamos elaborando un Plan Integral de Cultura de Seguridad Nacional que intentará aglutinar todos los planes que hay en los diferentes ministerios. Por parte del Estado, creo que sí que hay una conciencia muy clara de que somos la puerta sur de Europa, tanto de entrada como de salida, y de que tenemos que prestar especial atención al Magreb y al Sahel. Suele ocurrir que uno de los primeros viajes que hace un nuevo Gobierno es siempre a Marruecos. Pongo un ejemplo. El presidente del Gobierno, desde que estamos en pandemia y como es lógico, hace muchísimas videoconferencias y pocos viajes. Pues hace poco hizo un viaje a Mauritania, a una reunión del G5 del Sahel. Por tanto, creo que sí que hay una conciencia clara de esa importancia.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Cada vez es más baja la edad de aproximación al uso de la red y, según baja la edad, su uso es menos meditado. Es decir, si a una persona de dieciocho años le dices que se pueden estar enterando de a quién llama, te dirá que qué importa mientras le dejen llamar. Hay un ejemplo magnífico. Cuando alguien quiere descargarse una aplicación, antes tiene que aceptar los términos y condiciones. Hagamos un poco de examen de conciencia todos los que estamos aquí: ¿lo leemos o pulsamos «acepto»? Tan es así la cuestión que una empresa italiana de *software*, con cierto buen humor, hizo una aplicación de contactos y en los términos de dicha aplicación decía: «Si usted quiere bajarse esta aplicación me da a mí la capacidad de vender su alma al diablo». Du-

rante la primera hora que estuvo la aplicación en internet, 1.700 personas aceptaron que esa empresa vendiera su alma al diablo. Ésta es la aproximación del ciudadano normal a la red. El «a mí no me va a pasar nada». Y con esa aproximación es muy difícil proteger. Por tanto, sean ustedes dueños de su ordenador y dueños de su teléfono móvil. Y para ser dueños de su ordenador y teléfono móvil tienen que saber qué le ponen y en qué condiciones. Dejen de aceptar sin leer los términos y condiciones. ¿Para qué se bajan una aplicación? Utilicen su ordenador y su teléfono para lo que es. Y, cada vez que le impongan un sistema de trabajo, observen lo que es. Ésa es la mejor forma de protección. No se puede pedir al Estado que nos proteja de todo. El Estado hará todo lo pueda hacer para proteger el sistema sanitario o protegernos de grandes ataques de otro tipo pero el usuario de un sistema moderno tiene que ser capaz de protegerse y no sólo pedir que lo protejan los demás.

JAVIER GARCÍA VILA
Moderador

Hablaba antes el General Ballesteros de las represalias. Tenemos la idea de que en este ámbito de la ciberseguridad no funciona la disuasión. Ustedes son muy prudentes y no van a poner nombres pero todos tenemos la impresión de que países como Rusia o China campan a sus anchas por este ámbito y de que no le tienen ningún miedo a las consecuencias. Emilio Andreu, de Radio Nacional, pregunta si el Gobierno tiene voluntad, no conciencia sino voluntad, para responder a los ciberataques.

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

Yo no puedo hablar en nombre del Gobierno. Lo que sí tengo claro es que el Gobierno quiere proteger a los ciudadanos, pues

la primera obligación de todo gobernante es proteger a sus ciudadanos. Y esa protección incluye la ciberprotección. Cuando yo hablo de disuasión mediante la represalia, hablo de muchos tipos de represalias. Por ejemplo, está la represalia diplomática, que es la que se ejerce normalmente: si me haces algo me pongo de acuerdo con mis aliados y te sanciono, expulso a tus diplomáticos, rebajo las relaciones comerciales, etcétera. Pero éste es un tema muy complejo porque luego viene la contra-represalia, es decir, si yo tengo instrumentos que me permitan atacar al ordenador que me ha atacado, y eso sólo se puede hacer en el ámbito de la ciberdefensa. Los ejércitos tienen armas puras de defensa y tienen armas de ataque que sólo se conciben para la represalia como pieza fundamental de la disuasión. No son para atacar a nadie sino para mandar el mensaje de que no deben ser atacarnos. Todos los gobiernos han dado por buenas las estrategias de defensa y, si son válidas en lo convencional, por qué no van a serlo en otros campos. Pero siempre como respuesta a un ataque, nunca para llevar la iniciativa.

JAVIER GARCÍA VILA
Moderador

El último tema que os quería plantear a los dos es el despliegue del 5G. Lo que quiero preguntaros es si en España se está haciendo el despliegue de esta tecnología de última generación en condiciones de seguridad o si deberíamos preocuparnos.

GENERAL FÉLIX SANZ ROLDÁN
JEMAD entre 2004 y 2008 y director del CNI entre 2009 y 2019

Yo no estoy en el despliegue, como todo el mundo puede imaginar, pero estoy seguro de que se está desplegando con las máximas condiciones de seguridad posibles. De eso no tengo ni la menor duda. El 5G es una tecnología muy nueva, muy bien di-

señada y se está desplegando de la forma más segura posible a día de hoy. De eso no me cabe la menor duda.

GENERAL MIGUEL ÁNGEL BALLESTEROS
Director del Departamento de Seguridad Nacional

España es el país con más fibra de Europa y el tercero del mundo. Eso se debe a que somos un país que vive en ciudades, en vertical, lo que por cierto es bastante negativo para las pandemias, pero para la fibra viene fenomenal. Eso nos da una enorme ventaja competitiva en la implantación de todo lo que es comercio electrónico y perder esa ventaja competitiva sería un error. No podemos parar el progreso. No podemos parar esto durante tres o cinco años y ver qué ocurre luego. No se puede hacer eso. De ahí que las operadoras ya estén empezando a ponerse en marcha. De hecho, como la mayor parte de los países europeos, España está pendiente de decidir su posición respecto a la seguridad en el tema 5G. El Reino Unido tomó su decisión en enero y la acaba de cambiar, teóricamente por lo que está ocurriendo en Hong Kong. Ahora el Reino Unido acaba de decir que no se admiten equipos de China y que en 2027 esto tiene que estar limpio. España tiene que encontrar un equilibrio, siguiendo las instrucciones de la Unión Europea, entre desarrollo tecnológico y económico, donde tenemos una ventaja competitiva. Eso sí, siempre garantizando la seguridad de las redes que deben tener esa seguridad. Es un tema en el que se está trabajando ya desde hace tiempo. Lo que nos gustaría es que Europa, en vez de dar recomendaciones, hubiera adoptado una posición común, como hizo con la NIS, con la Iniciativa de la Protección de la Red. Pero no ha sido así. Hay que tomar decisiones que están pendientes y habrá que adoptarlas en un tiempo breve. Y será, seguramente, el fruto de ese equilibrio entre el desarrollo tecnológico, el desarrollo económico y lo demás, y sobre todo con la necesaria seguridad para los ciudadanos y los Estados.

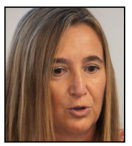
JAVIER GARCÍA VILA
Moderador

Con esto terminamos. Ha sido un placer escucharos y por ello os doy las gracias.

5. ¿QUIÉN PROMUEVE LOS ATAQUES CIBERNÉTICOS?

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto
del Ciberespacio (MCCE)

ROSA DÍAZ
Directora general del Instituto
Nacional de Ciberseguridad (INCIBE)



LUIS JIMÉNEZ
Subdirector general del
Centro Criptológico Nacional (CCN-CERT)

Moderador
ÁNGEL GONZALO
Jefe de Internacional de Onda Cero

Rosa Díaz, el General Rafael García Hernández, Ángel Gonzalo y Luis Jiménez

La mayoría de las amenazas cibernéticas a las democracias están patrocinadas por grupos terroristas o actores estatales interesados en desestabilizar a sus adversarios. El objetivo de la amenaza puede estar enfocado en las infraestructuras críticas, en la alteración de los resultados electorales o en su percepción, de modo que la niebla consiga dejar a los votantes en la incertidumbre. Los ataques pueden ser encubiertos o servirse de la difusión de mensajes claros y directos que calen en el voto de los electores. ¿Cuáles son las ciberamenzas más peligrosas? ¿Quiénes están interesados en generar esa desestabilización? ¿Quiénes patrocinan los ataques en el ciberespacio?

ÁNGEL GONZALO
Moderador

Hemos escuchado algunas cosas realmente interesantes desde que ha comenzado este seminario. Me estaba fijando en la introducción al asunto que abordamos en esta sesión: «¿Quién promueve los ataques cibernéticos?». Se nos plantean una serie de cuestiones muy interesantes, como los efectos de los ciberataques en la alteración de resultados electorales o las dudas que pueden sembrar en el electorado. Otra cosa que me parece muy importante son las amenazas enfocadas a las infraestructuras críticas. Todos sabemos que Microsoft ya alertó en su momento sobre organizaciones como Strontium, que desde Rusia, supuestamente, ha intentado interferir en procesos electorales y ha participado en ataques a multinacionales, en espionaje comercial, etcétera. Me voy a permitir citar una novela que nunca será un clásico en los anaqueles de la historia ni será estudiada en literatura, pero que me pareció muy curiosa. En el año 2018, la editorial Planeta publicó un libro titulado *El presidente ha desaparecido*, de Bill Clinton y James Patterson, donde se plantean una serie de hipótesis muy interesantes. Por un lado, que el ciberespacio, como hemos venido escuchando a lo largo de este seminario, es un nuevo esce-

nario de confrontación. Como consecuencia de un ciberataque a las tecnologías que usamos en nuestra vida cotidiana podemos vernos privados de realizar transacciones económicas, de realizar viajes, de hacer gestiones en la administración, incluso de tener medicinas en los hospitales. El libro explica que lo que ocurriría en un caso extremo es que retornaríamos a una especie de Edad Media debido al cambio en los usos y en las costumbres de nuestra vida cotidiana. Otra amenaza que me parece interesante –que se cuenta en el libro de manera muy gráfica– es el ataque a las infraestructuras críticas. Hay un momento en el que el jefe de un comando ciberterrorista le dice al presidente que ya no se trata de estrellar aviones en torres, pues desde donde están les basta un ordenador para interrumpir el abastecimiento de agua potable a la ciudad de Los Ángeles.

En primer lugar, voy a dar la palabra al General de División Rafael García Hernández, que es el Comandante del Mando Conjunto del Ciberespacio.

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

Quisiera empezar dando las gracias a la organización por esa capacidad, que nosotros llamamos de resiliencia, que consiste en sobreponerse a la adversidad, en este caso a la adversidad de la COVID, pues aunque todo estaba programado para celebrar este seminario de forma presencial en Toledo, al final lo estamos haciendo de otra forma distinta gracias a la capacidad de la Asociación de Periodistas Europeos de hacer frente a esa adversidad. Y, por supuesto, gracias a todos los que están tanto aquí presentes como a los que nos siguen *online*.

Traía preparadas cuatro ideas, pero la mayor parte han sido ya expuestas por los ponentes anteriores, por lo que he tenido que reinventarme sobre la marcha. Expondré algunas ideas y, sobre las que ya han sido tratadas, simplemente daré una pincelada.

La introducción de Ángel me ha hecho pensar en la ciencia ficción. Ahora mismo estoy viendo la serie *Homeland* y, entre otras cosas, en uno de los capítulos matan al vicepresidente del Gobierno con un ordenador, porque tenía un chip implantado en el marcapasos que gracias a esa tecnología hacen explotar. Éste es un cibercrimen que, aunque ocurra en una serie de televisión, nos puede dar una idea de en qué mundo nos movemos.

Centrándome en el tema, quería contarles una visita que hicimos al departamento de ciberseguridad de uno de los bancos más importantes de este país. El departamento tenía tres secciones: una sección de defensa, una sección de inteligencia y una sección de respuesta, que es exactamente la misma composición que tenemos en el Mando del Ciberespacio. Tenemos un grupo de defensa, un grupo de inteligencia y un grupo de respuesta, exactamente igual que el banco. Es más, ellos tenían bastante más gente que nosotros, porque los activos que le pueden quitar a ellos son contabilizables en euros y la información que nos pueden quitar a la administración del Estado, aunque sea igual de importante, resulta más difíciles de contabilizar en euros. El hecho de que estuvieran organizados exactamente igual que nosotros me llamó mucho la atención pues demuestra que están, como mínimo, igual de concienciados de lo que deberíamos estarlo en la Administración General del Estado.

Entrando en el tema de quién promueve los ataques cibernéticos, la respuesta es muy simple: los malos. ¿Quiénes son los malos? Aquí se han mencionado tanto a los grupos nacionales, que pueden estar o no asociados a una nación en concreto, como a los terroristas, como el Daesh, que usan el ciberespacio para difundir propaganda y radicalizar a sus simpatizantes. También están los *hackers* patrióticos, que actúan de forma personal pero en nombre de un Estado, y los *insiders*, que quieren hacer daño, sea por venganza o por motivos económicos. No vamos a engañarnos: en este mundo, sea a través del ciberespacio o de otro modo, casi siempre hay un trasfondo económico.

Las revistas especializadas ya le han puesto nombres a estos malos. La 39 sospecha que proviene de Irán; la 41 que proviene de China; la 38 de Corea del Norte; la 32 de Vietnam; y la famosa 28, que es la que conocemos como Strontium; todas opiniones de revistas especializadas, no mías. Estas amenazas persistentes son, posiblemente, grupos muy especializados –mucho más especializados de lo que nos gustaría que estuvieran– que, con el apoyo o no de una nación, son los que más daño nos hacen a todos; no sólo a los Estados, a la Administración General del Estado, sino también a las empresas y a las infraestructuras críticas. Los Estados reaccionan de varias formas a estos ataques, a estas amenazas persistentes, ya que no es lo mismo un activista que entra por sí solo en tu ordenador y lo secuestra que secuestrar el ordenador de la red eléctrica del Estado. Hay Estados, como Reino Unido, Estados Unidos y Canadá, que acusan directamente a Rusia de intentar robar datos de la vacuna contra el coronavirus y otros países que no hacen una atribución política porque no tienen los suficientes datos como para llevarlos a un juez, que en cualquier caso no existe pues ese marco legal está todavía por desarrollar. Aún no hay un juzgado internacional que sea competente para juzgar a ese grupo de rusos que han atacado a ese grupo de empresas en Estados Unidos. No existe el marco legal para hacer esa atribución. Pero, por ejemplo, Australia sí ha acusado a China como sospechoso de atacar empresas australianas, porque tiene los suficientes indicios como para hacer una atribución política. Repito, como no hay un juez, aunque tuvieran pruebas no podrían llevarlas a un juzgado e interponer la denuncia. La no existencia de ese marco legal supone un serio problema. De hecho, incluso organizaciones supranacionales como la Unión Europea, que intentan de alguna forma regular este marco, se encuentran con la dificultad de no poder identificar claramente el origen del ciberataque. En palabras de la propia UE: «Internet es el salvaje oeste, muy fácil de atacar y muy difícil de defender». Por eso, a pesar de que se intenta establecer un mecanismo para coordinar esa atribución, al final la Unión Europea termina diciendo que se trata de una decisión soberana, de una decisión de cada uno de los países miembros. La UE no tiene competencia para atribuir a un país en concreto un ciberataque y por eso lo deja en manos de los Estados miembros. En la UE pueden coordinar a nivel europeo determinados mecanismos, como la Directiva NIS, pero, en lo que se refiere a la atribución, ésta depende de cada país. El Reino Unido, por ejemplo, se reserva, textualmente, «el derecho a responder a un ciberataque en cualquier forma». Es decir, un ciberataque para ellos es un ataque a su soberanía. Pueden responder a él con otro ciberataque o con cualquier otra acción, que no tiene por qué ser una acción militar. A mí, particularmente, me encanta la posición de la ministra de Defensa de Francia, que cuando presentó la estrategia de ciberdefensa de las Fuerzas Armadas francesas dijo: «Hoy nos dotamos de un marco legal y asumimos ese marco legal. Francia emplea y empleará armas cíber en sus operaciones militares». Esto, que ocurrió el 18 de enero de 2019, nos hace ver que hay países –y aquí estamos hablando de disuasión– que no sólo tienen la intención de usar herramientas cíber sino que lo dicen públicamente. Los ponentes anteriores han comentado que la disuasión en el ámbito nuclear ha funcionado, al menos hasta ahora, y que quizá debiéramos emplear ese mismo tipo de mecanismo en el ámbito cíber, pero me temo que, ahora, como mucho estamos en paridad en ese ámbito con los países que hacen de malos. Si no tenemos una capacidad de respuesta, jamás podremos alcanzar la supremacía en el ámbito cíber; algo que ya se ha mencionado varias veces esta mañana. Esa capacidad de respuesta debe ser inherente al ámbito cíber porque, si no, siempre estaremos como mucho al mismo nivel y no tendremos la posibilidad de ejercer la disuasión. Aquí he de decir que, en la orden ministerial de creación del Mando Conjunto de Ciberdefensa, éste figura como autorizado para ejercer esa respuesta, aunque dentro de unos límites: que sea legítima, proporcionada y opor-

tuna. Así pues, tenemos una capacidad de respuesta que debería de llegar a poder alcanzar ese poder de disuasión, de forma que si tú me atacas yo te puedo atacar y, como mínimo, hacerte el mismo daño que me has hecho tú, que es el mismo caso que en la disuasión nuclear. Curiosamente, y hablando de nuevo de Francia, ayer vi la noticia de que han realizado un ejercicio aéreo con cincuenta aviones, de los cuales unos cuantos eran nucleares. Es decir, que repiten esa disuasión nuclear para decirle al resto de los países que no van a atacar, porque hasta ahora todos hemos compartido el *statu quo* en el ámbito nuclear, pero que quede claro que siguen teniendo la misma capacidad y que no porque no la ejerzan dejan de tenerla. Y nos hacen un ejercicio aéreo para demostrarlo.

Antes de concluir, quisiera compartir una idea que algún pensador aquí presente ha publicado recientemente haciendo una equiparación que resulta muy acertada. Hasta ahora, en el ámbito marítimo las fuerzas navales, las Standing Naval Forces de la OTAN, han funcionado. No ha habido ningún combate, ni con las fuerzas rusas ni con otras. De hecho, siguen funcionando pues, aunque la OTAN sea una organización defensiva, también ha ejercido de alguna forma esa capacidad de disuasión en el ámbito nuclear. Así que no veo descabellado ejercer esa disuasión también en el ámbito cíber. En prensa hemos leído que la OTAN ha sufrido varios ataques cíber en sus redes pero que, como organización defensiva que es, no tiene capacidad de disuasión o de respuesta. Pero esa capacidad de disuasión sí la ha tenido con las fuerzas navales y con las fuerzas nucleares.

Dejo aquí la idea –que repito no es mía sino de alguien que está aquí presente– de si la OTAN debería tener capacidad de respuesta en el ámbito cíber y si esa capacidad de respuesta no equilibraría un poco la balanza, como se equilibró en el ámbito nuclear. Poco más quería decir. Creo que, más que escuchar mis palabras, será interesante entrar en debate con las preguntas que ustedes hagan

ÁNGEL GONZALO
Moderador

Gracias, General. A continuación intervendrá Rosa Díaz, la directora general del Instituto Nacional de Ciberseguridad, el INCIBE.

ROSA DÍAZ
Directora general de INCIBE

Gracias, Ángel. Buenos días a todos y muchas gracias a la Asociación por la invitación. Lo cierto es que INCIBE no se dedica a la atribución. Nosotros estamos enfocados a la ayuda a las víctimas, sean pymes, empresas o ciudadanos.

Empezaré explicando quiénes somos para aquellos que no nos conozcáis. Somos una empresa pública adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial, que está dentro del Ministerio de Asuntos Económicos y Digitalización. Tras el Real Decreto Ley de transposición de la Directiva 12/2018, nos hemos convertido en entidad y CERT de referencia para ciudadanos y para empresas privadas; además de encargarnos de toda la parte de infraestructuras críticas privadas.

Uno de nuestros pilares y objetivos fundamentales es el fomento de la confianza digital de la que tanto se ha hablado en las mesas anteriores, de esa necesidad de extender la cultura digital siendo conscientes a la vez de su problemática y sus peligros y, por supuesto, también de las oportunidades que nos plantea el ciberespacio. También trabajamos en el impulso del sector de la industria y la innovación, tan importantes en estos momentos de pandemia. En la situación en la que nos encontramos, la ciberseguridad es un sector en crecimiento, un sector que en los próximos años puede traer mucha riqueza a nuestro país. Uno de nuestros objetivos es precisamente ése y, por supuesto, también detectar el talento y promocionarlo. Se dice muchas veces que

este es un sector que se conoce poco y, dentro de ese poco conocimiento, es muy importante que traslademos a la opinión pública, a nuestros hijos y amigos, las posibilidades de empleabilidad que tiene el sector de la ciberseguridad. Actualmente no solamente se precisan carreras STEM sino también perfiles tanto técnicos como sociológicos y de derecho que puedan ayudar a esa parte técnica a luchar contra la ciberdelincuencia. Desde aquí yo os animo a que entréis en este maravilloso mundo que está lleno de oportunidades, al igual que también de mucha problemática. Se ha hablado de la transformación digital, una transformación que esta pandemia está acelerando y que pone de manifiesto la piedra angular de la ciberseguridad. Yo creo que la apuesta de todos los que estamos aquí es clara: la ciberseguridad debe ser un pilar en las estrategias de las compañías. Y creo que estamos avanzando mucho en España a este respecto. Se ha hablado aquí de la Agenda Digital del Gobierno para los próximos cuatro años, del Plan Digital 2025. De los diez ejes estratégicos que tiene esta estrategia uno es la ciberseguridad, lo cual ya denota cómo estamos dando pasos para situar la ciberseguridad en el centro.

Aunque no puedo decir mucho sobre los enemigos concretos a los que nos enfrentamos, si puedo hablar de esa parte de CERT que tenemos, de los incidentes que ayudamos a solucionar. Ahí hay muchos intereses políticos, sí, pero también hay mucho dinero. España es un país de pymes: el 98% del tejido empresarial de España son pymes, micropymes o autónomos. Así que, cuando se lanza un ataque de *ransomware*, lo que se busca es la cantidad. Es decir, tú lanzas el ataque, lanzas un correo electrónico malicioso y, con que pique un 0.001%, ya estamos hablando de miles de compañías, que en muchos casos se ven obligadas a cerrar porque no pueden hacer frente al ataque al no tener una copia de seguridad. Ni tan siquiera pueden volver a poner sus sistemas en funcionamiento tras ese *ransomware* y la petición de rescate en *bitcoins*. Las motivaciones de los ciberataques son múltiples pero la económica es una de las más importantes. Aunque

algunos ciberdelincuentes parece que se han especializado en determinado tipo de cíber, los ciberataques que se lanzan a la ciudadanía y a las empresas son los mismos de siempre: *malware*, *phishing*, *business email compromise*, intrusiones…

Es muy importante la cultura de ciberseguridad, que el usuario sepa que el peligro existe y es muy grande. Quisiera daros unos datos de los incidentes que gestionó nuestro CERT el año pasado. De un total de 107.000 incidentes gestionados, más de 72.000 fueron de empresas y ciudadanos, mientras que los operadores estratégicos y las infraestructuras críticas no llegaron a 800 ataques. Por otra parte, en el caso de la red IRIS, de la red académica, son más de 30.000. Y, si hablamos de los incidentes por categorías, el top tres, que ocupa casi el 90% de todos los incidentes, son el fraude, los sistemas vulnerables y el *malware*. A fecha de agosto de 2020 tenemos 79.000 incidentes, de los cuales 63.000 son contra ciudadanos y empresas y más de 750 contra operadores críticos, lo que nos indica que este año vamos a tener más incidentes de este tipo. Unos 15.000 son ataques a la red IRIS, con las mismas tipologías que el año pasado.

Ahora les voy a dar unos datos sobre la pandemia. Si echamos la vista atrás, desde primeros de marzo, cuando empezamos a hacer un seguimiento de la situación con la COVID, de los 40.000 incidentes que hemos registrado solamente un 1% tiene que ver con la COVID. En total, unos 350 incidentes, que son muy pocos. No es que esté habiendo más incidentes sino que los ciberdelincuentes aprovecharon ese momento de no tener información, de estar ávidos de saber, de buscar información en internet, de teletrabajar, de las clases *online* para hacer estafas, para vender productos falsos, dominios fraudulentos, etcétera. Son incidentes cada vez más mediáticos, pero no hay un aumento exponencial de los mismos. Un ejemplo de suplantación de una marca es el caso de Sanytol, en el que un enlace te dice que metas tus datos para que te envíen unas muestras gratuitas. Antes hablaba el General Sanz Roldan de que 1.200 personas cedieron

su alma a una empresa. Pues bien, en este caso, lo hicieron por una muestra gratuita. Que la gente ponga sus datos en un enlace es el petróleo de este siglo, pues con esos datos se accede a más información que permite realizar nuevos ataques.

Otro problemática ha sido la extorsión. Recibes mensajes de que tienen un vídeo sexual tuyo y si no pagas un rescate van a mandar ese vídeo a tus conocidos. Lo que hacen los ciberdelincuentes es conseguir una clave, que ha sido vulnerada en algún momento de tu vida, que tu recuerdas haber utilizado en alguna ocasión. Por eso debemos utilizar gestores de contraseñas para no tener esa problemática, para que no puedan adivinar nuestras claves. Te dicen que tienen una de tus claves, te dicen que tienen ese vídeo y te extorsionan para que pagues un rescate. Aunque tú sepas que nadie te ha podido grabar un vídeo, te dejan con la duda y hacen todo lo posible para que les pagues. Este caso de extorsión lo hemos visto con mucha asiduidad durante la pandemia; además hemos recibido muchas llamadas al respecto.

Respecto al *phishing*, pongo el ejemplo de la Agencia Tributaria, pero seguro que habéis oído también el del SEPE, pues hay una infinidad de *phishing*. Tú te crees que recibes un correo electrónico de la Agencia Tributaria en el que te dicen que tienes equis días para descargar, imprimir y enviar firmado un documento. Como intentan darle la mayor credibilidad a todo este proceso, también te piden que rellenes un formulario y, en algunos casos, incluso tu cuenta bancaria. Y eso es precisamente lo que no debemos hacer. Es de sentido común pero muchas veces el sentido común es el menos común de todos los sentidos. Otro ejemplo, en este caso relativo a ayudas económicas. Te dicen que el Estado te destina una ayuda de entre 350 y 700 euros y que, para recibirlos, debes rellenar los datos de un formulario, donde por supuesto te piden los datos de tu tarjeta. Entonces la gente pica, se inscribe y ya no hay forma de buscar a ese ciberdelincuente.

En una campaña sobre cíber-COVID que pusimos en marcha junto a otras organizaciones que también están en este seminario, teníamos tres temáticas que trasladar a empresas y a la ciudadanía: consejos y ayuda sobre cómo teletrabajar más seguro, cómo entretenernos con nuestros hijos mientras estábamos todos confinados y, a nivel de privacidad, cómo conseguir preservar la seguridad de las personas. Esa campaña la podéis encontrar en nuestra página web. Por supuesto, la tecnología también ayuda. Desde nuestra secretaría y desde el Gobierno se ha lanzado una aplicación, Radar COVID, que se está poniendo en marcha en todas las comunidades autónomas. Lo que queremos reflejar con esta aplicación es cómo la tecnología también ayuda en un momento de pandemia, de manera colaborativa y anónima, a que estemos más seguros en nuestras interacciones habituales cuando estamos fuera de casa, sin perseguir la recogida de datos. Para su información, tenemos un teléfono, el 017, que es una línea de ayuda confidencial y gratuita disponible los 365 días del año de 9 de la mañana a 9 de la noche.

Para finalizar, hemos hablado de que el ser humano es el eslabón más débil de la cadena. Es sobre el ser humano sobre el que debemos poner el foco. Es necesario concienciarle porque, por mucho que tengamos un sistema robusto y pongamos todas las medidas de seguridad que hay a nuestro alcance, el 95% de los problemas relacionados con la ciberseguridad son resultado de la acción u omisión de las personas. Según un estudio del National Cyber Security Center del Reino Unido, 23 millones de cuentas fueron vulneradas por usar la misma contraseña: 123456. Es un dato de 2018 pero os aseguro que cuando salgan los datos de 2020 volverá a pasar lo mismo. Nosotros somos la fortaleza más importante para luchar contra la ciberdelincuencia.

ÁNGEL GONZALO
Moderador

Gracias, directora. Por último intervendrá Luis Jiménez, subdirector general del Centro Criptológico Nacional.

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

Antes de nada, quiero agradecer la invitación que se me ha cursado para participar en esta mesa con compañeros que estamos en el día a día trabajando en la ciberseguridad de este país. Voy a intentar responder a la pregunta de quién nos ataca, aunque no voy a dar nombres. Simplemente, voy a explicarles qué es o cómo se realiza un ciberataque y, al contarles yo como se realiza un ciberataque, piensen ustedes quién puede tener la capacidad de hacerlo. Nosotros, cuando estudiamos los ciberataques, analizamos los incidentes según un modelo, que está siendo utilizado por muchísimos países, por el que se distinguen cuatro elementos fundamentales. No es posible realizar un ciberataque si no existe el primer elemento de este modelo, que es una vulnerabilidad. Para que un sistema informático o un sistema de comunicaciones pueda ser ciberatacado debe tener una vulnerabilidad; si no es imposible realizar un ciberataque. ¿Es suficiente con que tenga una vulnerabilidad? No. Hace falta un segundo elemento, que es que alguien sea capaz de hacer un programa que explote esa vulnerabilidad. ¿Es suficiente con que haya una vulnerabilidad y un programa que explote esa vulnerabilidad? No. Hace falta un tercer elemento, que es ser capaces de colocar ese programa, ese *exploit*, dentro del sistema para que pueda explotar esa vulnerabilidad. Eso es lo que nosotros denominamos el vector de ataque, la manera en que se puedes introducir el *exploit* dentro de ese sistema. Y, por último, el cuarto elemento que hace falta para que un ciberataque tenga éxito es tener una infraestructura que me permita explotar el ataque, fundamentalmente para conseguir dos cosas: que la explotación del ataque sea eficiente, es decir, que pueda o manipular el sistema o destruirlo o sacarle la información de una manera eficaz; y, en segundo lugar, romper la posibilidad de investigación o la posibilidad de atribución del ataque. Estos cuatro elementos, la vulnerabilidad,

el *exploit*, el vector de ataque y la infraestructura de explotación, son lo que nosotros analizamos cada vez que nos enfrentamos a un ciberataque. Ahora podemos hablar largo y tendido sobre cada uno de estos elementos.

El primer elemento, como decía, es la vulnerabilidad. Todos los sistemas, hoy en día, salen al mercado con vulnerabilidades. Como sociedad de la información, tenemos un talón de Aquiles en relación a las vulnerabilidades con las que salen al mercado las tecnologías. Ahora mismo, un montón de gente en el Centro Criptológico Nacional, un montón de gente de la administración pública, están parcheando los sistemas Windows por una vulnerabilidad que ha sido publicada recientemente. Se llama Zerologon y es una vulnerabilidad muy grave pues en una escala de cero a diez está clasificada con el diez. El Zerologon está afectando a muchísimos ordenadores de las administraciones públicas y de empresas. Como decía, es una vulnerabilidad muy grave embebida en un protocolo de comunicaciones de los sistemas operativos de Microsoft. Ha sido descubierta por Microsoft, en lo que es otro aspecto importante de las vulnerabilidades. Existen las vulnerabilidades que son conocidas y aquellas que no son conocidas. Las que son conocidas, gracias a Dios, se conocen porque el mundo de la investigación en ciberseguridad trabaja a destajo para levantar y hacer sistemas cada vez más seguros, cada vez menos vulnerables, y en cuanto se conoce una vulnerabilidad se publica para que inmediatamente se pueda parchear y, consiguientemente, resolver. Pero también hay un montón de vulnerabilidades que no se conocen y que están ahí. Es un gran problema, porque son vulnerabilidades que muchas veces no están siendo explotadas porque están en un estado latente, pero pasarán a ser explotadas en el momento que sea necesario. Y esto lo enlazo con lo que decía antes nuestro moderador de los ataques a las infraestructuras críticas. Hoy en día, el peligro de las infraestructuras críticas es conocer exactamente qué vulnerabilidades latentes y explotables tienen que hoy por hoy no sabemos

si podrían ser activadas en caso de conflicto o de crisis. Tenemos mucho que trabajar en el ámbito de las vulnerabilidades, en el ámbito de que la tecnología salga al mercado sin vulnerabilidades o, por lo menos, con sistemas o con arquitecturas de seguridad que permitan detectar las vulnerabilidades y contrarrestarlas lo antes posible.

El segundo elemento que he mencionado es el *exploit*, la capacidad de hacer programas que exploten las vulnerabilidades. Los *exploits* pueden ser muy sencillos. Por ejemplo, el famoso *WannaCry*, el programa que hacía uso de la vulnerabilidad del sistema de compartición de ficheros de impresoras era muy sencillo de realizar. Lo podía hacer prácticamente cualquier estudiante de ingeniería informática. Sin embargo, hay otros *exploits* que requieren desarrollos de ingeniería de años. O sea, hay una capacidad de I+D en relación con el desarrollo de *malware*, con el desarrollo de programas que explotan vulnerabilidades. Lo que hay detrás de estos programas no son grupos de aficionados. Ni siquiera son grupos de expertos. Son auténticos grupos de investigación y desarrollo en el ámbito de los ciberataques patrocinados por Estados, si es que no son directamente agencias de Estados. Los *exploits*, como digo, pueden ser muy sencillos o muy complicados. Para hacerlos, para hacer programas maliciosos que exploten las vulnerabilidades, se debe conocer muy bien el funcionamiento de las tecnologías, el funcionamiento del *core*, del corazón de cada sistema informático o de cada sistema de comunicaciones. Ese conocimiento no existe o, al menos, no de forma generalizada. Como sociedad, tenemos una gran carencia –España en concreto y Europa en general– de expertos que tengan un profundo conocimiento del funcionamiento de las tecnologías de la información. Los sistemas cada vez son más complejos y cada vez es más difícil saber determinar la seguridad de un sistema. Ese *expertise* es algo necesario, pero nosotros tenemos poca gente preparada. De hecho, hay muchos incidentes en cuya investigación ha participado el CCN donde nos falta el *man-*

power, la fuerza humana, pues no tenemos expertos suficientes para corregir, para desinfectar los equipos o para repararlos. Y cuando acudimos a empresas para que nos ayuden tampoco encontramos equipos de expertos que puedan entender bien el problema, lo que está ocurriendo en el sistema, de forma que puedan parchear o contener la infección. Existen equipos, como los del Mando Conjunto del Ciberespacio, los de INCIBE, los de las grandes empresas y algunos equipos en las universidades, pero no existe una masa crítica suficiente de expertos como para hacer frente al análisis de las vulnerabilidades, al parcheo o a contrarrestar los *exploits* que hacen uso de esas vulnerabilidades.

En referencia al vector de ataque, aquí entra fundamentalmente el factor humano. Antes nos contaba Rosa que si tenemos un sistema cuya contraseña es 123456 facilitamos mucho la entrada al atacante, permitiéndole depositar en ese sistema un *exploit* que haga uso de la vulnerabilidad. Ha habido mucha labor de concienciación en España y en Europa al respecto. Los medios de comunicación cada vez hablan más de los ciberataques y de la ciberseguridad. Hoy en día, si preguntas por la calle, cualquier persona sabría contarte alguna anécdota de algún ciberataque o de algo que le ha ocurrido en un sistema informático. Existe sin duda cierto nivel de concienciación, pero ni mucho menos suficiente. Hay mucho trabajo por hacer.

En relación con el vector de ataque, es muy importante configurar los sistemas de una manera segura para evitar la posibilidad de que el atacante coloque su programa, su *exploit*, en nuestro sistema. Aquí entramos en algo que hacemos mucho en el Centro Criptológico Nacional, que es emitir guías de configuración segura para los diferentes dispositivos de las diferentes tecnologías. Nosotros, como ciudadanos y como usuarios de tecnología, tenemos en nuestros teléfonos alrededor de cuarenta parámetros que configuran la seguridad del dispositivo. Nadie los toca y muy poca gente sabe que puede perfectamente utilizar su dispositivo en mejores condiciones de seguridad que cuando lo

saca de la caja recién comprado. Ahí también hace falta trabajar mucho para que configuremos la tecnología de manera que sea segura y evitemos así ese vector de ataque que aprovecha una vulnerabilidad de nuestro sistema.

Por último, la infraestructura de explotación fundamentalmente la utilizan los atacantes para romper la atribución, para dificultar la investigación, para que no podamos saber de dónde vienen los tiros. Aquí hay un ámbito que todavía tenemos que trabajar como sociedad, que es la actualización o modernización de nuestras leyes, de manera que nos permitan atribuir los ciberataques. Y que nos permitan investigar, porque hoy en día técnicamente es muy difícil investigar los ciberataques desde el punto de vista de la atribución y lo tenemos que complementar con una serie de medidas que no son fáciles de aplicar. El motivo es que la naturaleza de la red es así. Es decir, internet se creó para preservar el anonimato. Hoy en día, lo que se busca cuando se desarrollan grandes sistemas de comunicaciones, grandes sistemas de información, es que sean de fácil uso, que sean eficaces, que sean eficientes y abiertos, que no tengan puertas y que estén lo más conectados al mundo que sea posible. Esa capacidad de anonimato, esa capacidad de conectarse a cualquier lugar del mundo desde cualquier lugar del mundo utilizando múltiples protocolos que puede ser anonimizados, permite que los atacantes monten infraestructuras de explotación que son muy difíciles de investigar para determinar quién está detrás de dichos ataques. Nuestro Código Penal y nuestra Ley de Enjuiciamiento Criminal nos dan un montón de herramientas para hacer investigaciones, pero eso no es suficiente. Hay que modificar algunas reglas técnicas del funcionamiento de los sistemas de internet para poder garantizar las investigaciones y que éstas puedan llegar a buen puerto. Yo hago siempre el símil de la circulación vial. Si tuviésemos una infraestructura de carreteras maravillosa, llena de autopistas y autovías, de rotondas y de semáforos, pero no existieran normas de circulación, todo sería un desastre; circular

por la carretera no sólo sería incómodo, sino incluso peligroso. Por eso nos hemos dotado de una serie de normas que regulan la circulación por las vías públicas, que incluyen, por ejemplo, que no puede circular ningún vehículo que no tenga su matrícula correspondiente. Entonces, ¿todos los sistemas que se conecten a internet deberían estar matriculados, de tal forma que supiéramos perfectamente a quién pertenecen? A lo mejor ése es el futuro si queremos seguir disfrutando de todos los beneficios que tiene internet, que tiene la conectividad.

Hoy en día, las infraestructuras de comunicaciones permiten la atribución; no sólo a nivel político o a nivel legal, sino a nivel técnico. De alguna manera, deberíamos tocar los estándares, tocar las normas técnicas, para poner un poco de orden, señales, semáforos, matrículas, en los protocolos de comunicaciones, en el *software*. Así tendríamos unas reglas del juego con las que todos nos encontrásemos cómodos y en las que se pudiese evolucionar en esta sociedad de la información, en este IoT, o «internet de las cosas», al que nos dirigimos. Muchas gracias.

ÁNGEL GONZALO
Moderador

Muchas gracias, Luis. Vamos a apurar el tiempo que nos queda con preguntas de las personas que están siguiendo en la distancia esta mesa redonda. Por ejemplo, Alfredo Sanz nos pregunta sobre la disuasión activa frente a los ciberataques. Nos dice que la postura de la OTAN es la misma que en cualquier otra área, incluida la nuclear, y que, aunque como organización defensiva no cuenta con medios de ataque, sus miembros sí los tienen. Como en todo club de buenos amigos, si el club es atacado, los miembros responden individual o colectivamente. En esta línea, algunos países de la OTAN disponen de medios de ciberataque que se han utilizado en caso necesario. ¿España podría disponer de medios de ciberataque? ¿Sería conveniente que los utilizara?

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

España, en la organización del Mando Conjunto de Ciberdefensa, ahora del Ciberespacio, tiene tres grupos: defensa, inteligencia y respuesta. Y, si tiene un grupo de respuesta es porque tiene medios para poder responder a un ataque.

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

No olvidemos que para tener capacidad de ofensiva, para tener capacidad de ciberataque, lo que tienes que conocer son las vulnerabilidades del adversario. Y para eso hay toda una labor de inteligencia que hay que realizar antes de tener esa capacidad.

ÁNGEL GONZALO
Moderador

Si me permitís, quisiera haceros una pregunta a cada uno. Para el General, utilizando términos de la antigua Guerra Fría, ¿podríamos hablar de ciberdestrucción mutua asegurada? Rosa, igual que existieron en su momento fichajes de expertos en defensa nuclear, biológica o química, ¿fichan las organizaciones criminales ahora cerebros para operar en la red utilizando *malware*? Y para Luis, respecto a la capacidad de colocar un *exploit*, ¿de qué grado de traición, es decir, de tener el enemigo en casa, estamos hablando?

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

Todavía no ha caído en mis manos ninguna novela sobre la destrucción mutua asegurada en el campo cíber pero, después de esa

anécdota que he contado sobre la serie *Homeland*, si lo trasladamos a que nos puedan envenenar el agua o dejar media España sin luz o que se caiga la red de la Seguridad Social, o todo simultáneamente, no sé si sería una ciberdestrucción mutua asegurada pero se parecería bastante.

ROSA DÍAZ
Directora general de INCIBE

Sobre el fichaje de malos, de lo que estamos hablando realmente es de estructuras criminales profesionalizadas. Por supuesto que fichan a cerebros. Como se ha dicho aquí, existe una necesidad de talento y estas organizaciones tienen mucho dinero. Hay mucho beneficio económico posible así que claro que fichan y pagan muy bien.

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

Entre los vectores que se utilizan para colocar el *exploit*, por supuesto está el *insider*, el empleado interno que puede facilitar mucho las cosas a la organización madre.

ÁNGEL GONZALO
Moderador

Tenemos una pregunta de Enrique Cubero, que nos dice que la inteligencia artificial está penetrando cada vez más sectores de actividad y que un sector en el que parece tener más posibilidades de aplicación es la ciberseguridad. Sin embargo, la inteligencia artificial también puede ser utilizada por los malos. ¿Hay evidencias de que las ciberamenazas estén empleando inteligencia artificial, o *machine learning*, para los ataques? Y, de ser así, ¿cómo se está empleando?

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

En los sistemas de alerta temprana que despliega el Centro Criptológico Nacional, estamos trabajando en aplicar técnicas de inteligencia artificial, precisamente con el objetivo de que la detección de los ciberataques sea lo más automatizada posible. Si nosotros, con poco presupuesto y poca gente a nuestra disposición, estamos haciendo estas cosas me imagino que los malos van por la misma línea, sólo que en sentido contrario.

ÁNGEL GONZALO
Moderador

Una nueva pregunta. ¿Para cuándo una ciberdefensa integrada en la OTAN, igual que existe una defensa aérea integrada?

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

Si hablamos solamente de defensa, la OTAN ha avanzado bastante en ese sentido y tiene un centro de operaciones de seguridad. Pero también es verdad que empezó un poco tarde y que su organización todavía tiene que perfeccionarse. Pero sí que existe una organización donde colaboramos todos los países de OTAN. Eso no es algo nuevo. Y también se está integrando la defensa cíber en la OTAN.

ÁNGEL GONZALO
Moderador

Pregunta Juan Cuesta: «La UE ha impuesto recientemente sanciones como la prohibición de viajar a países de la UE o el control de fondos a seis individuos de China, Rusia y Corea del Norte. Ésta es la primera vez que se utiliza esta herramienta. ¿Se podría hacer algo más? ¿Son útiles esas sanciones?».

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

La Unión Europea publicó un documento en enero de este año, conocido como el *tool box*, o la «caja de herramientas», donde viene a decir que hasta ahora los países hemos callado los ciberataques que hemos sufrido y que es hora de empezar a hacer públicos esos ciberataques. Se ha avanzado mucho en ese sentido. Ahora mismo se comparte muchísima información entre las distintas agencias de seguridad en relación con los ciberataques, precisamente para poder determinar y aplicar toda una serie de herramientas diplomáticas. Yo creo que son efectivas pero entran dentro del terreno de la geopolítica y la geoestrategia, que es algo en lo que no me voy a meter.

ÁNGEL GONZALO
Moderador

Miguel Ángel Aguilar tiene una pregunta para cada uno. Para el General: «En los ciberataques, ¿funciona la disuasión del débil al fuerte?».

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

La disuasión funciona siempre y cuando dispongamos de las herramientas y de la voluntad de demostrar que, aunque seamos un país más pequeño, somos capaces de llevarla a cabo. Por ejemplo, aunque el país equis tenga doscientos millones de habitantes y Francia sólo tenga ochenta, Francia, siendo mucho más pequeña, ha demostrado públicamente que tiene la voluntad de emplear

sus armas cíber. Ésa es la clave definitiva para la disuasión: que salga la ministra de Defensa francesa diciendo que tiene la voluntad de utilizar las armas de las que dispone.

ÁNGEL GONZALO
Moderador

Para Rosa: «¿Cómo colaborar contra las estafas? ¿Deben comunicarse las sospechas?».

ROSA DÍAZ
Directora general de INCIBE

Depende de a qué llamemos sospecha. Cuando recibes un correo electrónico, si hablamos de esas estafas que suelen venir por *phishing*, por supuesto que hay que ponerlo en conocimientos de las fuerzas y cuerpos de seguridad, que buscan patrones para luchar contra la ciberdelincuencia. Es decir, si no se denuncia o se informa en el 017, donde definirán si algo es una amenaza o no, si no lo comunicamos, si la policía no tiene esas muestras y esos ejemplos para intentar hacer investigaciones, no llegaremos a ningún sitio, pues a la hora de establecer patrones no es lo mismo tener una estafa que tener cien. Lo que ocurre es que muchas veces da vergüenza reconocerlo. ¿Cómo voy a reconocer que me han estafado? ¿Cómo voy a admitir que he pagado en bitcoins? Esto es algo que ocurre muchas veces. Pero todos los organismos estamos de acuerdo en que hay que denunciarlo, porque sólo así podremos luchar contra ello.

ÁNGEL GONZALO
Moderador

Y para Luis: «¿Anonimato y consecuencias es igual a atrevimiento e impunidad?».

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

Probablemente sea correcta esa ecuación. El anonimato permite hacer muchas cosas. El anonimato hace que nos atrevamos a hacer cosas que sin ella no haríamos e impide la investigación y las consecuencias. Pero me gustaría resaltar que anonimato no es lo mismo que privacidad. Se puede perfectamente preservar y proteger la privacidad sin que exista el anonimato en las redes. Son dos cuestiones totalmente distintas. Hay que preservar y proteger la privacidad, pero técnicamente habría que retocar el anonimato que actualmente existe en los sistemas.

ÁNGEL GONZALO
Moderador

Otra pregunta respecto al tema de ciberseguridad y ciberdefensa nacional: «¿Ustedes también consideran que es necesaria la creación de un centro nacional de operaciones de ciberseguridad y ciberdefensa?».

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

En la mesa anterior se ha hablado de la necesidad de crear un centro de operaciones de seguridad de la Administración General del Estado, algo que ya está aprobado por el Consejo Nacional de Ciberseguridad. La cuestión es si dar un paso más adelante, de tal forma que ese centro de operaciones de seguridad de la Administración General del Estado se convierta de alguna forma en los ojos de todos los demás. Tener por encima un puesto de mando, como lo ha llamado el General Sanz Roldán, indudablemente sería una ventaja, como siempre lo es poder tener una cabeza pensante, con uno o varios organismos ejecutores alrede-

dor. Con una centralización así se favorecería mucho la respuesta a incidentes y ataques.

ÁNGEL GONZALO
Moderador

Siempre que la ministra de Hacienda lo permita, claro.

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

Siempre que los Presupuestos Generales del Estado lo doten de una partida presupuestaria.

ROSA DÍAZ
Directora general de INCIBE

Por dar un mensaje de tranquilidad a toda la audiencia, aunque en España existen diferentes organismos a nivel operacional, tenemos una legislación que nos dota de todos los recursos y de comisiones permanentes que permiten que todos estemos comunicados. En los diferentes organismos que existen actualmente, estamos todos bajo un marco legal común, unidos, juntos, trabajando y colaborando para que España sea más cibersegura.

MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación de Periodistas Europeos

A propósito de la respuesta del General, quería apuntar que la actitud francesa fue la misma que tuvo con la fuerza nuclear. Eso está muy bien explicado por el General Beaufre en su libro *Introducción a la estrategia*, donde lo que dicen los franceses es que la defensa nacional de Francia ante todo tiene que ser francesa. Aunque no tenga la potencia nuclear que tienen los norteamericanos o los soviéticos, soy capaz de causarles un daño inaceptable. Eso es lo que se llama disuasión del débil al fuerte y por ahí a lo mejor podríamos caminar también nosotros.

Respecto a este asunto del anonimato, yo creo que es un asunto sobre el que se debería reflexionar. El anonimato, por ejemplo, es muy importante en el periodismo. Hay muchísimas cosas que nunca sabríamos si de entrada tuviera que figurar el que lo presenta, el que lo denuncia, porque son cosas que tendrían unas consecuencias letales para el que lo hace. Por eso existe el *off the record*, que consiste en que alguien te cuenta algo con la condición de que mantengas el anonimato sobre el origen de la información. Tú sabes cuál es el origen y a partir de ahí trabajas, averiguas y después públicas. Pero tampoco puede ser que el que recibe la información piense que, publicándola tal cual la ha recibido, queda exento de responsabilidad y cuando le pregunte un juez baste con reservarse la fuente. En ese caso, si usted reserva la fuente, usted es el responsable de la información; el que va a ir a prisión es usted. Por tanto, es necesario operar a veces con reserva. Son absolutamente inaceptables la irresponsabilidad y el atrevimiento derivados del anonimato, del anonimato como sistema que permite cualquier desatino. Eso sí que me parece muy grave. Igual que hay una educación vial y a los niños en las escuelas se les enseña que con el semáforo en verde para los coches no pueden cruzar, debería haber una educación digital. Me parece que eso es fundamental, porque la gente entra en internet con mucha ingenuidad.

ÁNGEL GONZALO
Moderador

A ese respecto tenemos una pregunta: «Para que los ciudadanos tomen conciencia de la importancia de la ciberseguridad, ¿no sería importante desarrollar un plan de formación generalista en ciberseguridad que se incorporase a todo el ciclo educativo?».

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

Cuando hablo de anonimato, yo me refiero al anonimato de las máquinas. Yo necesito saber llegar a la máquina en la que se origina un ataque. Una vez que tengo identificada la máquina, para identificar a la persona que está detrás, para saber quién es, a qué se dedica, etcétera, ya tengo que ir al juez, con todas las garantías procesales que se derivan de ello. Pero, hoy por hoy, no puedo identificar la máquina porque los sistemas están construidos de tal manera que garantizar el anonimato de las máquinas.

Volviendo al símil de la circulación vial, usted no puede circular con un vehículo que no tenga matrícula. Eso es de lo que estoy hablando, de que no circule un paquete de datos por internet sin su matrícula. Otra cosa es identificar después quién es el propietario de ese vehículo. Eso ya entra dentro del mundo analógico, del mundo procesal, de las leyes… Desde el punto de vista técnico, lo que yo necesito a la hora de investigar un ciberataque es poder llegar a una máquina, poder identificarla. Y ahora eso no es posible.

MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación de Periodistas Europeos

En efecto, los coches tienen matrículas, pero si usted quiere saber quién es el propietario del coche esa información no está disponible para usted. Para la policía sí pero para usted no.

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

En efecto, está protegido por las leyes de privacidad. Yo distingo perfectamente lo que es privacidad de lo que es el anonimato. El problema es el anonimato de la tecnología.

ÁNGEL GONZALO
Moderador

¿Cómo se solapa la Ley de Protección de Datos con estos asuntos?

LUIS JIMÉNEZ
Subdirector general del Centro Criptológico Nacional

Gracias a que existe la Ley de Protección de Datos tenemos garantizado que todo lo que yo haga en internet permanezca en el ámbito de mi privacidad. Pero no es de eso de lo que estamos hablando. Yo estoy hablando de que, a la hora de investigar un ciberataque, necesito ser capaz de poder determinar, a nivel técnico, la máquina de la que procede ese ataque.

GENERAL RAFAEL GARCÍA HERNÁNDEZ
Comandante del Mando Conjunto del Ciberespacio

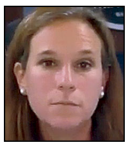
Me gustaría concluir esta sesión remitiéndome a la última pregunta del panel anterior, en la que se recordó la importancia de la creación de ese Foro Nacional de Ciberseguridad donde participen tanto las empresas como el ámbito educativo; uno de los grupos de trabajo se centra precisamente en la necesidad de concienciar sobre la ciberseguridad. De ese grupo de trabajo podría perfectamente salir ese plan nacional, o como queramos llamarlo.

ÁNGEL GONZALO
Moderador

Creo que ésta ha sido una experiencia extraordinaria; incluso me ha sabido a poco esta sesión. Ha sido un placer y un privilegio contar con los tres. Muchísimas gracias.

6. RETOS DE LA CIBERSEGURIDAD PARA EL SIGLO XXI

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad del Departamento de Defensa de Estados Unidos



Moderador
JAVIER FERNÁNDEZ ARRIBAS
Director de *Atalayar*

Madeline Mortelmans y Javier Fernández Arribas

La carrera nuclear en la que competían Estados Unidos y Rusia generó la MDA (Mutua Destrucción Asegurada), que disuadió del empleo del arma nuclear. Descartado el juego de la aniquilación, ahora la amenaza busca injerencias de distinta graduación que pueden afectar la base misma del sistema democrático.

Con las elecciones norteamericanas de noviembre de 2020 como horizonte de proximidad y el recuerdo de los comicios de 2016 como telón de fondo, Washington y Moscú juegan su partida en un tablero que difiere del de cuarenta años atrás, subidos al escenario de las nuevas tecnologías, que amplifican los impactos y permiten planificarlos con mayor precisión.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Damos comienzo a la quinta sesión del Seminario Internacional de Seguridad y Defensa: «Retos de la ciberseguridad para el siglo XXI». Para hablar de estos asuntos, nos acompaña por videoconferencia Madeline Mortelmans, la directora principal para Política de Ciberseguridad del Departamento de Defensa de Estados Unidos.

Ms. Mortelmans, buenas tardes en Madrid, buenos días en Washington. Es un placer tenerla con nosotros.

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Muchas gracias por haberme invitado. Para mí es un verdadero placer tener esta oportunidad para hablar con todos ustedes sobre el Departamento de Defensa, sobre cómo entendemos actualmente la amenaza en el ciberespacio y cómo estamos respondiendo a ella. Por supuesto, estaré encantada de responder a cualquier pregunta que quieran hacerme al final de la presentación.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Gracias, directora. Antes de dar paso a su presentación, quisiera presentar brevemente su perfil a los compañeros que están aquí presentes y a los que no están viendo *online*.

Como he dicho, Madeline Mortelmans es la directora principal para Política de Ciberseguridad del Departamento de Defensa de Estados Unidos. Anteriormente, desde 2004 trabajó en la Oficina del Secretario de Defensa, donde fue asistente especial de dos subsecretarios y asesoró sobre estrategias y presupuestos, sobre actividades *online,* sobre cooperación internacional y el compromiso con socios y organizaciones internacionales, así como en la implementación de la estrategia del Departamento de Defensa y sus planes, incluyendo los que están relacionados con las fuerzas del ciberespacio, sus capacidades y su utilización.

Anteriormente, fue contratista de la Agencia de Reducción de Amenazas de Defensa, dentro del programa cooperativo de reducción de amenazas, y estuvo asignada a la misión de Estados Unidos ante la Organización para la Seguridad y la Cooperación de Europa. Sin duda es un currículum muy extenso e interesante.

Sin más dilación, me gustaría dar comienzo a este panel con una pregunta sobre el alcance que pueden tener las tensiones del ciberespacio. Hemos hablado antes sobre la mutua destrucción asegurada y la pregunta es si usted cree que el ciberespacio puede alcanzar estas capacidades. ¿Podemos llegar a esa mutua destrucción asegurada en el ciberespacio?

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Es una pregunta fantástica. Si le parece bien, antes de meternos en harina, me gustaría compartir con todos ustedes algo de información acerca de cómo entendemos nosotros en general el entorno de la seguridad y cómo estamos trabajando en la respuesta. A continuación, si les parece bien, ya podemos entrar en esas ideas sobre la disuasión y como esto se desarrolla en general.

Estados Unidos reconoce desde hace tiempo la necesidad del acceso a la seguridad y la prosperidad internacional. Ésta es una visión general del Departamento de Defensa. Como mucha gente sabe, en 1969 el Departamento de Defensa desarrolló un proyecto que se centró en abrir un acceso fiable a la información –se llamaba ARPANET– que llevó al posterior desarrollo de internet. ¿Qué ha cambiado desde entonces desde nuestra perspectiva? La comprensión de la gravedad creciente de la amenaza que supone el acceso abierto a la información fiable. Nuestra superioridad militar disuade la agresión. Irán, China y Rusia, cada vez con más frecuencia, están tomando medidas en la zona gris, llevando a cabo campañas coordinadas de ciberactividad maliciosa que intentan socavar nuestra seguridad. En el contexto de esta amenaza creciente, el Departamento de Defensa ha desarrollado una estrategia y ha concluido que debemos cambiar nuestro enfoque. La ciberseguridad es necesaria pero no basta. Se requiere un enfoque más integral.

Me gustaría subrayar en concreto la idea de que debemos ser capaces de defendernos de lo que está por llegar, igual que hacemos en tierra, mar y aire y también en el espacio. El Departamento de Defensa de Estados Unidos está continuamente involucrado en todo el mundo, identificando y abordando las amenazas con el objetivo de dar respuesta a éstas antes de que lleguen a nuestras orillas, antes de que lleguen a nuestra nación. De la misma manera, creemos que tenemos que hacer lo propio en el ciberespacio. ¿Qué significa esto? ¿Cuáles son las perspectivas? ¿En qué consiste defendernos por adelantado en el ciberespacio?

Se parece bastante a lo que se espera que sea capaz de hacer un ejército tradicional. Es decir, generar información. Supone entender qué están intentando hacer nuestros adversarios y cómo

podemos encontrar esa información. De esta manera, el Departamento de Defensa, y nuestro comando de ciberdefensa, llevan a cabo lo que llamamos operaciones de *hunt forward*, operaciones de caza anticipada. Igual que lo hemos hecho con Montenegro, con Macedonia del Norte, con Ucrania y con otros países de todo el mundo, trabajamos de manera conjunta para combinar nuestro conocimiento y así obtener una visión general de la actividad que llevan a cabo nuestros oponentes. Pero no basta con comprender qué están intentando hacer nuestros oponentes. Tenemos que tomar medidas al respecto, por lo que también estamos tomando medidas para defendernos mejor en este ámbito.

Con ese espíritu, estamos utilizando mejores plataformas de defensa con el objetivo de hacer pública información sobre amenazas, contribuyendo así a la seguridad internacional. Muchas publicaciones del Departamento de Defensa sobre la información que se ha obtenido en China, Irán, etcétera, están ofreciendo beneficios a nivel global, están ayudando a detectar esta actividad maliciosa en todo el mundo.

Cuando resulta adecuado, el Departamento de Defensa está dispuesto a poner en práctica determinadas medidas, de acuerdo siempre con las normas internacionales. Me gustaría subrayar estos aspectos porque creo que es importante que entendamos cómo estamos aproximándonos a esas amenazas para promocionar la estabilidad y la seguridad y para fortalecer las normas de comportamiento. Es un contexto importante que marca el escenario para todo lo que pueda surgir a lo largo de la conversación de hoy.

Respecto a dónde nos puede llevar la tecnología de la información desde la perspectiva de la posible destrucción, creo que éste y otros conceptos de disuasión nuclear no se aplican tanto en el ciberespacio como en el espacio nuclear. Por ejemplo, las armas nucleares son excesivamente destructivas y, además, las operaciones nucleares son muy complejas y pasan por el espectro estratégico. Otra diferencia entre lo nuclear y lo cíber es que lo primero requiere un nivel muy técnico y una inversión muy amplia. Además, hay oportunidades para llevar el control de la proliferación nuclear. Por el contrario, las herramientas cibernéticas están al alcance de todo el mundo; no están limitadas a nivel nacional ni tampoco a un pequeño número de países. También hay una diferencia en cuanto a la atribución. En cuanto a armas nucleares, hay un camino muy claro hacia la atribución que se puede hacer de forma muy puntual. En el campo cibernético, en cambio, es más complejo porque tiene que ver con la idea de que habrá una respuesta asegurada, digamos ligeramente más complicada. Por último, la disuasión de la mutua destrucción asegurada es imposible en el ciberespacio, porque las herramientas cibernéticas están siempre disponibles, están siempre en uso. Es un principio establecido que una operación cibernética puede constituir un acto de guerra o permitir el uso de la fuerza. La perspectiva es que un ataque se basa en los efectos que provoca y no tanto en los medios a través de los cuales se consigue.

Quiero subrayar que la OTAN ha confirmado que el Artículo 5 se podría aplicar en el caso de un ciberataque. Asimismo, un ciberataque no necesariamente necesita una ciberrespuesta, mientras que en el campo nuclear sí que es necesaria una respuesta igualmente nuclear. No hay una obligatoriedad de que, si se utiliza un medio cibernético para atacar, nosotros tengamos también que responder de manera cibernética. Hemos evaluado nuestra superioridad militar y sabemos que ésta constituye un efecto disuasorio importante.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Sabemos que, si sufrimos un ciberataque, las personas pueden perder la luz, el agua, los servicios básicos, los bancos, etcétera. Es razonable pensar, por tanto, que el principal problema de los ciberataques es que puedan afectar a las personas en su vida cotidiana.

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Desde luego. Pero al mismo tiempo, si analizamos lo que puede ser una operación cibernética maliciosa, hay muy pocos intercambios tácticos de ceros y unos hasta que llegamos a lo que ha descrito usted. Hemos visto ejemplos claros del uso por parte de nuestros adversarios de una ciberactividad maliciosa que ha afectado a las infraestructuras críticas para los ciudadanos. Eso no es consistente con las normas de comportamiento. Subrayaría, por ejemplo, los ataques de 2017, que tuvieron unas consecuencias importantes para la seguridad internacional. Lo cual subraya la necesidad de la unidad en nuestro objetivo de fortalecer esas normas, así como de actuar de acuerdo con los comportamientos acordados.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Los principales actores del ciberespacio son Estados Unidos, Rusia, China y algún otro país. ¿Se puede hacer algo respecto a la capacidad desde el punto de vista de Estados Unidos?

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Creo que, principalmente, nos preocupa la ciberactividad maliciosa de China, Rusia, Irán y Corea del Norte. Pero, sin duda, hay una multiplicidad de ciberactores en este campo. Tenemos que ser conscientes de que esta ciberactividad no se limita a Estados, a naciones. En el caso de China, vemos que pueden obtener ventajas militares. En 2018, el Departamento de Justicia estimó que más del 90% de los casos de espionaje estaban relacionados con China y que más de dos terceras partes de los casos implicaban la revelación de secretos y también tenían que ver con China. Todo esto a pesar del compromiso de 2015 de que no se realizaría espionaje en aras del propio beneficio económico.

Más recientemente, en 2019, el Departamento de Justicia denunció una campaña llevada a cabo por China que puso en peligro la seguridad cibernética. Y, en julio de 2020, el Departamento de Defensa realizó también una acusación por robar terabytes de datos, incluidos datos que tienen que ver con el desarrollo de las vacunas de la COVID. Se está llevando a cabo espionaje para atacar infraestructuras críticas, pero también para erosionar la confianza en nuestros sistemas democráticos. En Estados Unidos ha habido intentos de interferir en las elecciones de 2016, 2018 y, ahora, en las de 2020, pero también en las elecciones de otros países socios y aliados. También hemos visto ataques que podrían afectar al suministro de energía en Estados Unidos. Pero, como bien saben, éstas no son las únicas amenazas.

Las sanciones contra Corea del Norte tienen que ver con las criptomonedas para generar fondos que apoyen sus programas de desarrollo armamentístico. Hemos visto que Irán ha llevado a cabo ciberataques disruptivos contra empresas estadounidenses y contra nuestros socios y también intenta conseguir información en Oriente Próximo. Y hemos visto organizaciones extremistas que han reclutado gente y que están amasando dinero dirigiendo ataques y distribuyendo *online* una propaganda terrible.

Además de estos actores principales, me gustaría subrayar, por ejemplo, una investigación independiente, la del CSIA, un *think tank* estadounidense que ha recabado una lista de ciberestrategias y ha subrayado que actualmente existen 78 países que tienen estrategias nacionales, de los cuales 31 tienen estrategias militares, ya sean ofensivas o defensivas.Por su parte, la empresa de seguridad FireEye ha elaborado un informe llamado «World War C»; en este caso la «C» no es de cookie sino que se refiere

a la ciberseguridad. Como decía, no estamos sólo ante una amenaza procedente de ciberactores estatales sino también de actores no estatales. Y debemos tener en cuenta también a los ciberdelincuentes. Sin ir más lejos, a principios de este año mis compañeros de Homeland Security han publicado una alerta sobre la creciente peligrosidad del *ransomware*, que ha causado una importante disrupción.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Si le parece, podemos hablar del rol de Europa. ¿Cree que se podría conseguir una colaboración más cercana entre europeos y estadounidenses?

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Por supuesto. Siempre hemos sido socios. Compartimos valores y sistemas económicos y nos hemos beneficiado de un sistema internacional común. Además, todos, de alguna manera, dependemos de internet para facilitar nuestro día a día. Tenemos, por tanto, un interés común.

La estrategia del Departamento de Defensa de 2018 subraya la importancia de fortalecer nuestra seguridad en el ciberespacio, así como la importancia de asociarnos con las interagencias y con la industria, con nuestro sector privado, pero especialmente con nuestros socios y aliados. Creo que tanto Europa como Estados Unidos debemos tener muy clara cuál es la amenaza a la que nos enfrentamos. Rusia y China, por ejemplo, están intentando socavar el orden internacional para entrar en nuestros países, para crear disrupción y para conseguir ventajas económicas y militares. No hay ninguna equivalencia aquí. Esto debería motivarnos

a ponernos en marcha y actuar. Necesitamos trabajar codo con codo. Tenemos que colaborar y fomentar unos estándares de gobernanza para fortalecer internet, unas prácticas óptimas consistentes que sean justas y que también protejan nuestros valores.

Estamos trabajando con esfuerzos conjuntos para establecer unos comportamientos cooperativos y para fortalecer la seguridad. Por ejemplo, el trabajo que estamos haciendo en la OSCE, de la que tengo el placer de formar parte, es un ejemplo excelente de cómo Estados Unidos y Europa pueden trabajar codo con codo para promover la seguridad en el ciberespacio y la estabilidad. Pero la cooperación no se puede restringir únicamente a las actividades *online*. También tenemos que concentrarnos en fortalecer la seguridad de nuestro *hardware* y *software*, asegurando unas prácticas óptimas que protejan la seguridad nacional. El desarrollo del 5G, por ejemplo, o de la inteligencia artificial, pueden suponer una serie de retos ante los que todos nosotros, como naciones y como comunidades que compartimos valores, tenemos que estar dispuestos a trabajar conjuntamente.

También subrayaría, desde el punto de vista del Departamento de Defensa y de los ministerios europeos de Defensa, que existen una serie de iniciativas que están en marcha en este momento que esperamos que nos ayuden a fortalecer nuestras capacidades. Igual que trabajamos conjuntamente en otros campos, estamos trabajando conjuntamente para fortalecer nuestra colaboración en el ciberespacio. Por ejemplo, a través de USEUCOM estamos haciendo esfuerzos de formación conjunta. También tenemos un compendio de formación del Departamento de Defensa disponible para nuestros socios. En marzo, llevamos a cabo un curso verdaderamente increíble en Alemania sobre estudios de ciberseguridad, que aunó a expertos de toda Europa para fortalecer nuestra comprensión común acerca de las amenazas a las que nos enfrentamos y fomentó una serie de iniciativas para fortalecer y mejorar nuestra ciberseguridad, como por ejemplo la conexión en un canal privado de Slack para indicar la información

que nos puede ayudar a defendernos mejor. También llevamos a cabo ejercicios multilaterales, como la NATO Cyber Coalition y los ejercicios Locked Shields del CCDCOE de la OTAN.

Me gustaría subrayar que Estados Unidos participa también en una serie de equipos internacionales; todo ello con el afán de colaborar para asegurarnos de que tenemos las políticas, los estándares y los marcos internacionales adecuados para fomentar la seguridad y la estabilidad internacional. Desde el Departamento de Defensa, también tenemos que llevar a cabo una serie de operaciones en el ciberespacio, igual que lo hacemos en otros ámbitos, para asegurar nuestra superioridad militar.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Hemos hablado de defensa y de seguridad, pero supongo que en el Pentágono, en el Departamento de Defensa, también preocupará enormemente la economía, el comercio, los negocios, etcétera, como objetivos de los ataques terroristas.

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Desde luego. Creo que una de las consideraciones claves sobre el campo cibernético es que forma parte intrínsecamente de la vida cotidiana de los estadounidenses y de nuestros socios europeos, pues es el telón de fondo que ha permitido, en gran medida, nuestro éxito económico. Y aunque hay una serie de implicaciones económicas en el campo cibernético que lo hacen diferente, creo que es tan clave como cualquier otro ámbito de nuestras vidas. En ese sentido, cuando aumentamos nuestra dependencia, aumenta nuestra vulnerabilidad. Cuanto más conectados estamos, más vulnerables somos. Nosotros llevamos en primera

línea de batalla de la tecnología mucho tiempo y estamos orgullosos de ello, pero eso también conlleva una serie de riesgos y de vulnerabilidades. En el Departamento de Defensa somos plenamente conscientes de esto y subrayamos la importancia de nuestra misión de defender la nación, tal y como está reflejado en nuestra estrategia. Así lo decimos explícitamente. Para ello, tenemos que estar preparados para proteger nuestras infraestructuras críticas de un ataque con consecuencias significativas, para lo que es necesario comprender a fondo lo que están intentando hacer nuestros adversarios y conocer las técnicas que están empleando. Esto nos permite también ayudar a nuestros socios y estar todos mejor preparados. De esta manera, si hiciera falta que actuásemos, estaremos todos mejor preparados. Yo reitero una y otra vez la necesidad de tener unas normas de comportamiento correcto, porque eso nos lleva a comprender nuestro papel en el ciberespacio, promoviendo y fortaleciendo unas normas que nos benefician a todos y contribuyendo así a la seguridad y la estabilidad en el ciberespacio, que a su vez promueven la prosperidad económica y el buen funcionamiento de nuestras sociedades.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Ms. Mortelmans, usted y yo somos muy conscientes del riesgo que suponen los ciberataques, pero ¿lo es la sociedad? Las redes sociales, las películas, los vídeos, etcétera, complican la percepción real de esas amenazas.

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Es una muy buena pregunta. Creo que, de muchas maneras, las películas y los vídeos sí que complican las cosas en lo que se re-

fiere a presentar una narrativa que simplifica demasiado la situación, que simplifica demasiado lo que es una ciberoperación, mostrándola como una cosas fácil y al alcance de cualquiera. En la televisión siempre se simplifican las cosas. Éste es un terreno muy complejo pero, seas un ciudadano particular, una empresa o un Gobierno, el hecho de comprender hasta qué punto dependes de lo digital es realmente muy importante.

También hay que decir que no solamente son un riesgo las acciones que se plantean en el ciberespacio, sino que el dominio digital se puede utilizar para amplificar mensajes relativos a la interferencia internacional con el objetivo de sembrar la discordia. El dominio cibernético, por decirlo así, derriba fronteras y esta comunicación libre que valoramos tanto también puede ser explotada y aprovechada por nuestros enemigos. En el Departamento de Defensa hablamos de ello como una ecuación que está integrada por vulnerabilidad, amenaza e impacto.

A medida que avanzan las tecnologías, las vulnerabilidades son cada vez mayores. Utilizamos tecnologías cada vez más avanzadas, más sofisticadas, y también introducimos cada vez más datos *online*. Esto crea más vulnerabilidades y también plantea impactos mayores en el caso de surgir cualquier problema. Y el riesgo no va a hacer sino crecer a medida que adoptemos el «internet de las cosas» y avancemos hacia el entorno 5G. También nuestras amenazas están creciendo. La escala y el alcance de lo que están haciendo nuestros enemigos son cada vez mayores. Por lo tanto, estamos ante un reto importante, por lo que es importante que en todo el mundo comprendamos mejor esta situación.

Dicho esto, no quiero centrarme sólo en las amenazas ni tampoco asustar a la gente, porque no todo está perdido. Muchas veces se dice que lo importante es elegir bien. Si nos fijamos en la historia de las incidencias cibernéticas del pasado reciente, vemos que siempre se han explotado vulnerabilidades que ya eran conocidas y que se ha hecho mediante parches que ya estaban disponibles. Es decir, que ya existía una solución que, con una

buena ciberseguridad y un *software* actualizado, hubiera podido mitigar el impacto de esos incidentes cibernéticos. Como digo, los principales incidentes han derivado de cosas que realmente se hubieran podido evitar con un buen sistema de ciberseguridad. Lo que necesitamos no es una panacea que resuelva de golpe la amenaza cibernética sino que la gente adopte buenas prácticas *online*, que tenga el *software* actualizado, que utilice los modelos correctos… En otras palabras, que todos estemos lo más al día posible. En resumen, existe una amenaza importante pero no está todo perdido. En la mayor parte de los casos, una buena política de ciberseguridad nos va a permitir abordar estos retos.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Tenemos algunas preguntas de nuestros invitados. Pedro González, de RTVE y colaborador de *Atalayar*, pregunta si tienen indicios de que Rusia o China pueden intentar interferir en las próximas elecciones estadounidenses. ¿Cómo abordarían esa amenaza potencial?

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

El Departamento de Defensa forma parte de un esfuerzo a nivel gubernamental para responder a las amenazas de cara a nuestras elecciones. En cuanto a esta amenaza concreta, el director de Inteligencia Nacional ha emitido un comunicado respecto a las amenazas procedentes de países como China y Rusia. Por tanto, sí estamos alertados. En cuanto a cómo estamos trabajando en todo ello, quiero decir que el Departamento de Defensa participa en un esfuerzo pangubernamental. Nuestra ventaja competitiva estriba en nuestra capacidad de operar fuera de Estados Unidos.

Estamos trabajando para generar información de lo que están intentando hacer nuestros adversarios para interferir en las elecciones. Es decir, qué cambios quieren introducir en nuestras redes, sistemas e infraestructuras o cómo pueden intentan influir en las opiniones del pueblo estadounidense. Estamos intentando recabar la mayor cantidad de información posible.

El segundo paso, como he dicho, tiene que ver con cómo fomentar una buena defensa. No es suficiente saber lo que quieren los adversarios. Tenemos que asegurarnos de que las personas correctas tengan la información correcta. Lo que estamos haciendo es informar al Departamento de Interior sobre cuestiones que pueden ayudarles a defender mejor nuestros sistemas. Y también estamos identificando actividades encubiertas. Esta información la transmitimos al FBI, que trabaja con nuestros socios del sector privado, con las empresas de redes sociales, etcétera. Lo que hacen quienes nos amenazan es violar los términos de servicio con un enmascaramiento. Por nuestra parte, tenemos la voluntad de afrontar este problema y, de ser necesario, emprenderemos las acciones necesarias, como ha dicho el secretario de Defensa, pues para nosotros esto es prioritaria.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Pregunta Georgina Higueras, que ha sido corresponsal del diario *El País* en Asia-Pacífico: «¿Qué país supone una mayor amenaza para Estados Unidos en el ciberespacio, China o Rusia?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Ésa es una pregunta que no es nada fácil de contestar porque la naturaleza de sus ciberactividades maliciosas es diferente. China

realiza campañas coordinadas a largo plazo. Su ciberactividad intenta erosionar nuestras ventajas económicas y de defensa; realmente se trata de prácticas inaceptables. Podría señalar unas estadísticas que resaltan la ingente cantidad de información relativa a propiedad intelectual y otros aspectos económicos que ha robado China. En cambio, lo que quiere Rusia es impedir el correcto funcionamiento de ciertas actividades. Ambas son amenazas muy importantes pero diferentes en su naturaleza. Pero ambas son amenazas muy importantes en las que estamos centrados.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Alejandro Grosso Grazioli pregunta: «Qué agencia lidera la acción en el ámbito de la ciberseguridad en Estados Unidos. ¿El Departamento de Defensa, la CIA, el Departamento de Interior...? ¿Cómo se coordinan las distintas agencias?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Tenemos una estructura muy compleja. Dentro del Gobierno estadounidense, cada departamento, cada agencia, tiene un papel distinto. El Departamento de Interior se ocupa de la protección de nuestras infraestructuras críticas ante los ciberataques. Tienen una agencia llamada CISA que se ocupa de todo ello y que trabaja con nuestro sector de infraestructuras para advertirles de posibles amenazas. Luego también hay agencias sectoriales, donde atendemos la defensa en el sector industrial, trabajando con nuestros socios para asegurarnos de que cumplen con nuestras normas de protección de la información. Por su parte, el FBI se ocupa de la investigación de los delitos cibernéticos, del espionaje cibernético, etcétera. Y el Departamento de Defensa, como

sabéis, se ocupa de las operaciones militares. Por lo tanto, cada organización tiene sus propias tareas y trabajamos en equipo para abordar estos retos y amenazas aprovechando nuestras ventajas competitivas. Las elecciones son un ejemplo excelente del nivel impresionante de coordinación y de cooperación que tenemos y de cómo ponemos toda la carne en el asador y logramos un resultado óptimo. Nuestra ciberestrategia de 2018, que fue la primera en dieciocho años, articula la forma en la que todos trabajamos juntos y los objetivos que deseamos cumplir.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Desde las Islas Canarias, pregunta Alberto Suárez, que es un joven analista: «¿Tiene usted miedo usted de que China pueda interferir cibernéticamente en el proceso político de 2020 en Estados Unidos o de que pueda adoptar de alguna forma represalias a causa de la política arancelaria de Estados Unidos?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Como decía antes, el director de Inteligencia Nacional ha publicado una declaración que caracteriza la forma en la que percibimos las amenazas de nuestros adversarios. Les recomiendo que lean esta declaración. Yo, como técnica de defensa que soy, no puedo referirme a temas políticos.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Ana Alonso, de *El Independiente*, pregunta si somos más vulnerables a los ciberataques en la actualidad debido al coronavirus.

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Creo que todo esto tiene más que ver con el tema de los delitos cibernéticos, que es algo de lo que se ocupa el FBI. Desde la perspectiva del Departamento de Defensa, les puedo decir que nosotros lo que hemos hecho es intentar que la gente trabaje desde sus domicilios y que esté conectada. Pero claro, cuantas más redes tengas, cuanto más distribuidas estén tus operaciones, más vulnerable eres ante cualquier ataque cibernético. Por lo tanto, sí, existe un desafío añadido ahora que estamos trabajando de forma remota en esta era del coronavirus. No obstante, tengo que decir que mis compañeros han hecho un trabajo fantástico para permitirnos trabajar de forma remota de un modo seguro. Además, el Departamento de Defensa está acostumbrado a este tipo de operaciones distribuidas, por lo que no dudo de que tendremos éxito en esta cuestión.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Otra pregunta: «¿Cuál es el papel de Sudamérica en la ciberdefensa?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Desde nuestro punto de vista, nuestros socios de Sudamérica son socios críticos con los que tenemos una serie de alianzas a la hora de identificar las amenazas a las que nos enfrentamos. Hay muchos expertos en tecnología y tenemos muchas alianzas bilaterales que queremos ampliar en el sector cibernético. En cuanto

a la cosmovisión de Sudamérica, yo realmente no puedo hablar en nombre de una región que no es la mía. Lo que sí puedo decir es que estamos encantados de trabajar codo a codo con ellos y deseosos de participar en un diálogo con la región del hemisferio occidental en su conjunto.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Roberto Uzal pregunta: «¿El sistema financiero de Estados Unidos también tiene una alta dependencia del espacio cibernético. ¿Forma eso parte también de las responsabilidades de su departamento?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Nuestro sector financiero es una de nuestras dieciséis infraestructuras críticas y mis compañeros del Departamento de Interior trabajan concienzudamente y sin descanso en este ámbito. Luego está el Departamento del Tesoro, que es una agencia específica para el sector financiero y con la que éste mantiene una alianza muy robusta. En el Departamento del Tesoro colaboran de forma constante con empresas, así como con el Consejo para el Uso Compartido de Información. Ha habido una serie de programas piloto para promover el trabajo conjunto entre el sector financiero y el Departamento de Interior con el propósito de comprender mejor las amenazas a las que se enfrentan e intentar generar información que les pueda ayudar a defenderse y asegurarse de que están bien preparados. Tanto el Departamento de Interior como el de Defensa trabajamos de forma activa con una serie de sectores para asegurarnos de que entendemos cabalmente sus necesidades.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Otra pregunta relacionada: «¿Funciona de forma correcta la cooperación entre la administración y las grandes empresas? Por ejemplo, con Facebook, Microsoft y el resto de grandes compañías tecnológicas estadounidenses. ¿Les proporcionan estas grandes tecnológicas toda la información que necesitan para evitar ciberataques?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

En el Departamento de Defensa tenemos una página de Facebook y utilizamos productos de Microsoft; utilizamos muchos productos del sector privado. Éstas son nuestras relaciones privadas. Ahora, en el sector operativo trabajamos a través de nuestros socios en el mundo civil, como el FBI, para asegurarnos de disponer de una comunicación realmente sólida. Es un enfoque básicamente pangubernamental.

El FBI tiene una alianza a largo plazo con las empresas de redes sociales a la hora de comunicar actividades que puedan estar sucediendo *online* y en el Departamento de Defensa, a su vez, tenemos una alianza con el FBI, al que, además, ayudamos con la información que nosotros recogemos. Si, por ejemplo, hay una incidencia con amenazas, trabajamos con el Departamento de Interior para asegurarnos de que éste tiene la información correcta y puede dirigirse a los sectores adecuados, a las empresas adecuadas, para que la comunidad en su conjunto esté protegida. También publicamos cada vez más información propia, en coordinación con el FBI y el Ministerio de Interior. Nuestro cibermando tiene su propio perfil de Twitter, donde informan sobre *software* malicioso, sobre amenazas a la seguridad nacional, et-

cétera. Y otros organismos gubernamentales también utilizan las redes sociales. Lo que queremos es que la comunidad tenga la información adecuada en el momento adecuado, de tal manera que la defensa sea lo mejor posible.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

«¿Cómo conceptualiza el Departamento de Defensa las amenazas híbridas en el ciberespacio?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Dedicamos mucho tiempo a las ciberamenazas, a las ciberactividades maliciosas… En nuestra revisión del año 2018, nos dimos cuenta de que no podemos analizar los incidentes como actividades individuales, sino que hay que analizarlos como campañas coordinadas que se llevan a cabo como parte de un esfuerzo estratégico por obtener una ventaja asimétrica, que puede ser económica, defensiva, etcétera. Si nos fijamos, por ejemplo, en las fugas de información industrial, si pensamos en ellas como incidentes aislados quizás no sean tan preocupantes pero, analizadas de forma colectiva, analizando el impacto que tienen en su conjunto, vemos que se ha robado un fragmento de información clasificada de un sitio, otro fragmento de otro, etcétera. Así, de forma colectiva, podrían conseguir información muy importante sobre nuestros sistemas de armamento, lo cual, por supuesto, es algo que no podemos permitir. De ahí la necesidad de ser más proactivos, tanto en términos de cómo defendemos las cosas como en otros ámbitos. Hasta 2018 hablábamos de defender nuestra información donde quiera que estuviera, pero a partir de entonces decidimos ser más proactivos en lo que respecta a la respuesta. Hay que analizar estos actos como lo que son: actos coordinados. No se pueden analizar de forma aislada.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Fernando García Vaquero pregunta: «Si se produjera un ataque sobre un miembro de la OTAN, ¿daría lugar a la activación del Artículo 5? ¿Sería necesario utilizar el paraguas del mandato de Naciones Unidas?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

En el caso del Artículo 5, utilizaríamos los mecanismos de consulta y procedimientos habituales en la OTAN. Lo que quiero poner de manifiesto es que los medios de ataque son menos importantes que los efectos de estos ataques. Del mismo modo que si se produjera un ataque aéreo no sólo responderíamos por vía aérea, un ciberataque no necesariamente tiene que abordarse solamente a través del ciberespacio. Se trata de operaciones militares y por tanto nos reservamos el derecho de responder de la forma que consideremos más apropiada. En un caso así, el debate en la OTAN sería similar al de cualquier ataque, pues hay muchos adversarios que utilizarán el ciberespacio para conseguir efectos en otros dominios.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Juan Cuesta pregunta: «¿La fragilidad de la seguridad en el ciberespacio podría obligar a algunos Estados a reducir el intercambio de información con sus aliados, a decidir qué comparte

y con quién?». Y una segunda pregunta: «En la decisión de excluir a Huawei de la red 5G, ¿hasta qué punto es real el riesgo y hasta que punto se trata de proteger los propios intereses?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

La primera pregunta tiene que ver con el intercambio de información. El hecho de poder comprender las amenazas nos asegura que podamos defendernos mejor. Estamos totalmente comprometidos con esto. Trabajamos con nuestros aliados, con nuestros socios, a nivel clasificado y no clasificado. Antes de la COVID, yo viajaba frecuentemente a la sede de la OTAN para analizar esas amenazas con los compañeros. Algo que, por cierto, hacemos muy bien en equipo y que creo que es importante poner de manifiesto.

En cuanto al 5G, realmente el riesgo es importante. Como he dicho antes, es fundamental tener muy claro cuál es la amenaza. Cuando analizamos el abanico de cuestiones relacionadas con la tecnología 5G y su aplicación, si nos fijamos en una serie de factores, como por ejemplo las prácticas deficientes de Huawei en materia de ciberseguridad y las leyes de seguridad de China, que requieren que cualquier empresa china proporcione cualquier tipo de información que le solicite el Gobierno chino, pues, realmente, resulta lógico que todo país soberano se plantee si ese nivel de riesgo es aceptable.

La posición de Estados Unidos es muy clara. El Congreso lo ha dejado nítidamente claro y el Departamento de Defensa también. No es aceptable permitir que una empresa rival que tiene en marcha un requerimiento tenga acceso privilegiado a nuestras redes, a nuestra información. Eso es algo que no podemos permitir. Plasmado de esta manera tan clara, para nosotros no hay duda alguna sobre la cuál es la decisión correcta.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Una nueva pregunta: «¿Cómo determinan ustedes si un ataque realmente es un ataque o una estrategia psicológica?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

En lo que se refiere a las influencias que vienen del extranjero, un aspecto clave es que no analizamos la información. En Estados Unidos tenemos unas leyes que garantizan la libertad de expresión y esto incluye el derecho a recibir cualquier tipo de información. Es lo primero que hicieron nuestros padres fundadores, garantizar la libertad de expresión, y nosotros nos esforzamos por proteger esa libertad. Por tanto, no se trata de la información, sino de los actores. Hay actores, agentes extranjeros, que lo que quieren es ejercer su influencia de forma encubierta. Por eso lo importante es exponerlos, desenmascararlos, hacer todo lo posible para que no puedan ocultar lo que intentan hacer.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Otra pregunta: «¿Cómo pueden los países periféricos protegerse de las campañas de desinformación que vienen del extranjero?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Hay algunos estudios muy interesantes al respecto. Por ejemplo, el Consejo Atlántico ha trabajado mucho en esta cuestión, tra-

tando de entender cómo pueden defenderse mejor los países. Todo tiene que ver con informar al público, con educar al público acerca de las amenazas que existen y fomentar el pensamiento crítico. Esto cae un poco fuera de lo que hacemos nosotros, pero les recomiendo que lean estos textos. Algunos países en Europa llevan enfrentándose a este desafío mucho tiempo. El ciberespacio no fue el que creó este problema; simplemente lo amplió y creó nuevos vectores del problema. Si nos fijamos en lo que ha sucedido históricamente podemos aprender mucho de nuestro propio pasado sobre cómo luchar contra estas amenazas.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Antes de finalizar, tenemos una última pregunta, en este caso de Daniel Galvache desde Buenos Aires, Argentina. Dice: «Un análisis de los ataques rusos del 2016 dejó claro que las redes sociales juegan un papel importante en las campañas de desinformación de la inteligencia rusa, que plantea información falsa para influir en la información que tienen los votantes sobre los candidatos electorales. ¿Estados Unidos ha desarrollado algún sistema para garantizar una detección precoz de las noticias falsas?».

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Como he dicho, el Departamento de Defensa forma parte de un esfuerzo pangubernamental. Nuestros compañeros del FBI están haciendo un trabajo impecable en este sentido. Realizan informes, trabajan de sol a sol con el Congreso para desarrollar buenas prácticas… Lo que puedo decir es que, para el Departamento de Defensa, todo tiene que ver con los actores. El objetivo es generar una información clara sobre lo que quieren conseguir esos

actores para luego poder ofrecer recomendaciones, consejos, que conduzcan a una defensa más eficiente. Entre todos, estamos haciendo un esfuerzo para que nuestros compañeros del FBI desenmascaren a estos actores. Porque si se producen estas actividades maliciosas es importante emprender las acciones necesarias. Somos parte, como digo, de un esfuerzo pangubernamental y nuestros compañeros del FBI han trabajado mucho en esta cuestión. No puedo hacer otra cosa que felicitarles.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Madeline, muchísimas gracias por sus palabras, por sus comentarios. Hemos aprendido muchísimo de usted. Ha sido un placer escucharla hablar de la seguridad y la defensa en el espacio cibernético. Espero que podamos vernos de nuevo en otra ocasión.

MADELINE MORTELMANS
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

Muchas gracias a ustedes por invitarme. Para mí ha sido un placer participar en este encuentro.

7. CHINA, ¿CIBERPOTENCIA SIN CONTROL?

MARIO ESTEBAN
Investigador principal del Real Instituto Elcano
y profesor titular del Centro de Estudios de Asia
Oriental de la Universidad Autónoma de Madrid

IGNACIO RAMOS
Profesor de Relaciones Internacionales y
delegado para Asuntos Chinos en la
Universidad Pontificia Comillas

CORONEL CARLOS JAVIER FRÍAS
Doctor en Paz y Seguridad Internacional.
Colaborador del Instituto Español de
Estudios Estratégicos (IEEE)

Moderadora
GEORGINA HIGUERAS
Excorresponsal de *El País* en Asia-Pacífico

Mario Esteban, el Coronel Carlos Javier Frías,
Ignacio Ramos y Georgina Higueras

La ambición de China por convertirse en la primera potencia tecnológica le ha llevado a desplegar una gran estructura defensiva contra la intrusión de «malos actores», capaz de brindar a sus fabricantes, investigadores y desarrolladores la protección adecuada ante posibles ataques cibernéticos. Esa estructura se complementa con la entrada en vigor, en enero de 2020, de la Ley de Criptografía y la actualización de regulaciones de diciembre de 2019. Ambas medidas se encuentran bajo el paraguas de la Ley de Ciberseguridad, en vigor desde junio de 2017, que identifica como «industrias clave» las de los sectores energético, financiero, transportes, telecomunicaciones, salud, eléctrico, agua, gas y seguridad social. La legislación dicta instrucciones precisas sobre cómo las empresas y organizaciones del sector público y privado, tanto chinas como extranjeras, deben proteger sus redes, pero las empresas extranjeras temen que, con la adaptación de esas estrategias, China acabe adueñándose de toda la información de las empresas que operan en el país.

GEORGINA HIGUERAS
Moderadora

Buenos días a todos, tanto a los que estáis aquí de forma presencial como a los que nos escucháis por *streaming*. Para mí es un orgullo participar otra vez en este seminario gracias a la Asociación de Periodistas Europeos y, aunque este año no podamos estar en Toledo, seguro que volveremos muy pronto. Precisamente la COVID, además de este cambio de sede, ha hecho que uno de nuestros participantes, Mario Esteban, no pueda estar de forma presencial con nosotros, pero lo tenemos por videoconferencia.

Hoy vamos a hablar de China como ciberpotencia, sin control o con control. A la hora de analizar China y su relación con el ciberespacio, tenemos que retroceder hasta el nacimiento de internet. Internet nació en 1983, cuando China estaba inmersa en su gran campaña de reforma y apertura, esa campaña emprendi-

da por Deng Xiaoping que consiguió transformar el país, convirtiendo una autarquía maoísta en la segunda potencia económica mundial. En aquel momento, China tenía los ojos absolutamente abiertos a lo que ocurría en el exterior, después de muchos años de aislamiento en los que había dado la espalda a la revolución industrial, por lo que pagó el alto precio de las invasiones a manos de potencias extranjeras. China estaba muy pendiente de todo lo que era nuevo y entendió que el ciberespacio era el futuro. A partir de ese momento se concentró en estudiar, analizar dicho ciberespacio, dedicando muchos de sus esfuerzos a convertirse en una ciberpotencia.

Hay dos hitos de gran importancia en la relación de China con la ciberdefensa, o ciberseguridad. En el año 2008, durante la guerra de Georgia, China ve cómo Rusia se introduce en los sistemas informáticos de Georgia y consigue alterar su proceso de toma decisiones durante la guerra. Eso fue un choque para China. El segundo se produce en 2010, cuando Estados Unidos e Israel crean el virus Stuxnet para infiltrarse en el programa atómico de Irán. Es ahí cuando China se da cuenta de que la guerra cibernética puede acabar con la disuasión nuclear. A partir de esos momentos, China tiene muy claro que, para convertirse en la potencia que ya está camino de ser, lo importante es conseguir la supremacía a nivel cibernético. Su gran obsesión desde ese momento ha sido lograr esa supremacía.

Xi Jinping llega al poder en 2012, cuando China ya es una potencia económica. Entonces, decide que hace falta que su peso económico esté acompañado por una influencia internacional. Y se da cuenta de que, para lograr esa influencia internacional, le hace falta tener una fuerza de combate global, un ejército fuerte que le respalde. Porque el ejército que tenía antes China era un ejército campesino, un ejército que no había tenido ninguna experiencia combativa desde 1979, cuando decidió ir a dar una lección a los vietnamitas y los chinos prácticamente salieron escaldados. Ganaron por el enorme peso numérico, pero China se llevó una buena lección. A partir de ese momento, Xi Jinping emprende la reforma del Ejército Popular de Liberación y, para tener esa capacidad global, crea dos nuevos cuerpos. Además de Tierra, Mar y Aire, crea la Fuerza de Misiles y la Fuerza de Apoyo Estratégico. La Fuerza de Apoyo Estratégico es la que abarca todas estas nuevas fuerzas actuales, que son las ciberfuerzas, las capacidades electromagnéticas, etcétera. Esta Fuerza de Apoyo Estratégico rinde cuentas únicamente a la Comisión Militar Central, que es el órgano del Partido Comunista que controla todo el Ejército Popular de Liberación y toda la estrategia de China. Por supuesto, la preside también Xi Jinping. Con este brazo, China persigue esa supremacía en el ciberespacio en cuya lucha está metida actualmente.

La web norteamericana *The National Interest* decía en 2018 que lo que más le preocupaba de China como rival de Estados Unidos era su enigmática capacidad para realizar operaciones cibernéticas ofensivas, que abarcan desde acciones psicológicas a la destrucción de infraestructuras, además de la capacidad de sembrar el caos en el sistema financiero, energético o de transportes. Hasta ese momento se consideraba que China se dedicaba más a la ciberdefensa pero, a partir de entonces, queda claro que también es una gran potencia ofensiva en aspectos de ciberseguridad. Hasta entonces, la parte de ciberdefensa estaba dedicada a la política interior y se dividida en dos partes muy importantes. La primera, la protección de la población contra las malas influencias exteriores, como la pornografía, el radicalismo islámico y el separatismo, pero también la democracia y los derechos humanos. Había que evitar la influencia que todo esto pudiera tener en su población, había que apartarlo del pueblo. El segundo brazo dentro de esa ciberdefensa china es lo que se llama la Gran Muralla Digital, que tiene como objetivo proteger a sus fabricantes, a sus emprendedores y sus centros de investigación y desarrollo de ataques cibernéticos exteriores. China tiene la mayor policía cibernética del mundo al servicio de esta Gran

Muralla Digital. Según el diario de Pekín, el *Beijing Daily*, en el año 2013 había más de dos millones de policías cibernéticos dedicados al control, sobre todo, de la población china. Es de suponer que ahora serán muchísimos más, sobre todo porque hace dos años se hizo público que la policía cibernética estaba autorizada a infiltrarse en las redes sociales, a tomar identidades distintas para infiltrarse en ellas y controlar a la población, controlar las críticas al Gobierno, cualquier tipo de disidencia, etcétera.

El marco legal de esta Gran Muralla Digital es la Ley de Ciberseguridad que se promulgó en enero de 2017 y entró en vigor en junio de ese mismo año. Según la administración del ciberespacio de China, dicha ley «pretende salvaguardar la soberanía en el ciberespacio, la seguridad nacional y el interés público, así como los derechos y los intereses de los ciudadanos». Se trata de una ley muy ambigua, muy amplia, con 76 artículos, que más que proteger lo que hace es dar cobertura legal a los mecanismos chinos para la monitorización y la censura de los ciudadanos, de los medios, de las webs, de las redes sociales... Precisamente al amparo de esta ley, en 2018 se cerraron 10.000 blogs de gestión privada y WeChat tuvo que eliminar 300.000 artículos y cerrar más de 200.000 cuentas de usuarios, supuestamente por albergar contenido violento, pornográfico, engañoso o crítico. Tuvo que cerrarlas porque la ley responsabiliza directamente a los individuos y organizaciones del contenido de todo lo que se publica.

Podríamos decir que esta ley también consolida el proteccionismo chino. Lo consolida porque impone una serie de revisiones periódicas y de seguridad a las pocas empresas extranjeras que operan en los denominados sectores críticos de las industrias clave, que son el energético, el financiero, transportes, telecomunicaciones, salud, agua y seguridad social. Esta legislación establece la obligatoriedad de las empresas y organizaciones, del sector público y del sector privado, tanto chinas como extranjeras, de proteger las redes. En su artículo 24 exige a los operadores que proporcionen servicios de comunicación y que identifiquen

con datos reales a los usuarios. Además, tienen que facilitar la información personal y todos los datos recopilados deben de guardarse en China. Esto significa que muchísimas VPN que tenían los chinos han dejado de ser útiles. De hecho, la mayoría de las VPN chinas han muerto ahora que todos los ciudadanos chinos tienen que identificarse con su nombre real y decir para qué quieren utilizar esa VPN; la mayoría de ellos las querían precisamente para saltarse la Gran Muralla Digital y entrar en Facebook, para buscar en Google o para acceder a los medios de comunicación extranjeros que pueden estar prohibidos en China.

Además, esta ley se complementa con la primera ley de criptografía que ha tenido China, que entra en vigor en 2020. Es evidente que las empresas extranjeras temen que esta ley de ciberseguridad les obligue a facilitar a China el espionaje y el robo de su propiedad intelectual, ya que, con los controles que impone el Gobierno pueden verse obligadas a facilitarles el código fuente de sus programas y sus datos más confidenciales. No es de extrañar pues que esa ley haya sido muy mal aceptada entre las empresas extranjeras que operan en China.

En resumen, China regula estrictamente las tecnologías extranjeras, en las que evidentemente no confía el Gobierno chino, que se esfuerza por desarrollar sustitutos nacionales. Es lo mismo que está haciendo la administración de Donald Trump. Según China, el 80% de los ataques cibernéticos que sufren sus instituciones estatales procede de Estados Unidos. Por su parte, Estados Unidos no sólo culpa a China de atacar sus sistemas sino que además ha declarado la guerra a Huawei y a ZTE, afirmando que no se puede confiar en estas dos empresas por su cercanía al Ejército Popular de Liberación; basta recordar que el fundador de Huawei es un antiguo oficial del ejército chino, Ren Zhengfei. Aunque, por otro lado, el historiador británico Peter Frankopan dice que es una paradoja que Estados Unidos mantenga esta posición, ya que su Agencia de Seguridad Nacional creó un programa clandestino que se llama Operation Shotgun

para infiltrarse y *hackear* los servidores de Huawei. Por tanto, Huawei no representa ningún peligro para la seguridad nacional de Estados Unidos.

Todo esto demuestra hasta qué punto se ha declarado la guerra en el ciberespacio entre China y Estados Unidos. A principios de agosto, la Casa Blanca lanzó la campaña Red Limpia, que tiene como objetivo erradicar las aplicaciones chinas y otros productos tecnológicos de la red estadounidense. Y la semana pasada, el ministro de Asuntos Exteriores chino, Wang Yi, lanzó lo que ha llamado la Iniciativa Global de Seguridad de Datos, que, en sus propias palabras, da cuerpo al compromiso de China de velar por la seguridad de los datos a nivel mundial. Wang Yi lanzó esta iniciativa durante una reunión con sus homólogos de la ASEAN, la Asociación de Naciones del Sudeste Asiático, donde les dijo que quería una respuesta activa, es decir, que tenían que manifestarse pronto al respecto.

¿Qué significa todo esto? ¿Por qué esta guerra? Porque el pastel cibernético es un pastel muy jugoso. Hay 3.500 millones de internautas en el mundo. Además, la economía digital, que está creciendo a pasos agigantados, ya supone el 15% del PIB mundial. No es de extrañar que ya se hayan sumado más de treinta países a la iniciativa de la Red Limpia de Trump; y todavía no sabemos cuántos se van a unir a la iniciativa de China.

Tal vez el mayor reto al que nos enfrentamos en este momento no sean las amenazas en el ciberespacio, como decimos en este seminario, sino las amenazas que desde la tierra vamos a llevar al ciberespacio, ya que Estados Unidos y China parecen decididos a construir un «Muro de Berlín digital», dividiendo por completo los dos sistemas digitales. El resultado será una bipolarización del mundo digital, una división del mundo en dos redes digitales totalmente distintas que nos va a obligar a todos decidir del lado de quién estamos. Ese espacio que hasta ahora era libre y abierto, parece que ahora se va a convertir en un espacio dividido.

Para aprender un poco más sobre la ciberpotencia china, tenemos con nosotros a tres expertos en la materia: uno en temas militares, otro en geoestrategia y otro en asuntos culturales.

Mario Esteban es investigador principal del Real Instituto Elcano y profesor titular del Centro de Estudios de Asia Oriental de la Universidad Autónoma de Madrid. Ha colaborado como analista sobre China con el Parlamento Europeo, con la Comisión Europea y con el Ministerio de Defensa y ha sido profesor invitado en la Universidad de Lenguas Extranjeras de Pekín y en la universidad finlandesa de Turku, además de investigador asistente en la Academia de Ciencias Sociales de China.

También nos acompaña Ignacio Ramos, que es profesor del Departamento de Relaciones Internacionales y delegado para Asuntos Chinos de la Universidad Pontificia Comillas. Ignacio ha vivido tres años en Taiwán y, como parte de su labor académica, ha pasado largas temporadas en la China continental. Actualmente es comisario del proyecto de la Unión Europea *2019-2020: Cultural Routes of Europe Itinerant Exhibition*, que es una exposición que recorre distintas ciudades chinas.

Finalmente, el Coronel Carlos Frías es doctor en Paz y Seguridad Internacional, máster en Estudios Estratégicos y colaborador habitual del Instituto Español de Estudios Estratégicos y del CESEDEN, el Centro Superior de Estudios de la Defensa Nacional, en temas estratégicos y de seguridad.

Sin más dilación, le cedo la palabra a Mario Esteban.

MARIO ESTEBAN
Investigador principal del Real Instituto Elcano y
profesor titular del Centro de Estudios de Asia Oriental
de la Universidad Autónoma de Madrid

Muchas gracias a los organizadores y gracias, Georgina, por la presentación. Lo primero que quiero decir es que hay dos aspectos que, aunque me parecen fundamentales, no voy a abordar,

pues entiendo que ya ha habido sesiones específicas sobre ellos y que, dado el perfil de algunos de los ponentes, en la próxima mesa también se les va a prestar atención. Me refiero a los ciberataques que llegan a España desde China, que ayer mencionó la directora del CNI, y a la desinformación, a la que estará dedicada la siguiente sesión. En cualquier caso, si alguien tuviese interés en el papel específico de China en estos temas, yo estaré encantado de abordar este tema en el turno de preguntas.

Como decía Georgina al referirse a la segunda parte del título de esta sesión, ese «sin control», cuando hablamos de China posiblemente el asunto sea que hay demasiado control del Estado. Aquí podemos contraponer, simplificando mucho, tres modelos o tres visiones sobre el mundo digital. La europea, concentrada en el individuo, en los derechos individuales; la norteamericana, en el que juegan un papel muy importante una serie de empresas con una clara vocación monopolística; y el de China, en el que el papel central es para el Estado, que entiende el ciberespacio como un ámbito para consolidar su poder y expandir su influencia a nivel internacional. En este sentido, el impacto a nivel interno que ha tenido en China el desarrollo del ciberespacio, del mundo digital y las nuevas tecnologías, en la relación entre el Estado y la sociedad, así como la influencia de China en el mundo, ha sido muy distinto al que mucha gente predecía en Occidente hace diez o quince años.

No voy a hablar de ciberataques ni de desinformación, que probablemente sean las dos amenazas más evidentes. Voy a usar un enfoque un poco distinto, centrándome en aspectos que teóricamente podrían ser de cooperación, que podrían ser una vía para la cooperación en relación con el ciberespacio entre Europa, España y China pero que sin embargo no lo son, o no lo son en gran medida, debido a diferencias normativas. Se debate ahora sobre hasta qué punto tenemos que entender nuestra relación con China en términos de valores, en términos ideológicos. Yo creo que es evidente que no podemos reducir la relación con China al debate ideológico, pero tampoco debemos obviarlo. Y creo que este tema concreto que estamos abordando, el ciberespacio, es un buen ejemplo.

Hablaba de teóricas vías de cooperación. Una en el ámbito económico y una segunda en la cooperación internacional. En el ámbito económico, como sabéis, en Europa los servicios sobre el ciberespacio los proveen empresas norteamericanas. Somos un mercado cautivo de empresas americanas. Hay pocas empresas europeas y son poco potentes en este campo. En ese sentido, las fuerzas norteamericanas tienen una fuerte vocación monopolística, por lo que teóricamente la entrada de empresas chinas debería generar una mayor oferta que, para nosotros, como consumidores, sería algo positivo. Además, como China y Europa compartimos ese objetivo de reducir nuestra dependencia de empresas norteamericanas en sectores tecnológicos sensibles, a priori podría haber sinergias, proyectos de financiación mutua, cooperación tecnológica, etcétera. Pero ¿qué sucede? Como decía antes, tenemos unas diferencias ideológicas muy grandes. Por un lado, en China hay una visión tecnonacionalista muy fuerte, como ha comentado Georgina. Las reglas del juego para las empresas europeas en China no son las mismas que para las empresas chinas en Europa. El mercado chino está mucho más cerrado y las empresas europeas sufren un tratamiento discriminatorio, mientras que las empresas chinas se benefician de una serie de apoyos y preferencias por parte del Estado. Además, el marco normativo favorece la apropiación de los datos de las empresas europeas en China. Las empresas europeas que operan en el país asiático tienen muchas más restricciones para mover sus datos fuera de China que en el caso inverso. Además, por la legislación vigente que también ha mencionado Georgina, en caso de exigencia por parte del Estado, teóricamente estarían obligadas a facilitar esa información que se les requiera.

El marco doméstico es claramente distinto. No sólo por esta cuestión legislativa, ya que no sólo es una cuestión de marco ju-

rídico, sino una cuestión sistémica más amplia. Todos sabemos cuál es la jerarquía en las relaciones entre el Estado y las empresas en China. Esto, lógicamente, genera preocupación sobre la confiabilidad a la hora de cooperar con empresas chinas. Y ahí se enmarca todo el debate en torno a Huawei y su papel en el despliegue de las redes 5G a nivel global.

Otro ámbito en el que teóricamente podría haber un margen para la cooperación sería en los países en vías de desarrollo, pues hay multitud de países que no tienen los recursos financieros y tecnológicos para desarrollar su propio espacio digital, para desarrollar su industria, servicios, tecnologías digitales, etcétera. Esto genera una brecha muy importante y dificulta que alcancen los objetivos de desarrollo sostenible de la Agenda 2030. Ahí China y Europa podrían cooperar con financiación o tecnologías conjuntas, o incluso mediante la unión de empresas europeas y chinas. Pero volvemos a la cuestión de los valores, volvemos a la cuestión de la forma de proceder. Lo vemos en el marco de la «Ruta de la Seda Digital», donde mucha de la financiación china se produce en términos que no son transparentes. Es financiación ligada a condiciones y en muchos casos los desarrollos tecnológicos que China ofrece están orientados al control social por parte de las autoridades. Lógicamente esto genera dificultades.

Más allá de estas dos áreas de posible cooperación teórica, pero frustrada, quería mencionar cómo, dentro de este modelo tecnonacionalista, que bien podríamos denominar tecnoautoritarista, el Gobierno chino está utilizando las nuevas tecnologías y el ciberespacio para aumentar el control social sobre la población. Esto genera dilemas interesantes también para nosotros. Lo que se está desarrollando por parte del Gobierno chino, o con el apoyo del Gobierno chino, son tecnologías muy invasivas contra la privacidad de la población, pero son tecnologías que también ofrecen servicios que facilitan la vida a la población. Aquí hay que hacer una reflexión profunda. Esto lo hemos visto, por ejemplo, en la lucha contra la COVID-19, donde se produce una cierta transacción entre privacidad y servicios, entre privacidad y eficacia en la labor del Estado. No podemos obviar este modelo que se está fraguando en China y tenemos que reflexionar sobre las implicaciones que esto puede tener dentro de Europa.

Quería compartir una última idea. Tenemos que ser conscientes de que los valores y las ideas son distintos en China y Europa. No sólo a nivel del régimen, no sólo a nivel de las autoridades, sino también en la población. Hay estudios al respecto, realizados por investigadores extranjeros desde fuera de China, que evidencian un gran apoyo entre la población china a todo este sistema de crédito social, a este sistema de transacción de privacidad a cambio de servicios. Termino con esta reflexión.

GEORGINA HIGUERAS
Moderadora

Gracias, Mario. Es tu turno, Ignacio.

IGNACIO RAMOS
Profesor de Relaciones Internacionales y delegado para Asuntos Chinos en la Universidad Pontificia Comillas

En primer lugar, decir que me siento muy honrado, y también muy contento, de haber sido invitado aquí a compartir mis conocimientos sobre China, como decía Georgina, desde un punto de vista más de tipo cultural, con el fin de intentar entender ese *background*, ese trasfondo, y qué cabe esperar tanto por parte del Gobierno chino como de la población. Y qué le cabe esperar a Occidente, en la medida en que este creciente globalismo en China es imparable. ¿Nos conducirá a una nueva Guerra Fría, como planteaba Georgina, o devendrá en un híbrido con las formas de vida de Occidente?

Lo primero que quería decir es que resulta fundamental tener este tipo de debates. Ayer, uno de los ponentes decía que

dentro de cuatro años este seminario se dedicaría a cierto tema. Yo me aventuro a predecir que tendremos que hablar más de China. Habrá que multiplicar las plataformas para que Occidente logre comprender más en profundidad a China e iniciar un proceso de diálogo, antes de sumirnos en una especie de guerra que nos sorprenda a todos en una actitud pasiva.

Mi punto de vista es que, efectivamente, China es una ciberpotencia con mucho control. Quisiera destacar, por complementar lo que ha dicho Georgina sobre la ley de seguridad, que a partir 2017 lo que se ha hecho en China es ligar cualquier acción relacionada con el mundo cibernético digital con la identidad real de los ciudadanos. Cuanto te descargas una aplicación en China, ésta te obliga a identificarte, incluso con una foto o con tu documento nacional de identidad.

Sabemos que China tiene un grave problema de divisas. Para evitar la falsificación –en la que son tan buenos históricamente– China no ha querido emitir billetes grandes. Con una economía que está creciendo mucho, su mayor billete es el de cien yuanes. No existen billetes más grandes que el de cien, que equivale a unos quince dólares. Si hay que hacer grandes transacciones con dinero en metálico, eso es un problemón. Por eso China no ha tenido más remedio que hacer la transición al pago digital. Ya nadie paga en metálico en China, ni siquiera para comprar un chicle. Casi todo el mundo paga con WeChat, con Alipay o con otra herramienta similar.

China ha dado muchos pasos, mucho más rápido que cualquier país de Occidente, en esta digitalización y encriptación de su modo de vida. El dinero es la institución que fundamenta una sociedad, así como la confianza mutua. China ha dado muchos pasos y lo ha hecho muy rápido. No es casualidad que en la carrera del 5G China ya haya llegado a un punto en el que está preparada para implementar una serie de cosas mientras Occidente se muestra temeroso y busca todo tipo de excusas –especialmente Estados Unidos– para frenar la implementación del 5G, porque Occidente sencillamente no está preparado. Recuerdo que el año pasado vino a España una señora alemana de una comisión de la Unión Europea para abordar las relaciones con China. Su mensaje era que nuestros amigos eran Estados Unidos y las razones que daba para ello eran básicamente culturales, filosóficas y demás. Hablaba de nuestros *partners*. Allí había gente de Siemens, de Ericsson, de sus superconductores... Pero la realidad es que, a nivel tecnológico, estas empresas están todavía muy por detrás de Huawei, por poner un ejemplo.

Lo principal es ligar la identidad personal con la identidad digital, algo que ha ocurrido ya en China, dando forma, por así decirlo, a una especie de médula espinal del sistema chino. El resultado es que todo está mucho más controlado. Cualquier movimiento, cualquier transacción económica, aunque sea de un yuan, queda registrada. Para eso China ha ido creando sus instrumentos, sus herramientas. Se hablaba ayer aquí de la necesidad de crear un mando de operaciones cibernético. Pues bien, China lo tiene desde hace varios años. La administración del ciberespacio es la que promulga estas leyes.

Me voy a centrar en la percepción de los chinos para acercar un poquito más esa cultura, ese magma sociocultural que conforma una quinta parte de la humanidad. Los analistas calculan que en el año 2024 China alcanzará en PIB a Estados Unidos; yo creo que, por la situación actual de pandemia, esto se puede producir incluso más rápido. En otro indicador como es la PPP, o Paridad de Poder Adquisitivo, China ya ha alcanzado a Estados Unidos. Y no sólo está creciendo China, sino toda Asia. *The Asian century is set to begin*. Es impresionante ver como, en tan sólo veinte años, el PIB se ha equiparado entre Asia y el resto del mundo. Debemos incluir a Japón, Corea del Sur, India…

¿Cómo percibe la población china, ese quinto de la humanidad, ese control? Yo lo equipararía a como un católico tradicional entiende a la madre iglesia. Hay una serie de dogmas que se entienden como puntos de no retorno. Es decir, si los pones en

cuestión se hunde todo el edificio. Esto no quiere decir que no haya habido un proceso para llegar hasta ahí, pero una vez que se alcanza un consenso histórico y éste se ratifica en una percepción compartida, eso ya pasa a formar parte de nuestro modo de vida, de nuestro dogma, de nuestra base.

¿Qué elementos tiene este dogma en China? Que el cibercontrol existe y todo el mundo se sabe observado. Y también la fe de que es efectivo, de que tiene un poder real. Por otro lado, no es excesivamente arbitrario, lo cual es muy importante para los chinos, que confían mucho en la inteligencia artificial, pues asumen que los algoritmos no son arbitrarios ni van en plan *ad hominem* a por una persona o un grupo. El cibercontrol es algo que afecta a contenidos no gratos para el Gobierno porque amenazan, sobre todo, la unidad nacional. Eso es lo que legitima este cibercontrol; y además protege de las falsificaciones y de los engaños entre los chinos.

Por eso, en China el cibercontrol es percibido fundamentalmente en términos de ciberseguridad. Imaginemos una ciudad cualquiera, de tamaño pequeño del centro de China –no hace falta que sea ni Beijing ni Shanghái– donde, cuando una persona se salta un semáforo en rojo la cámara la capta y, con una probabilidad del 99%, la reconoce. Después, en el sistema aparece el nombre completo de la persona, su género, las veinte cifras del código de su tarjeta SIM y su domicilio. Pues este sistema de crédito social en pruebas se está implementando ya en algunas ciudades chinas. Creo que hay un episodio de *Black Mirror* que habla de esto, de cómo la gente se vota, se puntúan unos a otros, y de esta forma su crédito social sube o baja, determinando si eres un buen ciudadano o no. Y luego eso te afecta en todo: si pides una hipoteca, si puedes optar o no a cierto trabajo… Esto se está implementando ya y lo importante es que la mayoría de los chinos lo perciben en términos de ciberseguridad; eso sí, siempre que sea el Estado el que controle, nunca corporaciones privadas. Los chinos son muy desconfiados por el maltusianismo

ambiental en el que viven, con esa idea de que los recursos son limitados y hay superpoblación, lo cual amenaza el orden social y es un factor de empobrecimiento. Los chinos desconfían de los otros chinos y reciben de buen grado este tipo de cibercontrol.

Con la COVID-19 hemos visto la eficacia con la que China, Corea o Taiwán han logrado controlar la pandemia, lo cual ha sido posible en gran medida gracias a estas tecnologías. Cuando lo que está en juego es la salud, ya no resulta tan fácil decir que no son útiles o que no las queremos.

Para terminar, quiero reiterar que tiene que haber mucho más debate sobre China, pues China es un socio necesario. Mientras que en Europa hay países como Francia que sienten que China es el gran superpoder, por delante de Estados Unidos, países vecinos de China, como Corea, piensan que la gran potencia es Estados Unidos. Lo mismo ocurre en Japón. Los que temen a China más de cerca proyectan un Estados Unidos más fuerte y poderoso. En cambio, en Europa, ese pensamiento crítico, y también un poco receloso de Estados Unidos, aunque sea nuestro socio inequívoco, hace que se perciba a China como superpotencia.

A donde quería llegar es a que China realmente es un socio necesario. Creo que las dos próximas generaciones de europeos no perdonarían que, por una especie de actitud de avestruz, esta generación no perciba a China como la superpotencia que es, porque el resultado sería nuestro empobrecimiento. Creo que no es tan sencillo como decir eso de que yo me subiré al 5G cuando Ericsson despliegue su tecnología, aunque pierda unos años de avance tecnológico. No es tan fácil. Quizá la mejor forma de controlar China sea entablando una relación de cooperación. Los chinos tienen muy clara la idea de negocio, con un concepto muy similar al *win-win*, al beneficio mutuo. Ése es su gran principio. Europa, en cambio, necesita explicitar más sus principios, o al menos ser fiel a su conciencia. En muchas ocasiones, Occidente necesita poner por delante el principio de respeto a la dignidad del individuo, mientras que China es una sociedad que pone por delante la dignidad histórica de la nación. Fuimos grandes, fuimos humillados y tenemos que volver al sitio que nos pertenece. Por tanto, no podemos ser segundos. Xi Jinping no diría «*China first*», pero sí diría «*China second to none*».

GEORGINA HIGUERAS
Moderadora

Gracias, Ignacio. Coronel, tiene la palabra.

CORONEL CARLOS JAVIER FRÍAS
Doctor en Paz y Seguridad Internacionales. Colaborador del Instituto Español de Estudios Estratégicos

Aprovechando la referencia histórica que ha hecho Ignacio, me gustaría empezar recordando que en China la historia tiene un peso muy grande. Para los chinos, para su visión del mundo, China siempre ha sido el centro, el país más avanzado, más rico y poderoso, con la excepción de un pequeño intervalo en los últimos doscientos años, donde Occidente ha ocupado este papel de forma ilegítima. Por eso, gran parte de la propaganda china trata de devolver China al lugar que le corresponde en el mundo, que es el centro, el primer puesto en todos los órdenes.

Esto es importante porque a partir de ahí China hace su propia lectura de la historia. En términos chinos, cada vez que el poder central ha sido débil, China se ha fragmentado y ha acabado en una situación de debilidad interna, incluso de guerra civil. Uno de los momentos más recientes en los que se produce esto es el siglo XIX, a raíz de la Guerra del Opio, cuando las regiones costeras empiezan a recibir una influencia occidental que debilita el poder central de China. Hay que entender que, geopolítica y militarmente, China es una especie de isla. China está rodeada por una serie de territorios a los que no tiene acceso y desde los que no se tiene acceso a China. La expansión de China desde su

núcleo originario, cuando Qin Shi Huang, el unificador, unifica los reinos combatientes en el año 221 a.C., ha abarcado todo el territorio posible, hasta alcanzar una serie de barreras naturales que impiden una expansión posterior. China llega hasta la cordillera del Himalaya, hasta las montañas del Cáucaso ya la enorme estepa de Siberia, que en aquel momento está helada, haciendo prácticamente insostenible la presencia humana, hasta el mar de Japón... China se expande pues hasta que ocupa todo el territorio que físicamente puede ocupar. A partir de ahí, China es autosuficiente. En su momento tiene una agricultura riquísima alrededor de Pekín, donde está la etnia Han, el centro de China y con mucha diferencia la zona más rica, donde se mantiene el poder central. Periódicamente sufre invasiones desde las estepas del Cáucaso, algo que resulta interesante desde un punto de vista militar ya que tribus mucho más pobres, mucho menos avanzadas y teóricamente mucho menos poderosas, invaden con regularidad al mayor y más poderoso Estado de la tierra, aunque ése es un tema para otro debate.

Como decía, para los chinos, la historia muestra que China siempre ha sido autosuficiente, siempre ha sido el país más avanzado, el más rico, excepto durante un pequeño intervalo de tiempo. Y ellos consideran que la marcha normal de la historia es retornar a esa situación. Es importante recalcar lo de su autosuficiencia. China no comercia fuera porque no ve la necesidad. De hecho, los primeros intercambios comerciales se hacen a través del Galeón de Manila, cuando desde la presencia española en Filipinas se empiezan a intercambiar productos que en la época eran muy exóticos, muy caros, para después llevarlos a Europa. Pero ése es un comercio puramente marginal. China es autosuficiente y no necesita nada de fuera. Y ese no necesitar a nadie es algo fundamental en gran parte de la historia china. ¿Por qué? Porque la globalización para China es un una circunstancia con la que se encuentra por sorpresa. China, en su momento, no promueve la globalización; casi se topa con ella sin darse cuenta.

Eso sí, se da cuenta de que está nueva situación es muy favorable y aprovecha ese tren que pasa. A partir del momento en el que empieza a integrarse en el comercio mundial, China desarrolla un modelo económico que se basa fundamentalmente en los salarios bajos. China tiene una enorme cantidad de mano de obra a un coste muy bajo. Por eso acaba convirtiéndose en la fábrica del mundo. Todos llevamos ahora mismo encima algo fabricado en China. Pero éste es un fenómeno muy reciente. Hace cuarenta años no era ni mucho menos así.

¿Qué importancia militar tiene todo esto? Pues que, por primera vez en la historia del país, China depende del comercio exterior. Hasta ahora eso no había ocurrido nunca. Hasta ahora el ejército chino se dedicaba a repeler invasiones de los mongoles o a lidiar con vecinos mucho menores, peor armados y peor equipados. China no tenía un problema de seguridad hasta que pasó a convertirse en una potencia exportadora, pero a partir de ese momento necesita importar una gran cantidad de recursos que no tiene para alimentar sus fábricas. China es un país inmensamente rico en todos los órdenes, pero no lo suficiente como para abastecer a todo el mundo. Con lo cual China se encuentra ahora en una situación en la que depende de una serie de proveedores y de clientes, así como de unas vías de tráfico fundamentalmente marítimas. Eso ha generado una serie de problemas. Primero, las regiones costeras, que no son regiones que pertenezcan al núcleo central de la etnia Han, de repente se han enriquecido mucho, pues la mayoría de las fábricas exportadoras de China se asientan en regiones costeras, cerca de los puertos. Con lo cual zonas tradicionalmente marginadas del poder central chino se convierten en regiones muy ricas donde empieza a surgir una clase social de propietarios con un poder adquisitivo muy alto. Esto plantea una primera amenaza para ese poder central fuerte que garantizaba la estabilidad de China. De ahí que una de las primeras prioridades del Gobierno chino sea mantener la fortaleza del poder central. Y en esta ocasión lo hace a través del

Partido Comunista. Luego podemos entrar un poco más a fondo en cómo lo está haciendo Xi Jinping.

El segundo punto es que, por primera vez en su historia, China necesita una flota potente para garantizar la entrada de recursos y la salida de sus exportaciones. Si uno observa la geografía china, ve que tanto el Mar de China Oriental como el Mar de China Meridional están cerrados por una cadena de islas. Es decir, China tiene grandes clientes, tiene grandes proveedores, pero la puerta de entrada y la puerta de salida están controladas por una serie de islas que no dominan, en un mar que, fundamentalmente, está en manos de la flota norteamericana. China se encuentra pues en una situación en la que su prosperidad depende de mantener buenas relaciones con Estados Unidos.

Durante muchos años, China siguió siendo una nación relativamente pobre, una nación en vías de desarrollo, cosa de la que se ha aprovechado y de la que se sigue aprovechando. China se ha beneficiado de relaciones comerciales asimétricas, en el sentido de que se ha dado muchas ventajas a las empresas chinas mientras que las empresas europeas o norteamericanas han encontrado muchas trabas dentro de China. Todo esto era posible porque se aducía que China era un país en vías de desarrollo al que había que ayudar a levantarse. Ahora, China sigue intentando jugar la carta de que es un país en vías de desarrollo cuando claramente ése ya no es el caso. No obstante, China sigue jugando esa carta para defender esa asimetría de normas, tanto interna como externa.

Como decía, China necesita poder asegurar sus fuentes de suministro y garantizar sus vías de exportación, lo cual explica que necesite unas Fuerzas Armadas mucho más competentes que las que tenía hasta ahora. Además de eso, sabiendo que llegar a competir con la fuerza naval norteamericana es prácticamente imposible a corto y medio plazo, y dudoso a largo plazo, China intenta buscar nuevas vías exportación. En gran parte, la iniciativa de la nueva ruta de la seda viene dada por la necesidad de

buscar vías de comunicación alternativas a las navales que garanticen sus suministros y exportaciones, sin depender de la buena voluntad de la flota norteamericana

De todo esto podemos extraer dos elementos clave: que China por primera vez en su historia depende del exterior, lo cual nunca había sucedido, por lo que es una situación nueva para ellos, y, en segundo lugar, que China considera que depender del exterior y recibir influencias exteriores supone una amenaza a la estabilidad interna del régimen y, por tanto, a la de China.

¿Cómo lidia con estas dos situaciones? La parte cíber, que es de lo que estamos hablando hoy, está ligada a estas dos ideas. En primer lugar, a mantener la estabilidad interna. Como hemos visto, China ha desarrollado un sistema de control muy importante para que la población tenga la seguridad de que el Gobierno está encima de ellos. El resultado es que la opinión pública en China no es una opinión pública anónima, sino que tiene nombres y apellidos. Como nos ha contado Ignacio, al que se salta un semáforo en rojo lo tienen identificado inmediatamente. Qué decir de un comentario crítico relacionado con el Gobierno o un mensaje que de alguna manera no le guste a las autoridades. El control interno es pues un elemento fundamental para China.

Hay un segundo elemento que también es fundamental. El hecho de que el modelo económico de China esté basado en los salarios bajos, pues ese modelo muere conforme suben los salarios. En un momento determinado, China empezará a no ser competitiva con respecto a países que tienen costes de mano de obra incluso más baratos, ya hablemos de India, Indonesia o Malasia; hoy en día siempre hay alguien dispuesto a trabajar por menos. China sabe que su modelo económico tiene un recorrido limitado y que tiene que cambiar urgentemente de modelo. Pero, además, China tiene otra serie de elementos que hacen que sus perspectivas económicas puedan verse amenazadas. Uno de los más importantes, aunque no el único, es la demografía. Hacia el año 2030, gracias a la política de hijo único que se implementó

en los últimos años del comunismo, China va a perder una cantidad de población importante, que además será una población en edad de trabajar, pues las generaciones actuales, que son muy numerosas, van a entrar en edad de jubilación. El sistema de pensiones chino no es como el nuestro. Prácticamente sólo cotiza para las pensiones la población urbana. La mayoría de la población china, incluida la población rural que vive en ciudades gracias al sistema del censo, no tiene derecho a prestaciones sociales. En otras palabra, no va a cobrar pensión alguna. De ahí que sea posible que acaben en el modelo que los demógrafos denominan 421, en el que un trabajador tiene que mantener a sus dos padres y a sus cuatro abuelos. Eso es insostenible y China sabe que hacia el año 2030 va a empezar a ocurrir. Ésa es la ventana de oportunidad que tiene Xi Jinping para cambiar su modelo económico. A partir de ese momento, es muy difícil que China pueda mantener el modelo de salarios bajos, porque con un modelo de salarios bajos esa pirámide poblacional es insostenible. ¿Qué modelo puede ofrecer Xi Jinping a China?

Vamos a ver otro factor importante: el control interno. El comunismo, desde que cayó la Unión Soviética, ha constituido un fracaso en todos los países donde se ha implantado. China es una excepción, porque tiene este comunismo de Estado, pero sigue siendo un sistema comunista cerrado, con muy pocas libertades, donde el ciudadano tiene que permitir que el Gobierno entre hasta el fondo en lo que hace, en lo que no hace, en lo que compra, en lo que deja de comprar, etcétera. El ciudadano permite esto fundamentalmente porque está en una etapa de crecimiento económico del 6, 7 u 8% anual; aunque las estadísticas chinas hay que cogerlas con mucho cuidado. Aun así, es un crecimiento económico importante. El ciudadano ve que cada año vive un poco mejor, que las cosas mejoran, que cada año tiene más ingresos, que cada año hay mejores infraestructuras… En suma, el ciudadano está dispuesto a cambiar parte de su libertad por ese progreso continuo que parece que le ofrece el sistema comunista. O, por decirlo de otra manera, la legitimidad del sistema comunista, y por tanto del poder central chino, está basada en una situación económica favorable. Si esa situación económica se complicara o si llegara una crisis, la legitimidad del Gobierno comunista quedaría en entredicho. Con lo cual Xi Jinping no se puede permitir el lujo de que se produzca dicha crisis. Esto es como un señor que va en bicicleta: mientras vaya pedaleando, no se cae, pero si la bicicleta se para, se cae. Eso es lo que le ocurre al Gobierno chino. Tiene que mantener un crecimiento económico importante. Y se encuentra con que su modelo económico está en vías de agotamiento.

¿Qué puede hacer? Lógicamente, el único modelo económico que puede resistir en el tiempo es uno que esté basado en una economía innovadora y tecnológicamente avanzada, una economía que ofrezca servicios que no puedan ser reemplazados por los de un país con mano de obra más barata. China necesita transformar su modelo productivo, necesita ir hacia una economía basada en el conocimiento. Y necesita hacerlo al mismo tiempo que mantiene la estabilidad del sistema y evita las disensiones internas dentro de su población. Ése es un *sudoku* muy difícil de cuadrar pues fundamentalmente lo que implica es que China tiene que conseguir adelantar a Estados Unidos en materia de tecnología. El reto, desde luego, no es menor.

China ahora mismo es un país que tiene hambre de información, un hambre desesperada, porque sabe que el tiempo corre. El tiempo pasa y va en contra de su modelo económico, con lo cual necesita toda la información posible para desarrollar una tecnología propia tan potente que sea capaz de superar en un plazo de tiempo breve a Estados Unidos. De ahí que la inmensa mayoría de chinos que se encuentran fuera de su país lo graben todo, lo recojan todo, lo analicen todo, obteniendo diariamente terabytes de información que van a China.

Por otra parte, no hay que olvidar que una empresa china no es una empresa europea ni una empresa norteamericana. Como

hemos dicho, la prioridad de China es el Estado. Las empresas chinas son instrumentos del Estado y, como tales, sirven a ese proyecto de convertir la economía china en una economía innovadora en un plazo de tiempo breve. La función de una empresa occidental es ganar valor para sus accionistas. En cambio, una empresa china sirve al proyecto de reforma de la economía que marca el Estado chino. De ahí que las empresas chinas estén tan involucradas como cualquier otra institución estatal en esa recopilación de información con la que se busca mejorar el nivel tecnológico chino.

¿Qué implicaciones tiene todo esto? Vamos ahora a lo que nos ocupa, a los ciberataques. Como hemos visto, la inmensa mayoría de la actividad que tiene lugar en el ciberespacio chino tiene dos funciones: controlar a la población, algo que es fundamental para mantener la estabilidad de China, y recoger toda la información posible, con el objetivo de que China sea capaz de reformar su economía. Esto nos lleva a una serie de conclusiones. Hace cincuenta años, la vanguardia tecnológica era la tecnología militar. Internet fue un invento militar; el GPS, fue un invento militar. Muchas empresas funcionaban con presupuestos militares en productos de utilidad militar que luego se han revelado de utilidad civil. Ahora ése ya no es el caso. Ahora la inmensa mayoría de la tecnología se produce en empresas civiles. Las Fuerzas Armadas beben de esa tecnología pero ya no la generan ellas. De ahí que los objetivos de los ciberataques chinos ya no son las Fuerzas Armadas occidentales ni las instituciones del Estado, sino las empresas privadas con recursos tecnológicos. Tanto el Estado como las empresas chinas no tienen como función atacar a España. Su función es conseguir la información que puedan tener empresas españolas que puedan favorecer los intereses chinos. Y eso sin duda tiene implicaciones a la hora de la ciberdefensa, que deja de ser una cuestión estatal y se convierte mucho más en una cuestión de qué puede hacer cada empresa privada para proteger su información, que representa también su

ventaja tecnológica. Esto tiene un efecto enorme en el conjunto de las naciones. Que nosotros tengamos un Mando del Ciberespacio y que intentemos evitar ese tipo de ataques tiene una función desde el punto de vista del Estado pero, al final, esto es un problema que va a afectar fundamentalmente a las empresas privadas y, sobre todo, a las empresas tecnológicas.

¿Qué va a hacer China? ¿Realizará China ciberataques ofensivos con la idea de perjudicarnos a nosotros? Es posible que así sea, porque ahora mismo un ciberataque permite dañar a tus enemigos sin necesidad de iniciar una guerra abierta; y cuanto más interconectados estemos, mayor será el daño.

Hay una zona gris. Digamos que entre el negro, que sería una guerra abierta y declarada, y el blanco, que es una paz en la que todos somos amigos y aliados, existe una enorme gama de grises. Los ciberataques están localizados en algún punto de esa gama de grises. Si nosotros, o cualquier otro país, hace un gesto, una política, o lo que sea, que China considere que va en contra de sus intereses, ellos podrían responder con un ciberataque que perjudique nuestros intereses. No sólo contra España como país. El ciberataque puede estar dirigido a cualquier empresa privada española que haga una inversión que al Estado chino no le guste.

Los ciberataques tienen una particularidad. China, como hemos visto, tiene a dos millones de personas dedicadas a la ciberguerra. Dos millones son muchos millones. La cantidad de recursos que pone a su disposición es enorme. Y China puede focalizar esa enorme cantidad de recursos, instantáneamente, en un solo punto. Y cuando digo un solo punto no me refiero a España sino a una empresa española en particular. Si es necesario, China tiene la capacidad de concentrar todos los ataques de esos dos millones de personas sobre un solo foco, instantáneamente, de un día para otro. Con el agravante de que va a dejar el rastro que quiera dejar y el rastro que nosotros queramos admitir. Las posibilidades de defensa que tenemos contra un poder cibernético así son muy limitadas. ¿Puede un Estado occidental respon-

der de forma agresiva contra China aunque no tenga todas las garantías de que China está detrás un ciberataque? ¿Nuestros intereses se verían afectados tan gravemente como para responder militarmente, políticamente, económicamente o con un bloqueo o lo que sea, a un ciberataque chino? Son preguntas muy difíciles. Sin embargo, China tiene la capacidad de mandarnos un mensaje muy potente con sus ciberataques: «Esta política no me gusta. No estoy de acuerdo con esta medida…».

El ciberataque tiene muchas funciones. Su función fundamental es conseguir información, pero su segunda función es servir como instrumento de la política exterior china, que así nos manda información sobre qué medidas de las que tomamos o podemos tomar van a en contra de sus intereses. En los ciberataques, tanto como el daño que nos pueden hacer, es importante conocer a qué razones obedecen y qué nos quiere comunicar el Gobierno chino a través de esos ciberataques.

No hay que olvidar que, como decía Ignacio, China no es una potencia sin control. Al revés. Es una potencia controladísima. Los que somos una potencia sin control somos nosotros, Occidente, que *hackers* que hoy entran en un banco están mañana en el Ministerio de Defensa… La falta de control está aquí pues vivimos en una sociedad libre donde hay una serie de actores que, efectivamente, no tienen control alguno. En China ése no es el caso. Cuando se produce un ciberataque chino, detrás está el Gobierno chino. Es muy difícil que haya un ciberataque que no esté autorizado por alguna instancia del Gobierno chino. No olvidemos que China es una quinta parte de la humanidad. Hay muchos niveles de Gobierno y hay muchos niveles de control.

Sin embargo, como decía al principio, Xi Jinping es consciente de que, cuando China no ha tenido un Gobierno central fuerte, se ha debilitado. De ahí que una de las medidas que ha tomado Xi Jinping sea centralizar el poder. Como también hemos visto antes, la Comisión Militar Central es la que controla las Fuerzas Armadas chinas, que no pertenecen al Estado chino sino

al Partido Comunista. Xi Jinping se ha encargado de subrayar eso varias veces. Por ejemplo, el equivalente a la Guardia Civil en China, la llamada Policía Popular Armada, antes dependía del ejército chino y de los gobernadores regionales, pero Xi Jinping ha centralizado todo el control de la Policía Popular Armada en la Comisión Militar Central, que además ha reducido de tamaño y cuyos puestos ha copado con gente de su confianza. Xi Jinping es mucho más líder que sus predecesores, en el sentido de que ha llenado el Partido Comunista de gente que le es leal. Ha centralizado el poder y se mantendrá en él todo el tiempo que quiera, porque ahora mismo no hay nadie que pueda hacerle oposición desde dentro. Ha puesto hombres suyos en el servicio de información, ha puesto hombres suyos en seguridad pública y ha puesto hombres suyos en las Fuerza Armadas. Ahora mismo, el poder central en China es mucho más fuerte de lo que lo ha sido en mucho tiempo y está centralizado alrededor de Xi Jinping. Teniendo en cuenta que los ciberataques son un arma muy poderosa y que son un elemento fundamental para mantener esa estabilidad interna, todo lo que sean cibercapacidades están centralizadas y dependen de una manera más o menos directa del presidente Xi Jinping.

Resumiendo, las cibercapacidades chinas responden a necesidades que son constantes, inherentes y profundamente arraigadas en la historia de China. Necesitan mantener la capacidad de control sobre su población, porque cualquier escisión interna lleva a la inestabilidad, que históricamente los ha llevado incluso a la guerra civil. Por otro lado, los ciberataques dirigidos al exterior tienen como misión ayudar en el enorme empeño que tiene China por conseguir una economía tecnológicamente a la vanguardia del mundo en un período muy corto de tiempo. Es previsible que, conforme pase el tiempo, China cada vez tenga más prisa por alcanzar ese objetivo. Y eso quiere decir que es previsible que cada vez haya más ciberataques chinos, buscando información, buscando tecnología, intentando mejorar el nivel téc-

nico de sus empresas... Del mismo modo, en caso de que las políticas exteriores de los países europeos –o de determinadas empresas– vayan en contra del interés de China por mantener a su población aislada de la política interna, se verán obligados a emplear sus capacidades cíber para contrarrestar nuestras políticas o para mostrarnos su descontento con ellas.

Yo creo que la actividad cíber de China va a ir *in crescendo*, que va a ir creciendo cada vez más. Hasta ahora la globalización, sobre todo la globalización de protocolos, de sistemas de comunicación y de formas de entendernos, ha sido muy amplia. Ahora mismo, con mi teléfono móvil, aterrizo en Pekín, activo el *roaming* y puedo hablar con mi casa, porque utilizamos protocolos comunes. Pero para llegar a esos protocolos comunes, las empresas tienen que intercambiar información y ese intercambio de información se producía, básicamente, porque había unas normas de respeto a las patentes. Yo le doy información al otro para que podamos construir un sistema común, pero él va a respetar mi propiedad intelectual. Pero, claro, si no respeta mi propiedad intelectual, no le voy a dar esa información. Y China tiene merecida fama de no respetar la propiedad intelectual. De ahí que las empresas occidentales sean cada vez más reacias a compartir información con empresas chinas, sobre todo conscientes como son de que las empresas chinas están buscando aprovechar esa información. El riesgo de que al final acabemos teniendo dos familias tecnológicas separadas y escasamente compatibles es por tanto real. Es muy posible que acabemos teniendo por un lado una familia de empresas norteamericanas y, por otro, una familia tecnológicamente chinas y que yo, al final, en vez de ir con mi teléfono a todas partes, tenga que llevar dos, uno para hablar en Estados Unidos y otro para hablar en China. Europa ya veremos en qué lado queda. Ése es un riesgo patente. Y si China sigue manteniendo su política de absorber toda la información que pueda, de no respetar patentes, de ciberespionaje, etcétera, ese riesgo cada día estará más cerca.

GEORGINA HIGUERAS
Moderadora

Gracias, Coronel. Vamos a dar paso a las preguntas por *streaming*. Ana Guerrero pregunta si existe el riesgo en España de que un modelo mejor de ciberseguridad pueda ir en detrimento de los derechos fundamentales.

MARIO ESTEBAN
Investigador principal del Real Instituto Elcano y
profesor titular del Centro de Estudios de Asia Oriental
de la Universidad Autónoma de Madrid

En una sociedad democrática al final esperamos que el modelo que adoptemos dependa de lo que nosotros decidamos. El modelo chino exige sacrificar ciertos valores, aunque redunde en una mayor eficacia en relación a ciertos servicios. Esto nos genera un desafío importante: conciliar eficacia en la seguridad y en la provisión de servicios con el mantenimiento de los derechos individuales. Ésa es la pelea en la que estamos.

GEORGINA HIGUERAS
Moderadora

Pedro González, de *Atalayar*, pregunta: «¿Creéis que la UE logrará suficiente autonomía como para sacudirse las presiones de Estados Unidos y establecer una cooperación con China?».

IGNACIO RAMOS
Profesor de Relaciones Internacionales y delegado para
Asuntos Chinos en la Universidad Pontificia Comillas

Éste es un tema muy candente, que está muy abierto. Creo que ahora mismo la tendencia que está ganando el partido es más

proamericana y antichina, por así decirlo. Pero también creo que, a lo mejor, esa tendencia no es tan sostenible como parece y que de aquí a dos años puede cambiar las cosas, fundamentalmente por el tema de la batalla del 5G pero también por la vacuna de la pandemia. En principio va a haber muchas vacunas efectivas, pero los chinos llevan ya un mes aplicando una vacuna a su población civil. Ya han vacunado a cientos de miles de personas en el ámbito sanitario, en el ámbito diplomático… En el ámbito militar llevan ya incluso más tiempo vacunando. Yo creo que la pandemia nos tiene que ayudar a lograr ir más a fondo en las interpretaciones que hacemos de los datos.

GEORGINA HIGUERAS
Moderadora

Otra pregunta: «¿Cómo se podrían considerar las relaciones cibernéticas entre Rusia y China?».

CORONEL CARLOS JAVIER FRÍAS
Doctor en Paz y Seguridad Internacionales. Colaborador del Instituto Español de Estudios Estratégicos

Las relaciones cibernéticas entran dentro del marco de las relaciones generales entre Rusia y China. Aunque ahora mismo ambas naciones están muy próximas entre sí, eso es el resultado de lo que en relaciones internacionales se llama «equilibrio de poder». Rusia y China ven a Estados Unidos como un adversario y por eso coordinan sus políticas para oponerse a la potencia más fuerte del sistema, que es Estados Unidos. A la larga, Rusia y China tienen muchos motivos para tener fricciones entre sí, fundamentalmente por la cuestión de Siberia. Por un lado, tenemos una Rusia con una población decreciente, una población que además tiene muchos problemas de crecimiento, y por otro lado, en Siberia el cambio climático va a hacer accesibles muchos recursos que antes eran inviables. Y China no sólo necesita esos recursos si quiere mantener su economía sino que, además, tiene una población que todavía está en expansión; aunque, como he explicado antes, en unos años ese crecimiento se va a frenar. En todo caso, Rusia y China van a tener diferencias importantes en el futuro. Ahora mismo la tecnología rusa, en términos cíber, es una tecnología avanzada, pero probablemente menos que la china. China no necesita a Rusia.

GEORGINA HIGUERAS
Moderadora

Hay varias preguntas referidas a la Unión Europea. Dice Juan Cuesta: «El Parlamento Europeo ha pedido a la Comisión la diversificación de proveedores y una estrategia conjunta para disminuir la dependencia de Europa de la tecnología de ciberseguridad china, pero también de la estadounidense. ¿Es ésa una posición viable o un brindis al sol? ¿Se puede ser no alineado en esta nueva Guerra Fría tecnológica?». Y otra pregunta sobre Europa: «¿Estamos abocados a vivir bajo el dominio tecnológico de China o de Estados Unidos? ¿Qué papel tiene Europa? ¿No hay opciones para una soberanía digital europea?».

MARIO ESTEBAN
Investigador principal del Real Instituto Elcano y profesor titular del Centro de Estudios de Asia Oriental de la Universidad Autónoma de Madrid

Yo creo que la autonomía estratégica debe ser un objetivo para la Unión Europea, pero hay que trabajar desde hoy para alcanzar ese objetivo lo antes posible. Es evidente que no es algo que vayamos a poder alcanzar a corto plazo, pero se deben empezar a tomar medidas en esa dirección. Se está trabajando en la construcción de un mercado digital europeo, se está hablando de una

política industrial que pueda apoyar determinados sectores, de inversiones muy específicas para determinadas tecnologías… El objetivo es ése. Lógicamente, hasta que lleguemos ahí no vamos a ser equidistantes y está claro que vamos a estar mucho más alineados con Estados Unidos que con China, por intereses, por valores, etcétera. Pero creo que no hay que plantear esto como un todo o nada. El hecho de que hoy no seamos autónomos estratégicamente no quiere decir que no podamos y debamos avanzar en ese camino.

GEORGINA HIGUERAS
Moderadora

Gracias a todos. Gracias a los que nos están viendo en *streaming* y a todos ustedes por estar aquí hoy.

8. LA POLÍTICA DE LA DESINFORMACIÓN: LA MENTIRA QUE MATA

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

CARMEN ROMERO
Subsecretaria general adjunta de Diplomacia Pública de la OTAN

GENERAL FRANCISCO JOSÉ DACOBA
Director del Instituto Español de Estudios Estratégicos (IEEE)

Moderador
RAFAEL PANADERO
Jefe de Internacional de la Cadena SER

María Elena Gómez Castro, Rafael Panadero,
el General Francisco José Dacoba y Carmen Romero

Una de las maneras más efectivas de desestabilizar un país es mediante la proliferación de mensajes e informaciones falsas, orquestadas estratégicamente para polarizar a la sociedad o fomentar populismos en su seno. Estos abusos resultan corrosivos para los valores democráticos y son susceptibles de debilitar instituciones u organizaciones internacionales como la Unión Europea o la OTAN.

La crisis provocada por la pandemia ha puesto de relieve, además, la facilidad con la que se pueden difundir a la velocidad de la luz falsedades peligrosas. En palabras del Alto Representante para la Política Exterior y de Seguridad Común de la UE, Josep Borrell: «En estos tiempos del coronavirus, la desinformación puede matar». La mentira interesada supone una amenaza y podría estar reclamando una adaptación de los roles asignados a los medios informativos, a las Fuerzas Armadas, a las empresas y a los servicios de inteligencia. ¿Qué estamos haciendo para combatir la desinformación interesada y desinteresada?

RAFAEL PANADERO
Moderador

Vamos a empezar con esta última mesa antes de la intervención que cerrará el seminario. Esta mesa se convoca bajo el título «La geopolítica de la desinformación: la mentira que mata». Dado que estamos en un seminario organizado por una asociación de periodistas, parece muy oportuno el título porque la prensa, los medios de comunicación, siempre han mentido. No digo que toda la prensa o todos los medios hayan mentido, sino que siempre ha habido medios de comunicación que han mentido y, como dice el párrafo que introduce también esta mesa, mandar mensajes e informaciones falsas –que eso es, en definitiva, mentir– es una de las maneras más efectivas de desequilibrar a un país.

Lo que ocurre es que esto tampoco es un fenómeno nuevo ni reciente. Está de actualidad pero es un fenómeno antiguo; seguro

que todos tenemos varios ejemplos en la cabeza. Voy a citar uno muy conocido, muy antiguo, pero que creo que es muy significativo y que está muy conectado con el tema de esta mesa. Es el hundimiento del *Maine*, el acorazado estadounidense, en la bahía de La Habana en el año 1898, que llevó a que Estados Unidos declarara la guerra a España. De ahí surgió el famoso «más se perdió en Cuba». Nunca se pudo probar si aquello fue un ataque o si fue un accidente. Parece que fue un una explosión fortuita desde dentro del barco, pero la prensa estadounidense no quiso verlo así. En aquel momento, donde sí que había una guerra era entre la prensa de Estados Unidos, entre dos magnates, Randolph Hearst y Joseph Pulitzer, y aquella explosión nos dejó titulares del tipo «El acorazado *Maine* fue dividido en dos por una máquina secreta infernal del enemigo». Ya no se hacen titulares así. «Esperaron a la noche para lanzar la mina, después de que todos los hombres se retirasen a dormir, y todo el país vibra con fiebre de guerra». Efectivamente, es lo que buscaban: una guerra. Ese acontecimiento nos dejó noticias falsas como, por ejemplo, las del periódico de Pulitzer, que dijo que los oficiales españoles habían estado brindando tras la explosión, cuando parece que en realidad estuvieron intentando rescatar supervivientes. También nos dejó frases legendarias, como la que le dijo Hearst al dibujante que había mandado a La Habana para ilustrar todas las informaciones, que cuando vio que aquello estaba muy tranquilo y que no iba a haber guerra le escribió y le dijo: «Esto está muy tranquilo. Aquí no se va a dar una guerra. Me quiero volver». Y Hearst le respondió con una frase que también encaja muy bien con esta mesa: «Usted ponga los dibujos que yo ya pondré la guerra». Y, efectivamente, hubo una guerra. Y hubo también un aumento en las ventas de periódicos, que pasaron, en su caso concreto, de vender unos 400.000 periódicos a vender más de un millón.

Así que siempre ha habido mentiras. Siempre ha habido medios que han mentido con el objetivo de desestabilizar países. En-

tonces, ¿qué ha cambiado ahora? ¿Por qué incluimos esta mesa en este seminario de la Asociación de Periodistas Europeos? Porque éste sigue siendo un tema de actualidad, creo que por dos factores que compartiremos luego en la mesa. Creo que la crisis de la prensa, de los medios independientes –que también los ha habido siempre–, está afectando mucho. Ahora cuesta más ocupar huecos, llenar espacios. Y, en paralelo, tenemos las redes sociales, el fenómeno de internet que llena esos espacios. Las redes tienen capacidad para difundir más información y de manera más rápida y, por lo tanto, la capacidad de influir más y de una manera más contundente y efectiva en las opiniones públicas.

El resultado de todo esto es un nuevo escenario en el que nos tenemos que recolocar y redefinir todos: los gobiernos, las Fuerzas Armadas, las instituciones, los medios de comunicación... Ése es un poco el objetivo de esta mesa: hablar y debatir qué nuevo rol tenemos que jugar todos los actores implicados.

Decía ayer Miguel Ángel Aguilar que hubo un momento, antes de estos seminarios, en el que los periodistas veíamos a los militares como golpistas; y ellos… digamos que tampoco nos veían bien. Eso ha ido evolucionando y quizás este nuevo escenario de desinformación y de mentiras nos esté dando una nueva oportunidad para seguir redefiniendo estos papeles, esta relación. Ésta es la pregunta que nos vamos a hacer en esta mesa. Para responderla y para conversar sobre este asunto vamos a hacer una ronda inicial con los ponentes. Después abriremos una ronda de preguntas, tanto de quienes están aquí de forma presencial como de los que nos están siguiendo por *streaming*.

Tenemos la suerte de contar en primer lugar con María Elena Gómez Castro, Directora General de Política de Defensa. Es abogada, pertenece a la carrera diplomática y, antes de esto, ha sido muchas cosas que voy a intentar resumir: consejera de la Representación Permanente de España en la Unión Europea; experta en cuestiones de defensa en el Consejo de la Unión; asesora para Asuntos Internacionales de la ministra de Defensa; sub-

directora general de Seguridad en Exteriores; y representante permanente adjunta ante el Consejo del Atlántico Norte, el principal órgano de decisión de la OTAN. Desde 2017, como decía, es DIGENPOL, que es el órgano directivo que se encarga de planificar la política de defensa y coordinar la participación de España en organizaciones internacionales de seguridad.

Señora Gómez Castro, cuando quiera.

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

Muchísimas gracias. Buenos días a todos. Permítanme comenzar agradeciendo a la Asociación de Periodistas Europeos la amabilidad de haberme invitado un año más a participar en un seminario que siempre resulta del máximo interés para la labor de los periodistas, sí, pero también para la labor de quienes nos dedicamos a la seguridad y la defensa.

Hoy quisiera hablarles de varias cosas fundadas en libros que he leído y en las reflexiones que tenemos en las organizaciones internacionales, estructuradas en el contexto actual. Me refiero a la desinformación y la posverdad, a las nuevas guerras y las culturas de seguridad, a la respuesta y la responsabilidad y, finalmente, a asuntos vinculados también a la utilidad de la defensa.

Creo que, cuando llegamos a los cincuenta años, todas las generaciones tenemos la misma percepción de la siguiente generación, que es que han cambiado la historia por la anécdota y la reflexión por la emoción. Y eso, que es una constante, en el caso actual se multiplica exponencialmente debido a las nuevas tecnologías. Hoy nos sentamos aquí muchos analógicos y algunos digitales. Y esos digitales, que son los que Michel Serres llamaba los Pulgarcitos y las Pulgarcitas, en referencia a cómo manejan los teléfonos y se comunican, tienen una vida totalmente distinta a la de nuestra generación. Y también tienen una manera de adquirir el conocimiento diferente al nuestro, con modelos que

no somos capaces todavía de aprehender bien y, por lo tanto, donde reina el desconcierto. Sobre todo, creo que se ha quebrado el principio de autoridad, que es lo que las sucesivas generaciones hasta ahora sí habíamos tenido.

El conocimiento ya no se encuentra en grandes libros consolidados, sino que se encuentra en la red. Cuando en el colegio o en la universidad había que hacer trabajos, recurríamos a las grandes enciclopedias; siendo Espasa la mejor. Durante la universidad era la biblioteca de la Facultad de Derecho. Ahora hay una cosa que se llama «El rincón del vago» donde uno puede encontrarlo todo. No se sabe muy bien si es lo que verdaderamente tendría que ser pero, en todo caso, hay una manera fácil de adquirir cierta información para después proyectarla.

Los que somos analógicos y tenemos más de cincuenta años vivimos la Guerra Fría y, por lo tanto, nuestra sensación del peligro, del bien y el mal y de la amenaza es algo que llevamos de forma intrínseca. Muy suavizada, lógicamente, porque desde entonces no ha habido ninguna guerra, al menos que afectara directamente a Europa. Por lo tanto, esa sensación de amenaza es ahora menos presente, menos fuerte, de lo que fue en el pasado.

Las nuevas tecnologías han cambiado radicalmente nuestro mundo, han cambiado cómo adquirimos el conocimiento y cómo lo manejamos. Decía Ortega que hay tantas realidades como puntos de vista y que el punto de vista crea el panorama. Y eso lo decía hace muchos años sin que hubiera internet. Hablaba Ortega de los periodistas y de cómo proyectan las realidades. Pero es verdad que hoy, además de eso, hay lo que Zygmunt Bauman llama la «cultura líquida». Según Bauman: «La cultura líquida moderna ya no siente que es una cultura de aprendizaje y acumulación. A cambio, se nos aparece como una cultura del desapego, de la discontinuidad y del olvido. La cultura de la modernidad líquida ya no tiene un populacho que ilustrar y ennoblecer, sino clientes que seducir». Y eso es lo que ocurre hoy día en la red, donde hay una continuidad de clientes que seducir. Los titu-

lares más llamativos son los que obtienen más clics. Muy frecuentemente, esos titulares no se corresponden con el contenido que luego leemos, pero en todo caso ya tienen un clic y, por lo tanto, tienen más popularidad.

Henry Kissinger cree que esta revolución tecnológica, internet, quizá suponga el fin de la ilustración. Él dice que hay una acumulación y una manipulación de datos que impide la introspección –de nuevo reflexión frente a emoción, como les decía antes– y que los políticos –y éste quizás sea uno de los elementos más importantes– ya no tienen tiempo para pensar sino que simplemente tienen que reaccionar en tiempo real. Finalmente, esto también empodera a los radicales y crea un consenso a partir de subgrupos no siempre bien definidos y no necesariamente en posesión del conocimiento adecuado.

La desinformación puede denotar circunstancias en las que los hechos objetivos influyen menos en la formación de la opinión pública que los llamamientos a la emoción y la creencia personal. De nuevo, la emoción. La emoción es lo que produce ese interés por la lectura de artículos, por la lectura de noticias en la red. Pero es también un arma. Y quizá es aquí donde se incluye esa noción de seguridad y defensa cuando se habla de la desinformación, que ya no es un arma que esté sólo a disposición de la política dominante, como era en el pasado, sino también un poderosísimo y descontrolado recurso de la ciudadanía. Por ejemplo, en la reciente crisis de la COVID, la gran desinformación en la ciudadanía europea ha venido de fuera en varios casos, pero ha sido la ciudadanía la que la ha propagado, la que la ha consolidado y la que le ha dado la apariencia de realidad y objetividad. Por lo tanto, ése es uno de los elementos clave que debemos tener presente.

El medio, lógicamente, es el ciberespacio. Frente a las publicaciones en papel o los libros, en realidad donde la desinformación adquiere esa velocidad vertiginosa y ese impacto global es a en el ciberespacio. Y las características de esta desinformación

y de la posverdad son claras: intencionalidad y causar un efecto distorsionador. Es decir, hay un dolo en esta utilización de las noticias falsas.

¿Cuáles son los métodos por los cuales se llega tan fácilmente al ciudadano? En primer lugar, un método muy fácil: minimizar la cuestión. Por ejemplo, la complejidad histórica de un conflicto es sustituida por una trama simple y clara que no tiene en cuenta ni antecedentes históricos ni el contexto en el que se desarrolla, sino que cifra en blanco y negro, en bueno y malo, tanto lo que está ocurriendo como las consecuencias. En segundo lugar, es muy importante centrarse en una historia conmovedora que presumiblemente represente todo el conflicto. Sólo una. No valen ocho. Como apunta Harari en su libro *21 lecciones para el siglo XXI*, en una hambruna que se produjo en África se hizo una campaña con un niño y se obtuvieron muchísimos fondos. En cambio, cuando se hizo esa misma campaña, pero con ocho niños, se consiguieron muchos menos fondos que los que cuando había sólo una encarnación de la tragedia. En tercer lugar, está el diseño de teorías conspiratorias. El mundo contemporáneo es tan complicado que ninguno tenemos la capacidad de entender todo lo que ocurre a nuestro alrededor ni de buscar su justificación. Por lo tanto, la extracción de ciertos elementos de esa realidad compleja que después se hilvanan de tal modo que parezcan una teoría válida es el tercer gran elemento o método que se utiliza para esta elaboración de noticias falsas. Y, finalmente, se crea un dogma, se deposita nuestra confianza en alguna supuesta teoría, institución o líder que seguimos por donde nos conduzcan. Es allí donde aparecen todos los grandes retuiteos, donde un tuit se convierte en viral, hasta que, de repente, aparece una realidad distinta a aquella en la que tenía su origen inicialmente.

Dice también Harari que hay unas reglas básicas para el uso de la información. Si el lector quiere información fidedigna que pague por ella. Solicitar noticias apasionantes que no cuesten nada será a cambio de nuestra atención. Y esa atención se tradu-

ce en otras cosas: control de que la publicidad nos va a llegar, una identificación de cuáles son los parámetros que nos gustan y qué tipo de búsquedas estamos haciendo para utilizarlas para otro tipo de cosas. Es mejor tener acceso a noticias de alta calidad que, aunque cuesten algo de dinero, no abusarán de nuestra atención y muy probablemente tampoco se utilizarán para crear esos perfiles que servirán a otros para fines no siempre lícitos. Los medios de comunicación son, en este sentido, la fuente más fiable. Como también dice Harari, si alguna cuestión nos parece de importancia excepcional, hagamos el esfuerzo de leer la literatura científica relevante, de buscar, investigar y tener criterio, y no sólo una opinión, que es lo que aparece por encima de todo en estas noticias falsas.

Y a estas reglas que propone Harari yo añadiría una tercera, tan vieja como la historia: antes de mandar un tuit, preguntémonos *cui prodest*. ¿A quién beneficia? Cuando nos envían algo muy gracioso o muy escandaloso por WhatsApp, la tentación inmediata es compartirlo con todo el mundo, porque esto tiene una gracia fenomenal. Pero a veces se trata de grandes escándalos y uno debe hacerse siempre la pregunta: «Si yo lo retuiteo y lo comparto con mis amigos, mis conocidos, mi familia, ¿que ganó con eso? ¿Qué puedo estar provocando? ¿Adónde puede llegar? ¿Cuál es el efecto a largo plazo? ¿Quiero que esto se convierta en un elemento desestabilizador?». Y esas son preguntas que normalmente no nos hacemos. Las cosas que se convierten en virales abarcan las cuestiones más diversas pero habitualmente o son escándalos o son teorías conspiratorias o son vídeos de exaltación, que animan a que hierva la sangre y, por lo tanto, a la indignación. Y eso puede tener otros efectos a medio o largo plazo que tienen un impacto directo en la seguridad y la defensa.

Por eso la desinformación tiene que ser vista como un todo dentro de esta seguridad. Mary Calder habla en un libro sobre las culturas de seguridad globales, sobre cómo, cada vez más, las políticas han ido haciéndose biopolíticas. En realidad ya no son geopolíticas pues están centradas en el control de la población más que en el control de un territorio. Por lo tanto, la desinformación es un elemento esencial para cumplir estos objetivos y, además, muestra unos límites borrosos entre lo que está fuera y lo que está dentro. Así, las normas, inhibiciones y tabús de anteriores culturas de seguridad se desvanecen y no se respetan por ninguna de las partes. Es verdad que no hay una destrucción, como puede haber en una guerra a la antigua usanza, en las antiguas guerras, pero hay un daño que puede ser aun mayor para el *statu quo* del sistema político o democrático, para los valores que defendemos y, en definitiva, para la seguridad de los ciudadanos. Y también hay que tener en cuenta que, detrás de las noticias falsas, al hablar de conflictos, siempre hay sufrimiento. Se puede presentar como se quiera la guerra de los Balcanes o la guerra en Ucrania pero ha muerto gente, hay gente que está combatiendo, hay heridos, hay muchos desplazados y hay una realidad subyacente que es lo peor del conflicto y que queda desdibujada a causa de esta desinformación.

La desinformación es parte de un todo que hoy llamamos la guerra híbrida. Esta guerra híbrida es un modo de actuación, como dice OTAN, caracterizado por «el uso de amenazas de actividades a veces encubiertas, militares y paramilitares, convencionales y no convencionales, actos de sabotaje, coerción, desinformación o propaganda, y acciones civiles de todo tipo para influenciar a un adversario». No dice enemigo. Dice adversario, que no es lo mismo. Es algo mucho más amplio, un cajón de sastre donde caben muchas cosas. La Estrategia de Seguridad Nacional incluye además en estas acciones híbridas la presión económica.

Estas acciones híbridas son abordadas tanto por la Directiva de Defensa Nacional como por la Directiva de Política de Defensa, que como saben han sido acordadas hace unos meses. En el escenario estratégico, la Directiva de Defensa Nacional dice que los retos de seguridad proceden ahora «tanto de actores estatales,

entre los que existe una intensa competición estratégica, como no estatales, terrorismo y crimen organizado, con gran capilaridad entre todos ellos, especialmente evidente en las acciones de desinformación y las agresiones en el ciberespacio». Por su parte, la Directiva de Política de Defensa, que complementa la anterior, dice que existen muchos fenómenos transversales, como los ciberataques; la militarización del espacio; las amenazas híbridas, incluido su componente de desinformación; el cambio climático; los fenómenos meteorológicos catastróficos; los desequilibrios demográficos; los movimientos migratorios descontrolados y las pandemias que, como ha demostrado la COVID-19, pueden tener un impacto sobre el bienestar de los ciudadanos, sobre la estabilidad social y la seguridad internacional. A disposición de las Fuerzas Armadas y de las autoridades de defensa, estas directivas se orientarán a generar mayor resiliencia nacional e internacional ante los retos transversales.

Por lo tanto, es un todo. De ahí que, por ejemplo, a la hora de abordar cuáles son los elementos para contrarrestar la amenaza híbrida, en la OTAN se habla del espectro DIMEFIL, es decir, diplomacia, información, militar, economía, finanzas, inteligencia y legislación. La información, insisto, es sólo una parte de ello. En la Directiva de Política de Defensa queda efectivamente reflejada esa idea de bioseguridad, es decir, de protección del ciudadano frente a la geopolítica. Una manera muy fácil de comprender lo que son las amenazas híbridas, y quizá la mejor definición que yo he visto en todos estos años aunque ya es algo antigua, dice que «las amenazas híbridas, o la guerra híbrida, no es más que el enfoque global que se ha vuelto hacia el lado oscuro de la fuerza». Y, efectivamente, esto es precisamente lo que refleja esta nueva amenaza.

Tenemos ejemplos claros de cómo puede afectar a la defensa. Desde un punto de vista institucional, está el cuestionamiento de la utilidad de la defensa, olvidando cuál sería el coste de la no defensa o de la no seguridad. En los debates presupuestarios

siempre se produce una cuestión del coste de oportunidad, de para qué vale la defensa. Se intenta continuamente explicar para qué vale la defensa, cuando en todas y cada una de las situaciones críticas que ha habido, sea por conflictos armados o por todos estos nuevos riesgos y amenazas, como estamos viendo continuamente tanto en España como fuera, la intervención de las Fuerzas Armadas es esencial. Por lo tanto, también hay que atacar esa desinformación respecto a la utilidad de la defensa. Ése sería el aspecto institucional de la amenaza híbrida.

Desde el punto de vista operacional, son muchos los ejemplos. Si hablamos, por ejemplo, de la OTAN y de sistemas de defensa colectivos, a partir de la anexión ilegal de Crimea a manos de Rusia en 2014, la OTAN puso en marcha un plan de reforzamiento. Una de las medidas que se adoptaron fue el posicionamiento de agrupaciones tácticas en los países bálticos y en Polonia, en lo que se llamó la «Presencia Avanzada Reforzada». Pues bien, una de estas agrupaciones tácticas está en Lituania y la lidera Alemania. Poco después de su creación, se difundió la noticia de que varios soldados alemanes habían violado a una menor de dieciséis años, en un claro ejemplo de elemento distorsionador de una presencia que era de carácter disuasorio. Se utilizó ese recurso de realizar una acusación falsa para provocar incertidumbre en la población, para la que siempre es una cuestión sensible recibir a Fuerzas Armadas extranjeras. Por otra parte, era una manera de cuestionar la misma capacidad y legitimidad de la Alianza Atlántica para realizar este tipo de actuaciones. Obviamente hubo una concertación absoluta, tanto desde la OTAN –Carmen Romero lo podrá explicar mejor– como desde Alemania y la propia Lituania, para que esa noticia desapareciera en muy poco tiempo, para que fuera contrarrestada y quedara abortada y amortiguada.

Más recientemente, habrán visto en las noticias que Bielorrusia está acusando a la OTAN de estar posicionando fuerzas en sus fronteras, lo cual nunca ha ocurrido. Dicha acusación no es

una media verdad, ni siquiera una falsa verdad; sencillamente es mentira, porque no había nada de eso. Lo que pasa es que, en un entorno como el que tiene Bielorrusia, es una mentira que puede tener ciertos tintes de credibilidad y, por lo tanto, crear una apariencia y un estado de pensamiento que sea contrario a la Alianza Atlántica, algo que siempre ha sido muy importante en las operaciones de gestión de crisis. Ya desde la guerra de los Balcanes, el General Rupert Smith hablaba de la guerra entre las gentes. Porque los grandes conflictos ya se hacen entre las gentes. No hay un campo de batalla definido, no hay ejércitos, o al menos no los hay en todas las partes, sino que es en medio de la población donde se están desarrollando los conflictos, con la participación directa de ésta. Por lo tanto, uno de los grandes elementos que tenemos a nuestra disposición consiste en atacar la desinformación y crear empatía y sinergia con las poblaciones locales. Aquello que se llamó ganar las mentes y los corazones, que es una de las características y una de las condiciones *sine qua non* para poder operar en terrenos y en teatros tan complicados como los actuales.

Y, finalmente, está el terrorismo, especialmente el que conocimos con el Daesh a partir de 2014, que utiliza los medios de comunicación y, sobre todo, las vías de internet para difundir grandes escenas –que yo diría que son más bien películas– para mostrar sus grandes éxitos con el fin de captar adeptos en todo el globo. Ése es un elemento fundamental de la actuación de Daesh. De ahí que, cuando se estable la coalición global contra Daesh, uno de los cinco grupos de trabajo que se crearon fue el de la contranarrativa. Es decir, cómo replicar a esas pseudovictorias ilustradas como grandes películas, muy efectistas, que estaban apareciendo en las redes y que tenían efecto en el reclutamiento.

¿Cuál es la respuesta y la responsabilidad? La responsabilidad, desde el punto de vista estatal, es nacional. Por lo tanto, los Estados son los primeros que deben tener preparada una respuesta ante toda esta serie de riesgos y amenazas. Pero una de

las mayores responsabilidades, como decía, es también la responsabilidad individual. El individuo puede ser el gran vector que convierta una desinformación en un arma de desestabilización. En el caso de las organizaciones internacionales, se ha desdibujado la frontera entre lo interno y lo externo, en un *continuum* en el que es más necesario que nunca una aproximación global. El multilateralismo es la gran respuesta y la Unión Europea y la OTAN son dos organizaciones con unas características y capacidades específicas idóneas a este respecto. De ahí que se haya procedido a un desarrollo, en primer lugar conceptual pero también institucional, a través del diseño de estrategias, tanto en la Unión Europea como en la OTAN. Por ejemplo, está el establecimiento en la Unión Europea y en la OTAN de la Sección de Análisis Híbrido y la Célula de Fusión Híbrida, respectivamente. O, en el campo de la comunicación estratégica, está la División de Diplomacia Pública, de cuya gran labor hablará luego mi amiga y admirada Carmen Romero. También están las Task Forces de la Unión Europea para el este, para los Balcanes, y para el Sur, el Centro de Excelencia de Comunicaciones Estratégicas y los acuerdos técnicos en el ámbito cíber entre la Unión Europea y la OTAN. Para trabajar mejor conjuntamente, también se han articulado los ejercicios, paralelos y coordinados, que han tenido lugar en los últimos años, que han sido un buen banco de pruebas para testar esa capacidad que tienen ambas organizaciones para asistir a Estados afectados por este tipo de riesgos y amenazas.

En el caso de la Unión Europea y hablando de las amenazas híbridas, me gustaría referirme a una comunicación muy especial que se llama «La lucha contra la desinformación en línea. Un enfoque europeo», del 26 de abril de 2018. En la misma se hace un buen diagnóstico de todo el problema de la desinformación, se dan pautas para afrontarlo y se habla de los procesos electorales, que son uno de los elementos en los que más ha intervenido, o ha intentado intervenir, esta desinformación a ma-

nos de actores externos. El apoyo a un periodismo de calidad, como elemento fundamental de una sociedad democrática, es otro de los grandes pilares de esta comunicación, cuya lectura creo es muy útil.

La utilidad de la defensa ante todos estos nuevos riesgos y amenazas reside en primer lugar en el propio ADN de las Fuerzas Armadas. La anticipación, la preparación, la respuesta y la recuperación son elementos básicos de las Fuerzas Armadas y todos ellos resultan de absoluta utilidad a la hora de afrontar estos nuevos riesgos y amenazas. Por otra parte, la inteligencia y el conocimiento militar del entorno hacen que se pueda obtener una alerta temprana muy rápidamente y, por lo tanto, prepararse antes de que ocurran ciertas desestabilizaciones. También se pueden aprender y exportar a la vida civil desde el ámbito militar muchas cosas relacionadas con la protección de redes, porque, como saben ustedes, las redes de Defensa siempre han tenido una protección especial, con redes clasificadas, etcétera. Hay muchas lecciones identificadas a lo largo de los años que se pueden compartir: la gran experiencia en comunicaciones estratégicas acumulada por la propia intervención y por los propios teatros de operaciones en los que se ha actuado; los procesos de decisión, muy rápidos y muy bien articulados, que en muchos casos son trasladables también a la vida civil; la tradición de cooperar con organizaciones internacionales y distintos Estados; y, finalmente, la capacidad de disuasión y defensa, que también puede desarrollarse en estos ámbitos.

Termino con una breve reflexión. Estamos hablando de una responsabilidad compartida en el ámbito de la desinformación, individual, estatal y supranacional, mediante un multilateralismo eficaz. Lo más importante es saber quiénes somos, cuáles son nuestros valores, conocer la fiabilidad de nuestras instituciones públicas y creer en ellas: la democracia y la ley como principios básicos de la convivencia, el conocimiento como la mejor defensa y, sobre todo, esa conciencia de que nuestras vulnerabilidades

son las fortalezas de otros y, al revés, que nuestras fortalezas son sus debilidades. En este contexto, quizá a lo que tendríamos que aspirar es, como dice Nassim Taleb, a ser antifrágiles, que supone un paso más allá de la resiliencia y de la fortaleza: «El resiliente resiste a los choques y se recupera. El antifrágil, sale mejor y más fuerte». Ojalá entre todos seamos capaces de lograrlo por nuestra democracia.

RAFAEL PANADERO
Moderador

Muchas gracias, directora general. Nos has aportado ideas muy interesantes, entre ellas ésta de la responsabilidad individual, sobre la que empiezan a llegar ya preguntas y que creo que añade otro elemento que quizás salga a relucir en el debate de la educación, porque, como dices, el conocimiento ya no se encuentra en los libros, sino en la red, que es también lo que facilita que la ciudadanía propague desinformación, como ha ocurrido en el caso de la COVID. Mencionabas también esta responsabilidad a la hora de reenviar. Recuerdo un decálogo que sacó la FORTA sobre el tema de la desinformación y las *fake news* que se titulaba «Si dudas, no reenvíes». Por supuesto, está también la responsabilidad de los medios, de las Fuerzas Armadas, de los gobiernos, pero a ellos se suma el tema de la responsabilidad individual.

Vamos a dar paso a la siguiente ponente. Nos acompaña Carmen Romero, periodista de profesión con una extensa carrera internacional. Ha sido corresponsal de EFE en lugares de peso, como Bruselas, París, Moscú o Ginebra; como portavoz adjunta de la OTAN ha trabajado con tres secretarios generales y, actualmente, es la mujer española que ocupa un puesto de mayor jerarquía dentro de la organización de la OTAN, el de subsecretaria general adjunta de Diplomacia Pública, que es la división que se encarga de coordinar la comunicación de la Alianza Atlántica con el exterior.

Carmen no ha podido estar aquí en Madrid pero nos acompaña desde Bruselas vía telemática. Cuando quieras.

CARMEN ROMERO
Subsecretaria general adjunta de Diplomacia Pública de la OTAN

Buenos días desde Bruselas. Muchas gracias, Rafael, por esta introducción. Es un placer unirme a vosotros para hablar sobre un tema tan importante con panelistas y participantes de tan gran nivel. Éste es el segundo año consecutivo que este ilustre seminario me invita a participar y todavía no ha podido asistir en persona; espero lograrlo el año que viene, siempre y cuando decidan volver a invitarme. Como decía, es un honor para mí participar en este Seminario Internacional de Seguridad y Defensa, sobre todo por el gran respeto que me inspiran muchos de sus organizadores y de sus participantes. Entre ellos se encuentran uno de mis primeros mentores, Diego Carcedo. También uno de mis grandes primeros jefes, el que me lanzó a mi carrera internacional, Miguel Ángel Aguilar, director de Información de la Agencia EFE en 1989, cuando me envió como corresponsal a Ginebra, a la sede europea de Naciones Unidas. Muchas gracias, Miguel Ángel. Y es un lujo compartir plataforma con antiguas compañeras y amigas como Georgina Higueras, que estuvo en la mesa anterior, y María Elena Gómez Castro.

Entrando en el tema del creciente desafío de la desinformación, me gustaría situar la cuestión que estamos debatiendo en el contexto más amplio de la crisis que nos ocupa a todos ahora, la COVID-19. Sabemos que toda gran crisis viene acompañada de un paquete de ataques, de desinformación y de propaganda, y este también ha sido el caso con la crisis del coronavirus. Durante la pandemia, organizaciones internacionales como la OTAN y la Unión Europea, además de nuestros Estados miembros y socios, se han visto expuestos a una clara proliferación de desinformación. La Alianza ha estado lidiando con este tipo de desafíos desde hace décadas, pero este reto, como decía Elena, se ha convertido en algo cada vez más complejo debido a su creciente naturaleza híbrida y a su digitalización.

Cada vez son más los actores estatales y no estatales que están explotando la tecnología mediante campañas para dividirnos, para desconcertar y minar nuestras instituciones democráticas. La desinformación se ha convertido en una parte integral de la estrategia política de estos actores. Lo hemos visto de manera destacada durante la crisis de la COVID. Hemos visto campañas de desinformación y propaganda desde Rusia y China, en ciertos casos incluso desde fuentes oficiales, utilizando el espacio digital para intentar socavar nuestros valores, para socavar a organizaciones como la OTAN y la Unión Europea y para confundir a la sociedad occidental. ¿Qué estamos haciendo para combatir esta oleada de desinformación? Yo les puedo hablar de lo que está haciendo la OTAN y de cómo trabajamos en colaboración con otros, como es el caso de la Unión Europea. Nuestro enfoque para contrarrestar la desinformación y la propaganda implica una doble estrategia: una estrategia centrada en entender y analizar en profundidad el espacio informativo y una estrategia centrada en comunicar activamente y de forma deliberada.

Analizar en profundidad el espacio informativo es clave para evaluar la efectividad de nuestra comunicación, pues nos permite adaptar dicha comunicación y contrarrestar esa información de manera más eficaz. Para tener un mayor impacto en un espacio informativo tan saturado como el actual, nuestra comunicación se basa en los hechos, intenta ser lo más rápida posible, es transparente y, sobre todo, está detalladamente coordinada. Porque la coordinación, tanto dentro de la Alianza como con socios como la Unión Europea, es la piedra angular de todo nuestro trabajo, tanto para comprender el entorno informativo como para comunicar con nuestras audiencias. Y esto es particularmente importante cuando se trata de una crisis que evoluciona con rapidez, como es el caso de la actual pandemia.

Empiezo por la necesidad de tener un buen conocimiento del espacio informativo, incluida la desinformación. Esto es fundamental para permitirnos dar una respuesta creíble. Durante la COVID, el análisis de la OTAN ha identificado actores estatales y no estatales que explotan la pandemia para difundir desinformación y propaganda, buscando desestabilizarnos y dividirnos. En el caso de nuestra Alianza, hemos sido objeto de una serie de ataques de desinformación específicos en el período comprendido entre marzo y junio, coincidiendo con el confinamiento de muchos de los aliados que conforman la OTAN. En sólo 48 horas, los días 21 y 22 de abril, detectamos tres ataques coordinados contra la presencia de tropas aliadas en Letonia, Lituania y Polonia, es decir, contra la presencia avanzada reforzada de la que hablaba Elena. Estos tres países fueron el objetivo de campañas de desinformación simultáneas.

Primero, se difundió en línea una carta falsa de nuestro secretario general al ministro de Defensa de Lituania, que declaraba la intención de la Alianza Atlántica de retirar las tropas del país. Fue una operación de desinformación bien orquestada, que también involucró correos electrónicos falsificados y vídeos manipulados, pero aun así, no tuvo éxito. Y les voy a decir el motivo. No tuvo éxito porque las autoridades lituanas respondieron muy rápidamente a través de varias plataformas en coordinación con la sede de la OTAN. Los medios lituanos comprobaron sus fuentes antes de informar sobre la falsificación y nuestro secretario general habló con medios de comunicación bálticos e internacionales para exponer esta carta falsa como parte de un patrón de desinformación contra nuestros soldados destacados en la región. El segundo caso involucró una entrevista falsa, que circuló en línea, alegando que las tropas canadienses en Letonia habían llevado el virus a ese país, lo cual tampoco era cierto. Y, en el tercer caso, se difundió en internet una carta falsificada de un líder militar polaco que en apariencia criticaba a las tropas de Estados Unidos.

Las tres campañas utilizaron técnicas y procedimientos muy similares y fueron parte de un esfuerzo coordinado por dividir a la Alianza. Todos estos intentos de desinformación al final fracasaron gracias a la rápida coordinación, ya que la desinformación no pudo extenderse más allá de algunas plataformas digitales marginales, pero son un ejemplo de las sofisticadas campañas a las que nos exponemos.

Conforme se ha ido extendiendo el virus, las actividades digitales, por ejemplo de China, se han vuelto más asertivas. Es lo que muchos expertos denominan la diplomacia de la mascarilla. El objetivo parece ser doble: rechazar cualquier crítica a la respuesta de China a la pandemia y promover la imagen de China como un líder mundial responsable, con un modelo superior de gobernanza.

También hemos detectado algunos temas comunes en los que Rusia y China centraron sus esfuerzos de desinformación durante la pandemia, lo cual resulta muy interesante. Por ejemplo, un tema sobre el que tanto Rusia como China han coincidido en desinformar es la afirmación de que la COVID-19 se originó en otro lugar, ya sea en un laboratorio secreto en Estados Unidos o en un laboratorio secreto de la OTAN, como ha propagado Rusia, o que el virus fue llevado a China por un soldado estadounidense o que se originó incluso en Italia, como ha propagado China. Es también muy interesante un tuit de este pasado fin de semana en el que los ministros de exteriores de China y de Rusia acordaron cooperar en la lucha contra la desinformación. Hicieron un llamamiento a gobiernos y medios de comunicación para que refuercen su cooperación y rechacen la desinformación. Ésta también parece ser una manera de confundir y de desinformar.

Asimismo, actores no estatales han intentado explotar la pandemia para desinformar. Hablaba Elena de terrorismo. Nosotros hemos visto grupos terroristas que han intentado reclutar nuevos seguidores, montar ataques o mejorar su imagen pública durante

la pandemia. Algunos grupos terroristas incluso han llegado a afirmar que cometer ataques terroristas haría que los autores fueran inmunes al COVID, alentando a sus partidarios a aprovechar esa oportunidad para organizar más ataques.

Nuestra segunda estrategia para hacer frente a la desinformación es nuestra comunicación activa. La OTAN está convencida de que una comunicación pública activa y creíble es la mejor manera de contrarrestar la desinformación. Por eso, nuestra comunicación pública es factual y se basa en hechos y acciones reales. Frente a la desinformación durante la pandemia, nos hemos centrado en comunicar tres mensajes a la opinión pública. Por un lado, que la OTAN sigue plenamente operativa en su sede principal, con sólidas medidas de continuidad, para seguir operando y que la Alianza sigue preparada para disuadir y mantener a nuestras poblaciones en seguridad, que, en todo momento, nuestra vigilancia y capacidad de reacción se han mantenido inalteradas. Nuestro tercer mensaje ha sido un mensaje de solidaridad. Hemos mostrado con imágenes digitales el apoyo práctico proporcionado por los aliados de la OTAN a otros aliados, así como a nuestros socios. Hemos mostrado el importante papel que la OTAN y las Fuerzas Armadas aliadas han desempeñado en el apoyo de los esfuerzos civiles, con más de 350 vuelos para entregar centenares de toneladas de suministros críticos –varios de ellos a España– gracias a la ayuda solidaria de otros países de la OTAN. Hemos mostrado como nuestros soldados construían cerca de cien hospitales de campaña. Hemos mostrado a cerca de medio millón de soldados asegurando fronteras, transportando pacientes y ayudando con pruebas de detección de virus en países aliados. Hemos estado comunicando la verdadera solidaridad en acción, utilizando nuestras diferentes herramientas de comunicación. Y, lo que es más importante, estos tres mensajes han apoyado el objetivo político clave de la OTAN en esta crisis: evitar que la crisis sanitaria se convierta en una crisis de seguridad. La OTAN ha expuesto, y seguirá exponiendo, la desinformación

a través de una amplia gama de actividades con los medios, incluidas declaraciones, correcciones y sesiones informativas.

Para adaptarnos a los desafíos de esta crisis actual, incluido el aumento de desinformación, nos hemos centrado en intensificar nuestra comunicación digital. Hemos transformado los eventos cara a cara de diplomacia pública en encuentros digitales para seguir incentivando el debate público y político, como estamos haciendo en este seminario. Hemos expuesto los principales mitos y las narrativas de desinformación más importantes, por ejemplo a través de nuestro portal web, que se llama «Dejando las cosas claras». Por primera vez, hemos lanzado una campaña digital para concienciar a nuestras audiencias sobre el fenómeno de la desinformación y la necesidad de que verifiquen los hechos. Con esta campaña digital hemos llegado a un millón y medio de personas en Instagram, Twitter, Facebook y LinkedIn; nuestras historias en Instagram sobre esta campaña han sido vistas, por el momento, más de medio millón de veces.

Estamos comunicando también más en ruso, para aumentar nuestra transparencia en ese ámbito. Esto incluye artículos, traducciones de hojas informativas, vídeos en nuestro canal de YouTube en ruso, etcétera. Y estamos reforzando aun más nuestro partenariado con organizaciones que representan a nuestra sociedad civil, pues estamos apoyando más que nunca el trabajo de ONGs, de grupos de expertos, de académicos, de organizaciones de verificación de datos y de otras iniciativas de la sociedad civil para promover el debate, exponer información falsa y desarrollar resiliencia contra la desinformación.

Otra de las cosas que hemos hecho durante esta pandemia ha sido reforzar la marca OTAN, nuestro *brand*, para que la gente reconozca más fácilmente la asistencia facilitada por la Alianza. Reforzar nuestra marca es también un medio eficaz de hacer frente a la desinformación, dado que da más visibilidad a nuestras acciones solidarias. Por ejemplo, hemos resaltado la marca OTAN en la ayuda polaca distribuida en los Balcanes occidenta-

les, en la ayuda española en Lituania y Luxemburgo y en la ayuda estadounidense en Bosnia y Herzegovina.

También hemos producido contenido digital innovador para atraer la atención de los jóvenes, porque la COVID-19 nos ha dado la oportunidad de ser más atrevidos, de tomar más riesgos y ser más creativos en nuestra comunicación pública. Un buen ejemplo de ello es el vídeo que hemos publicado para concienciar a los jóvenes respecto al fenómeno de la desinformación, o la animación sobre lo que es la OTAN y cómo ha respondido al COVID.

En la OTAN evaluamos constantemente nuestra comunicación para seguir mejorando y les puedo decir que, pese a la desinformación, vemos que nuestros esfuerzos están dando sus frutos. Una forma de evaluar es utilizar sondeos de opinión. Realizamos un sondeo al inicio de la pandemia y otro en el mes de agosto y los datos nos indican que los ciudadanos de los países miembros de la Alianza valoran ahora más la labor de las Fuerzas Armadas que al inicio de la pandemia. Seis de cada diez ciudadanos en países miembros de la OTAN consideran que nuestras Fuerzas Armadas contribuyen a la innovación tecnológica, a crear y dar empleo y a la respuesta frente a la COVID-19. Y el 50% de las personas que hemos encuestado confían en la OTAN por su respuesta a la pandemia.

Una de las lecciones más importantes de esta crisis en lo que se refiere a combatir la desinformación, como decía Elena, es que es más importante que nunca unir fuerzas; con otras organizaciones, con nuestros países miembros y con la sociedad civil. En nuestra batalla contra la desinformación, nunca antes nos habíamos coordinado tanto. Ése es el caso con la Unión Europea –tanto con la Comisión como con el Servicio Europeo de Acción Exterior–, con Naciones Unidas y con el mecanismo de respuesta rápida del G-7. Todos hemos trabajado en estrecha colaboración para identificar, analizar y exponer desinformación. Hemos intercambiado continuamente análisis y hemos amplificado mutuamente nuestras campañas digitales, incluida la campaña de Naciones Unidas «UN Verified», lanzada justamente durante la pandemia, que estuvimos coordinando de manera conjunta desde el inicio y durante todo el proceso de seguimiento. Trabajar estrechamente con nuestros socios globales fortalece nuestra capacidad colectiva para abordar este desafío de la desinformación porque, mirando hacia el futuro, no hay duda de que este fenómeno va a seguir adquiriendo complejidad, a medida que se convierte en algo cada vez más gris y difícil de identificar.

Por lo tanto, tenemos que seguir trabajando, tenemos que estar preparados y seguir evolucionando. Organizaciones internacionales, gobiernos nacionales y locales, empresas privadas, la sociedad civil y los medios de comunicación libres e independientes... Todos los actores, incluida la OTAN, tienen un papel que desempeñar.

Concluyo compartiendo, como decía al principio, nuestro convencimiento de que la mejor respuesta a la desinformación es una comunicación pública objetiva y creíble que genere confianza en nuestras audiencias. También tenemos que seguir haciendo todo lo posible para ayudar entre todos a nuestra sociedad civil, a nuestros periodistas y a los medios de comunicación a aumentar su resiliencia para aprender a diferenciar lo que es un hecho de lo que no es real. Desde aquí estamos contribuyendo con nuestro granito de arena, informando del modo más profesional posible a nuestros ciudadanos acerca del trabajo crucial que la OTAN realiza todos los días para mantener a casi mil millones de personas en seguridad.

RAFAEL PANADERO
Moderador

Muchas gracias, Carmen. Muy interesante lo que has expuesto sobre casos concretos de ataques a la OTAN en estos meses. Has mencionado como está respondiendo la OTAN en general y co-

mo respondió Lituania. Ahí sale otro tema interesante, del que espero podamos hablar. Me refiero a si debemos responder o no y a cómo hacerlo, ante las desinformaciones, ante las *fake news*. Y has lanzado al principio y al final de tu exposición esa idea de unir fuerzas, de la importancia de la coordinación para reaccionar ante campañas de desinformación durante la pandemia. Aquí en Madrid sabemos bien de la importancia de la coordinación.

Vamos con el último invitado de esta mesa, que es el General Francisco José Dacoba, director del Instituto Español de Estudios Estratégicos. General de Brigada de Infantería, es diplomado de Estado Mayor y en Alta Gestión de Recursos Humanos por el CESEDEN, en Altos Estudios Internacionales por la Sociedad Española de Estudios Internacionales y por el Colegio de Defensa de la OTAN. Antes de ocupar su puesto actual, estuvo al mando de la sección de planes de Organización del Estado Mayor del Ejército. En el ámbito operativo, estuvo al mando de los cascos azules en Líbano, ha formado parte de la Coalición para la Reconstrucción de Irak y fue también uno de los primeros oficiales españoles destinados en los Balcanes. Ha participado en numerosas actividades de ámbito internacional, tanto dentro del Eurocuerpo como de los Cuarteles Generales de la Alianza. Cuando quieras, General.

GENERAL FRANCISCO JOSÉ DACOBA
Director del Instituto Español de Estudios Estratégicos

Quiero empezar también, como es lógico, agradeciendo a la organización que una vez más se haya contado con el Instituto Español de Estudios Estratégicos para este seminario. En mi caso, es la segunda vez que participo. Ayer decía el General Sanz Roldán que él venía siguiendo esta actividad desde hace décadas y mencionaba la habilidad de la organización para buscar títulos de impacto para las jornadas y para las mesas redondas. Concretamente, el año pasado el título era más que sugerente: «OTAN, el vértigo de la retirada americana». Tal vez este año habría sido igual de oportuno ese tema. Y veremos si el año que viene no lo es todavía más.

Esta mesa redonda tiene como segunda parte de su enunciado «La mentira que mata». Eso me permite, en cierto modo, tomar el relevo de quienes me han precedido hoy y centrar el foco en las operaciones militares, en cómo los contingentes militares se ven también afectados, seriamente afectados, por esta nueva arma que mata y que distorsiona enormemente el empleo de las Fuerzas Armadas en los diversos escenarios.

En las Fuerzas Armadas hemos hecho recientemente un documento titulado «Implicaciones del ámbito cognitivo en las operaciones militares», que creemos que es un tema en el que confluye toda la problemática de la desinformación y de otros procedimientos híbridos que se emplean en esta zona gris de la que estamos hablando. Lo publicamos en el CESEDEN hace pocas semanas y participó en su elaboración mi buen amigo y compañero, el Coronel Carlos Frías, ponente también en este seminario. Es un documento en el que, además, se han tenido en cuenta, si no todos los enfoques posibles, al menos sí los más relevantes. Hay un capítulo dedicado a los aspectos jurídicos, otro al papel de los medios de comunicación social y otro al aspecto psicológico. Y, como no podía ser de otra manera, hay capítulos específicos sobre las repercusiones para las Fuerzas Armadas. Yo invito a todos aquellos de ustedes que tengan interés y busquen profundizar en esta temática a que lo busquen en internet y lo lean.

Para no repetir lo que se ha dicho en otros momentos del seminario, voy a empezar diciendo que es evidente que la sociedad ha cambiado y, con ella, todos sus procedimientos. Y también ha cambiado la forma en que nos confrontamos a actores estatales y no estatales en todo el orden internacional; un cambio que viene impulsado de forma determinante por las nuevas tecnologías disruptivas de las que hablábamos antes. Habéis mencionado la existencia de nativos analógicos y nativos digitales, una separa-

ción absolutamente oportuna porque todavía somos muchos los analógicos que no somos conscientes del todo de que el cambio tecnológico que ha vivido la humanidad en las dos o tres últimas décadas es más relevante y disruptivo del que haya podido vivir nuestra especie en prácticamente toda su historia, al menos en lo relativo a su velocidad, a su celeridad. Esto es indiscutible. La propia globalización, que no es un fenómeno necesariamente pacífico, tiene enormes aspectos positivos pero también es un factor que incrementa las opciones de confrontación al poner en contacto estrecho intereses, a veces contrapuestos, que antes no estaban próximos ni en contacto.

El aspecto positivo es que las sociedades modernas –sobre todo las más avanzadas, nuestras sociedades– exigen que se renuncie al empleo de la fuerza, al empleo de la guerra, al menos en su concepción tradicional cinética. ¿Quiere esto decir que han desaparecido las guerras o los conflictos? Lamentablemente, no. Nosotros, en el Instituto Español de Estudios Estratégicos, tenemos experiencia en ello, puesto que una de nuestras tareas es monitorizar y hacer un seguimiento de la conflictividad en el mundo, por lo que pueda afectar a la seguridad nacional. Año tras año constatamos dichos conflictos en una publicación que a buen seguro conocen, *Panorama Geopolítico de los Conflictos*, en la que año tras año tenemos problemas para seleccionar los conflictos más relevantes para no hacer excesivamente prolija la documentación. Debemos dejar muchos fuera cada año porque la conflictividad, que pareció durante unos años que disminuía, está volviendo a repuntar. Es cierto que las grandes potencias prefieren, afortunadamente, evitar la opción de la confrontación directa, pero la otra cara de la moneda es que se aumentan las guerras *proxy*, las guerras mediante actores interpuestos. Pero además permanece la confrontación a los más altos niveles en todos los demás aspectos: la confrontación económica, comercial, tecnológica… Esta confrontación se desarrolla, a veces de manera muy intensa, en el ámbito cibernético, pues el ciberespacio es el ámbito donde más se está combatiendo en estos momentos en todo el mundo.

Se ha hablado aquí ya de la zona gris y de la guerra híbrida. Yo me voy a permitir resaltar una de las características de esta confrontación en la zona gris, en esa zona previa al confrontamiento armado y directo, que es muy relevante. Me refiero a la asimetría que hay en la confrontación entre los países democráticos y entre países que no tienen nuestros mismos principios, así como con actores no estatales que no están sujetos a las limitaciones que nosotros, afortunadamente, nos autoimponemos, como es el respeto a la ley de actuación en el marco de los derechos humanos, etcétera. Es ésta una asimetría que juega en nuestra contra, de la que hay que ser conscientes y que habrá que gestionar. Habrá que procurar minimizar sus efectos siendo conscientes de que tenemos la inmensa suerte de vivir en una de las diecinueve democracias plenas que hay en el mundo. Eso es algo que merece la pena defender a toda costa.

El conflicto en la zona gris resulta mucho más ventajoso para ciertos actores que el conflicto tradicional, puesto que permite mantener un esfuerzo continuado, permite ir sumando pequeñas ganancias con un esfuerzo relativamente pequeño, permite ir consolidando esos avances poco a poco; permite rechazar acusaciones, permite hacer atribuciones a terceros… Todo esto hace que la complejidad del nuevo campo de batalla sea cada vez más acusada, de tal manera que ahora, en los escenarios en los que están las Fuerzas Armadas españolas, constatamos que, en relación a los primeros despliegues, estos escenarios han visto una evolución muy compleja. Cada vez hay más actores interaccionando en un determinado escenario, ya sea Líbano, Letonia o Malí. Los contingentes militares ya no somos los únicos actores en un conflicto determinado; ni mucho menos somos ya el más relevante.

Los más antiguos en la sala recordarán un programa que había en televisión que se titulaba «Por tierra, mar y aire». Creo

que a algunos la vocación nos surgió viendo aquel programa, porque de no ser así no se explica por qué optamos por esta bendita profesión. Esa expresión identificaba los tres ámbitos en los que en décadas pasadas se podía dar el enfrentamiento, que era por tierra, por mar y por aire. Por eso teníamos un Ejército de Tierra, una Armada y un Ejército del Aire. Ya durante la Guerra Fría, y no digamos posteriormente, se incorporó un cuarto ámbito, que es el del espacio exterior, que nos está proporcionando serios motivos de estudio y de preocupación, puesto que es un espacio en el que se está produciendo una enorme conflictividad, que se está armando y al que tendremos que dedicarle nuestra atención. Un quinto ámbito, más reciente, es el del ciberespacio, que es el que ha concitado estas jornadas. Incluso hay un sexto ámbito, aunque en otros ejércitos lo clasifican de otra manera, que es el ámbito cognitivo, que es el que yo les mencionaba al inicio de mi intervención y que hace referencia a esa publicación que les he recomendado descarguen y lean. El ámbito cognitivo es nuestra mente. En este ámbito, el centro de gravedad de las operaciones no es conquistar la región industrial de la potencia adversaria o dominar un determinado accidente geográfico, un estrecho, un mar o el liderazgo de una determinada potencia. El centro de gravedad de la confrontación actual es la mente de las personas, de la ciudadanía propia y de la de terceros actores, sean éstos adversarios o no.

La DIGENPOL ya mencionó lo de la guerra entre la gente, que es algo indiscutible. Tomando la referencia histórica, durante mucho tiempo la guerra tuvo lugar al margen de la gente. El pueblo sufría las consecuencias pero el combate se daba entre dos fuerzas en un campo abierto. Por supuesto, había víctimas, pero la guerra tenía lugar, por decirlo de alguna manera, al margen de la gente. Lo que ocurre ahora, sobre todo desde las intervenciones en Irak y en Afganistán, a partir de 2001, es que la guerra ha pasado a desarrollarse entre la gente. Esto es muy significativo, sobre todo para las Fuerzas Armadas, ya que nos plantea

unos retos y exigencias muy elevados. Al introducir este sexto ámbito cognitivo, al introducir la mente de las personas, de las ciudadanías, en la ecuación, lo que ocurre es que la guerra pasa a producirse en la gente y, por lo tanto, el objetivo somos las personas. Y somos las personas las que, a veces conscientemente y muchas otras veces de forma inconsciente, nos convertimos también en soldados, como por ejemplo cuando retuiteamos desinformación o enviamos esos WhatsApps con información falsa. Entonces, nos convertimos en soldados de esta guerra de la desinformación. El objetivo es influir y la guerra es la guerra de las percepciones: es más importante la percepción que la propia realidad. Lo único que hace falta en esta guerra es un relato, una narrativa, sembrar esa narrativa y cosechar esa percepción, independientemente de que se ajuste o no a la realidad.

Es cierto que esto no es del todo nuevo. La voluntad de engañar al adversario, como es lógico, es consustancial a la propia confrontación y a la propia guerra. Por no retrotraernos demasiado, al actual Jefe del Estado Mayor de las Fuerzas Armadas de Rusia, el General Guerásimov, se le atribuye actualmente la supuesta teoría de lo que es la guerra y las amenazas híbridas, cuando eso no es cierto. Tanto la zona gris como el concepto de guerra híbrida vienen de bastante antes. Surgen en Estados Unidos con Hoffman y otros autores. Pero sí es cierto que Guerásimov escribió en 2013 un artículo del que les voy a citar una frase: «Las reglas de la guerra han cambiado». Esto lo dice un militar, el máximo responsable de las Fuerzas Armadas rusas. Y continúa: «El valor de los medios no militares para lograr fines políticos y estratégicos no sólo se ha incrementado, sino que en algunos casos excede la efectividad de las armas». Esto lo escribe en 2013. Probablemente de forma casual, en el año 2014 se produce la anexión de Crimea y la inestabilidad en la región oriental de Ucrania, en el Donbás, que todavía perdura y en la que vimos procedimientos de libro relacionados con estos procedimientos híbridos. Dice también el General Guerásimov, aun-

que ya en el año 2017, que «lo indispensable será obtener supremacía en el ámbito de la información y en la comunicación estratégica», que es precisamente lo que nos apuntaba Carmen Romero antes.

Como ven, existen grandes interacciones entre los conceptos más clásicos de la guerra y todos estos procedimientos nuevos, que no se excluyen unos a otros. Esta complejidad en los escenarios a la que hacía referencia se debe a que ninguno de estos procedimientos sustituye o desplaza a los anteriores, sino que se van sumando unos a otros. Seguimos teniendo acciones cinéticas. Por ejemplo, al Daesh hubo que derrotarlo en Mosul entrando, permítanme la expresión, «a tiro limpio» en el casco viejo de la ciudad. Pero, al mismo tiempo, están todos estos procedimientos que venimos mencionando.

También se ha mencionado que la información y el tratamiento de toda esta temática exceden lo militar en países democráticos como el nuestro, donde pasa a ser una responsabilidad global de las autoridades de los países al más alto nivel. Si esta lucha contra la desinformación ya es compleja en general, imagínense ustedes lo que es para las Fuerzas Armadas en operaciones o misiones concretas.

También es relevante recordar que las acciones en el ámbito cognitivo, tanto ofensivas como defensivas, se realizan en un entorno que puede fácilmente invadir los derechos básicos del ciudadano. Éste es un dato relevante que hay que tener en cuenta desde el mismo momento del planeamiento de las operaciones, ya no digamos durante su ejecución.

En cuanto a las repercusiones para las Fuerzas Armadas, en el caso del soldado –y cuando hablo de soldado no me refiero genéricamente a los que vestimos un determinado uniforme sino al soldado desde su más elemental empleo en una unidad–, éste está sometido a unos requerimientos técnicos por el propio manejo de la tecnología que hacen que su formación sea cada vez más compleja y, necesariamente, más continuada y permanente.

Nuestros combatientes necesitan una sólida formación moral y una sólida formación patriótica. Hay que creer y saber por qué arriesga uno su vida y su bienestar, algo que sólo se hace por un valor alto, elevado, que merezca la pena. Y eso habitualmente tiene un nombre; se llama patria. Pero también es importante tener una cierta formación en humanidades, de tal forma que todos los miembros de nuestro contingente puedan empatizar con las sociedades locales en las que nos proyectamos y en las que actuamos. Es importante saber por qué piensan así, cuáles son sus principios, sus costumbres, respetarlas y empatizar. Esto es clave para el éxito en misiones internacionales y yo, como soldado en esta mesa, me permito enorgullecerme de que los contingentes españoles son conocidos por esa capacidad de no imponer, incluso llevando un arma en la mano, de saber empatizar, de saber ponerse en el lugar de quienes están sufriendo, de quien está teniendo enormes problemas, que son la razón por la cual estamos ahí desplegados.

Finalizo con unos ejemplos. Alguno lo ha mencionado ya Elena cuando hablaba de Lituania, refiriéndose al contingente alemán durante el verano de 2017, cuando desplegamos la *Enhanced Forward Presence*.

Les pongo otros ejemplos. En 2006, en Irak se produce un enfrentamiento entre una unidad norteamericana y unos contingentes en el que se ocasionan diecisiete bajas entre la insurgencia. Cuando el campo de batalla se despeja y se supone que van a recoger a sus muertos, lo que hacen es colocarlos en una posición que da la impresión de que han sido asesinados en el momento de la oración. Se les coloca así de una determinada manera, alineados y mirando a la Meca. Y, después, emiten esas imágenes y las explotan, pues el mensaje que cala es que esas personas han sido asesinadas mientras rezaban.

Es también conocido el caso del Almirante Stavridis, cuya cuenta de Facebook fue vulnerada, de tal forma que el *hacker* pudo hacerse con todos sus contactos y éstos, al pensar que se esta-

ban poniendo en contacto con el Almirante, aceptaron su invitación y compartieron sus datos.

Hay otro ejemplo muy reciente, de 2019, que me parece muy relevante. Durante unas maniobras de una división norteamericana, la Primera Acorazada, en Polonia se difunde en redes sociales que un soldado norteamericano ha matado a un soldado polaco, le ha robado el coche y se ha dado a la fuga. La noticia, de entrada, puede ser creíble. La unidad a la que pertenece el soldado es real y esa unidad está de maniobras en ese momento en Polonia. Además, el nombre del soldado es real y las fotos que se difunden son reales, porque están sacadas de las redes sociales de ese hombre. Por lo tanto, si no nos paramos a profundizar en la noticia, ésta es absolutamente verosímil.

La pregunta es cómo se desmonta o cómo se deshace el daño que pueden hacer estas noticias. Recuerden la que para algunos fue la primera guerra híbrida, la de Líbano en el año 2006, cuando las fuerzas israelíes entraron al sur del río Litani y se desarrolló aquella breve guerra de 34 días, que fue una guerra muy híbrida, con mucha guerra de la información por parte de Hezbolá y de sus medios de comunicación, como Al-Manar. Aunque técnicamente Hezbolá no ganó la guerra, como no la perdió e Israel, aunque no la perdió, tampoco la ganó, al final el mensaje que quedó fue que la operación había sido un fracaso. Aquel fue un ejemplo muy claro de desinformación, o de información muy hábilmente elaborada.

RAFAEL PANADERO
Moderador

Muchas gracias, General. Es muy interesante ese nuevo campo de batalla complejo, que incluye también el ciberespacio y el aspecto cognitivo. Ya no hay que tomar la colina, sino la mente de las personas y ahí desde luego juega un papel importante la desinformación.

Vamos con las preguntas. Para empezar, voy a agrupar dos que tienen que ver con el mismo tema: la OTAN. Pregunta Georgina Higueras: «¿Cómo afecta a la OTAN el fuego amigo procedente de los tuits con mentiras o información inexacta del presidente Trump?». Y pregunta Miguel Ángel Aguilar: «¿Qué hace la OTAN cuando la desinformación proviene de actores estatales como el presidente Trump?».

CARMEN ROMERO
Subsecretaria general adjunta de Diplomacia Pública de la OTAN

En el caso del presidente Trump, lo que hemos aprendido durante estos años es que hay que centrarse en los hechos, las señales y las medidas que toma la administración norteamericana con respecto a la OTAN, que son medidas que refuerzan el empeño de Estados Unidos con la seguridad de los países europeos en la Alianza. Tanto la inversión económica como la presencia militar de Estados Unidos en Europa no ha bajado. Por lo tanto, conviene centrarse en los pasos que está dando la administración estadounidense, independientemente de lo que diga el presidente.

RAFAEL PANADERO
Moderador

Voy con otra pregunta que nos llega también de la sala. La formula Miguel González, de *El País*, y entiendo que es para los tres. «En este momento son las empresas tecnológicas las que deciden qué contenidos se retiran de la red. ¿Es una utopía contar con una autoridad independiente, preferentemente judicial, que decida qué es o no desinformación? Tenemos reciente el ejemplo del testimonio de la ingeniera de Facebook que contaba que hay temas que la plataforma detecta como información falsa que a la empresa no le interesa eliminar por distintas prioridades. ¿Es posible pensar en una autoridad judicial que decida estas cosas?».

CARMEN ROMERO
Subsecretaria general adjunta de Diplomacia Pública de la OTAN

En la OTAN estamos trabajando muy estrechamente con la Comisión Europea. La OTAN no tiene ninguna prerrogativa en materia normativa para la legislación relativa a grandes empresas digitales, pero sí estamos trabajando muy estrechamente con la Comisión para que las normativas que están desarrollando tengan muy en cuenta cuáles son los aspectos importantes a la hora de saber reaccionar a la desinformación. Y también es muy importante desarrollar una relación de confianza con Twitter, con Facebook, etcétera. Ha habido ocasiones en las que nosotros hemos tenido que recurrir a Twitter. El hecho de que haya una relación de confianza, nos permite que Twitter tome cartas en el asunto y contribuya a que haya menos información falsa

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

Lo único que puedo decir es que en España hay un Consejo Nacional de Ciberseguridad donde se tratan todos los aspectos transversales del ámbito del ciberespacio. Cuáles son las vulnerabilidades, cómo trabajar con el sector privado... A partir de ahí se desarrollará el ámbito normativo que sea necesario. Éste es un ejercicio conjunto en el que participa el nivel supranacional pero la responsabilidad en el desarrollo de estas normativas recae a nivel nacional. Aunque, como es lógico, la UE también tiene una capacidad normativa muy importante que sirve de referencia.

RAFAEL PANADERO
Moderador

Dice Ignacio Ramos, de la Universidad de Comillas: «Lo contrario a una mentira que mata quizá sea el relato que genera puentes.

¿Qué pueden hacer la política y el ejército para contribuir a un relato internacional y global que nos permita vivir más juntos? ¿Hay espacios para esa búsqueda y para ese debate?».

GENERAL FRANCISCO JOSÉ DACOBA
Director del Instituto Español de Estudios Estratégicos

Desde el ámbito de las Fuerzas Armadas, y en línea con las organizaciones a las que pertenecemos, se está desarrollando ya y está activa también la rama de StratCom. Las Fuerzas Armadas también necesitamos tener nuestra vía de comunicación con la sociedad a la que servimos. Ése es un esfuerzo que se viene desarrollando desde hace algún tiempo y que ha ido incluso modificando la estructura de nuestros Cuarteles Generales, de nuestros Estados Mayores, incluyendo ya células de planeamiento y de conducción específicas en el ámbito de la comunicación. Por supuesto y como es lógico, una estrategia de comunicación alineada con la de las autoridades nacionales y las organizaciones internacionales a las que pertenecemos, además de en función de las operaciones en las que estemos incluidos y con la de la organización que lidere una determinada operación, como puede ser Naciones Unidas en el caso de Líbano, por ejemplo.

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

La política de defensa no sólo se ha ejercido a través de la gestión de crisis y la participación en misiones y operaciones. Hay también buenas noticias en el ámbito de la diplomacia de defensa, es decir, en la relación bilateral con muchos países del mundo, y en todas las actividades de cooperación. Se está tejiendo esa red de seguridad colectiva, esa red de intercambio de experiencias en las que se produce un proceso de retroalimentación que nos hace más fuertes a todos, compartiendo vulnerabilida-

des y creando un sistema por el cual hacemos más fuertes a otros a la vez que nos fortalecemos nosotros. Yo creo que ése es uno de los grandes elementos que se hace en política de defensa, más allá de la gestión de crisis y de todas las buenas noticias que siempre llegan de la actuación de nuestras Fuerzas Armadas en el exterior, con estos programas constantes y permanentes.

RAFAEL PANADERO
Moderador

Javier Fernández Arribas, director de *Atalayar*, dice: «Es una satisfacción ver que la OTAN y los Estados han perdido el pudor y responden a las noticias falsas. ¿Los medios de comunicación deberían apoyar estas iniciativas de manera activa?». Esto nos lleva al origen de la mesa, al nuevo papel que deben jugar los medios en relación con las instituciones, los gobiernos, las Fuerzas Armadas, y también a esa pregunta de si siempre hay que responder o a veces es contraproducente responder a las noticias falsas.

CARMEN ROMERO
Subsecretaria general adjunta de Diplomacia Pública de la OTAN

Lo más importante es hacer todo lo posible desde nuestras instituciones –en nuestro caso desde una institución como la OTAN– para apoyar la independencia de los medios de comunicación, de tal manera que, como siempre dice nuestro secretario general, sigan preguntando, haciendo las preguntas más difíciles, las más complicadas, las más complejas y obligándonos a nosotros a responder. Por lo tanto, desde nuestras instituciones debemos hacer todo lo posible para apoyar a los medios de comunicación. Como decía al principio, nuestro granito de arena consiste en utilizar los recursos a nuestra disposición para apoyar a la sociedad civil, para ayudarla a que tenga mayor resiliencia, pero también

hacer todo lo posible, pese a que no sea una prerrogativa de la OTAN, para que los medios de comunicación sigan siendo fuertes. Sabemos que los medios de comunicación cada vez están en situaciones más precarias. Por eso debemos apoyar a los periodistas independientes. Eso es fundamental.

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

En el caso del Ministerio de Defensa, la ministra aboga siempre por la transparencia, por enseñar lo máximo posible para que se vea todo lo que las Fuerzas Armadas están realizando. Y yo creo que ése es un elemento esencial a la hora de evitar que luego se produzcan noticias falsas antes las que tengamos que reaccionar. Al dar las buenas noticias que se tienen, al mostrar lo que hacen día a día las Fuerzas Armadas, se evita que otros nos ataquen con lo que en realidad no son más que noticias falsas

GENERAL FRANCISCO JOSÉ DACOBA
Director del Instituto Español de Estudios Estratégicos

Yo rompo una lanza por los medios de comunicación. En el lugar en el que estoy ahora, en territorio nacional, tengo cierta relación continuada con los medios de comunicación nacionales y todo son ganas de colaborar, de interactuar unos con otros. Y, lo más importante, en operaciones en el exterior, todos los contingentes llevamos una célula activada prácticamente de continuo; una vez desplegados, la presencia de medios de comunicación nacionales en los distintos escenarios, en función de la actualidad, es casi continua. En ese sentido, la percepción del periodista desde este lado del uniforme es absolutamente positiva. Afortunadamente, esa mención que se ha hecho al principio del seminario a la animadversión que se tenían antes los periodistas y los militares es algo a lo que entre todos le hemos dado por completo la

vuelta. Ahora vivimos una situación en la que es un placer colaborar con cualquier medio de comunicación.

RAFAEL PANADERO
Moderador

Una pregunta de Daniel Calvache, desde la Universidad de Buenos Aires: «Apelar a la conciencia del receptor de la noticia para evitar la propagación de las noticias falsas puede parecer una manera de dejar al azar la propagación de éstas. ¿Es posible considerar algún mecanismo para validar la veracidad de las noticias sin dejarlo al azar, a la suerte o a la consciencia del ciudadano?».

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

Ahí entramos en un terreno pantanoso, que es la diferencia entre opinión y criterio. El criterio está fundado, la opinión no. Pero la libertad de expresión prima sobre todo. Lo que se intenta es –como ha dicho SEGENPOL comparando el ciberespacio con la parcelación de la alta mar– regular ese bien común que es el ciberespacio, pero hacerlo de forma compatible con la libertad de expresión y con otros fenómenos que son mucho más complejos, como puede ser la identificación del originador de una noticia falsa. En esta línea podríamos avanzar más, ya que dejaríamos de hablar de un tuit que no tiene nombre ni apellidos y habría un mayor control o, al menos, una identificación del originador. Es un debate muy complejo que corresponde a los juristas.

RAFAEL PANADERO
Moderador

La siguiente pregunta la formula Gonzalo Babé, presidente de Renacimiento Demográfico. Dice: «¿No hay una línea muy fina

si queremos que los instrumentos de control de la desinformación no sean limitadores de la libertad de expresión? ¿Cómo se puede gestionar ese control sin limitar esa libertad?».

GENERAL FRANCISCO JOSÉ DACOBA
Director del Instituto Español de Estudios Estratégicos

Lo hemos mencionado en las intervenciones anteriores. Esa asimetría a la que me refería en mi exposición es precisamente uno de los desencadenantes de este problema ya que, afortunadamente, en nuestras sociedades la libertad de expresión es un derecho indiscutible, como acaba de expresar la directora general. ¿Cómo se gestiona esto? Es muy difícil. No se puede hacer de manera monocolor. No podemos decir que eso lo tiene que arreglar la parte militar de una determinada operación o la parte jurídica. Tiene que estar incardinado en el planeamiento desde el mismo inicio del diseño de la intervención y luego es algo que hay que gestionar día a día, lo cual no es fácil.

RAFAEL PANADERO
Moderador

Acabamos con una última pregunta que se ha planteado ya en varias mesas. ¿Cómo se gestiona la relación con Rusia? Porque siempre se acaba señalando a Rusia cuando se habla desinformación, tanto desde el Gobierno como desde las Fuerzas Armadas.¿Cómo se mantiene una relación con un Gobierno como el ruso cuando se tiene este mar de fondo?

GENERAL FRANCISCO JOSÉ DACOBA
Director del Instituto Español de Estudios Estratégicos

No sé cómo se gestiona esto con el Gobierno ruso, pero lo que sí puedo decir –ya se ha comentado en una de las ponencias pre-

vias– es que uno de los problemas que tiene la desinformación, y en general las acciones en el ciberespacio, sean de desinformación, ataques de denegación de servicio o cualquier otro tipo de actuación, es la dificultad o imposibilidad de atribución. Nosotros podemos pensar que una determinada acción procede de un ordenador físico ubicado en cierta calle de San Petersburgo pero eso sólo nos dice dónde está ese ordenador. No nos indica quién hay detrás, por mucho que podamos sospecharlo. Y, al revés, se puede hacer ese ataque a un determinado Estado desde una ubicación geográfica fuera del propio Estado, en un país tercero. El gran problema que tenemos siempre al final es la atribución.

MARÍA ELENA GÓMEZ CASTRO
Directora General de Política de Defensa (DIGENPOL)

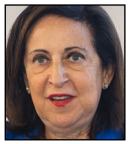
El tema de la relación con Rusia tiene una doble dimensión. Por una parte está la continuación del diálogo, porque no hablar no es una opción. Pero, por otra, es necesario establecer medidas y sanciones y suspender actividades de colaboración en el seno de la OTAN, tal como ocurre desde 2014.

RAFAEL PANADERO
Moderador

Nos despedimos aquí. Gracias a todos. Ha sido una mesa muy interesante.

9. SESIÓN DE CLAUSURA: POLÍTICAS DE DEFENSA EN EL SIGLO XXI

MARGARITA ROBLES
Ministra de Defensa



Moderador
MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación de Periodistas Europeos (APE)

La ministra de Defensa, Margarita Robles

MIGUEL ÁNGEL AGUILAR
Moderador

Llegamos al final de estas jornadas que nos han tenido apasionados durante dos días y que no hemos podido celebrar en Toledo, como ha sido tradición desde el año 1983, por razones de normas sanitarias. Te queremos agradecer vivísimamente, ministra, que hayas aceptado esta invitación. Este seminario ha contado siempre con la colaboración del Ministerio de Defensa; incluso en 2015 recibió el Premio Extraordinario de Defensa que otorga el Ministerio, lo cual es muy de agradecer ya que estos asuntos de la defensa todavía suscitan aprensiones y buscar patrocinadores es casi como buscar patrocinadores para una corrida de toros. En esta ocasión contamos también el patrocinio de Indra, El Corte Inglés y la Junta de Castilla-La Mancha, a pesar de no haber podido celebrar el seminario en Toledo como hemos venido haciendo en treinta de las ediciones anteriores.

Las jornadas han sido realmente valiosas y la ministra se encargará de poner el broche perfecto. Como decía, te agradecemos que estés aquí para clausurar y que hayas aceptado contestar a las preguntas que se te puedan hacer al terminar tu intervención. Querida ministra, ahora que se habla tanto de emociones, quiero expresar la nuestra por que hayas accedido a acompañarnos hoy. Adelante.

MARGARITA ROBLES
Ministra de Defensa

Muchas gracias, Miguel Ángel. Yo también estoy emocionada y muy honrada de estar aquí. Ya llevo varios años –creo que tres, desde que soy ministra de Defensa– asistiendo a esta clausura y quiero agradeceros muy especialmente la invitación porque, como tú decías, el mundo de la defensa y la seguridad es un mundo muy desconocido. Es un mundo que, muchas veces, en determi-

nados sectores, genera algunos tics del pasado, que yo creo que son fruto del desconocimiento de la realidad. Por eso siempre digo que todo marco que contribuya a conocer mejor a las Fuerzas Armadas y el papel que realizan es algo que, para mí, como ministra de Defensa, es muy importante. Por eso aprovecho cualquier marco –y voy a aprovechar éste– para elogiar y poner en valor el trabajo que realizan las Fuerzas Armadas.

Habéis tenido un seminario de un tema absolutamente apasionante, además de muy complicado, con unos ponentes de primera. Éste es un buen momento para reflexionar. A veces la gente te pregunta para qué sirve el Ministerio de Defensa y creo que es porque no todo el mundo es consciente de la que la realidad en la que vivimos. En este momento hay veinticinco guerras en el mundo. Hay 71 millones de refugiados en el mundo como consecuencia de la violencia y del hambre. Además, cada día son más los ataques en el ciberespacio, ataques de todo tipo en un espacio en el que desgraciadamente aparecen nuevos enemigos. Son unos enemigos que presentan una batalla hasta ahora desconocida, como la que hemos vivido y seguimos viviendo, desgraciadamente, con el coronavirus.

El compromiso que las Fuerzas Armadas españolas tienen en esa defensa de la paz, la libertad y la seguridad en el mundo –al amparo del Artículo 1 de la Carta de Naciones Unidas, pero también en otros organismos, como la OTAN y la Unión Europea– hace que nuestras Fuerzas Armadas lleven más de treinta años contribuyendo a la paz en el mundo. Y lo hacen con un altísimo precio. Más de 180 hombres y mujeres han muerto defendiendo la paz, la libertad y la seguridad del mundo. Ése es el mayor ejemplo posible de generosidad. Creo que, a veces, quienes critican a las Fuerzas Armadas no tienen el nivel de generosidad que tienen esos hombres y mujeres que se trasladan lejos de sus casas, que en este preciso momento están muy lejos de sus casas viviendo en ocasiones el drama de la COVID. Esa generosidad es algo que hay que poner absolutamente en valor, porque eso es

precisamente lo que hacen los hombres y mujeres de nuestras Fuerzas Armadas.

Unas Fuerzas Armadas, las españolas, absolutamente preparadas y modernas y que se han constituido en un punto de referencia tanto en el ámbito de la Unión Europea como en el ámbito de la OTAN. Y creo que hay que ponerlo en valor. Cuando en muchos foros internacionales se habla de España, o se siembran dudas sobre nuestro país, debemos decir que España es un país serio, preparado, comprometido con Europa y con los valores democráticos. Ese compromiso de país sólido, serio y fiable lo mantenemos allí donde estamos, en el ámbito de Naciones Unidas, en el ámbito de la OTAN, de la Unión Europea... Siempre pongo un ejemplo y es que, gracias a la presencia de las Fuerzas Armadas españolas, entre otras, en misiones de paz, el papel de las mujeres en Afganistán se ha potenciado enormemente. Cuando fui a Afganistán, yo tuve el honor de ser recibida por el presidente Ghani Ahmadzai acompañado por cuatro mujeres, que entonces eran el equivalente a Secretarías de Estado. Ellas me dieron las gracias porque, precisamente por ese esfuerzo y ese compromiso de la coalición y de las misiones de paz, las mujeres estaban viviendo un momento muy importante en Afganistán.

Y pasa lo mismo en Malí, donde ahora estamos viviendo un golpe de Estado y donde esa labor de entrenamiento que realizan nuestras Fuerzas Armadas, con el paraguas de la Unión Europea, es algo esencial, algo fundamental para las mujeres. Nos explicaba una Teniente Coronel de Malí cómo todavía, a pocos miles de kilómetros de aquí, las mujeres y los niños sufren agresiones sexuales y son utilizados como arma de guerra. Y, ante eso, un país sólido y serio como es España no se puede poner de perfil. Por eso agradezco inmensamente su labor a esos cerca de tres mil hombres y mujeres que están en este momento en misiones de paz en el mundo.

También hay que destacar la apuesta que España está realizando en el ámbito de mujeres, paz y seguridad de Naciones Uni-

das. España tiene una apuesta clarísima por el multilateralismo y entendemos que, en este momento, esa presencia dentro de estos organismos internacionales es esencial para consolidar esa paz y libertad que están tan amenazadas. Como decía antes, hay veinticinco guerras activas en este momento.

Desde el año pasado, cuando clausuramos este seminario en Toledo, han pasado muchas cosas; algunas internas, dentro del propio Ministerio de Defensa, y otras que son las que nos importan a todos, donde las Fuerzas Armadas han tenido y siguen teniendo un papel esencial.

Desde el punto de vista interno del Ministerio de Defensa, quiero poner en valor que estamos en esa apuesta por la modernización de las Fuerzas Armadas y por la transparencia, algo que nos parece básico y esencial. Transparencia porque nos sentimos orgullosos del Ministerio de Defensa y porque nos sentimos orgullosas de las Fuerzas Armadas. Por eso quiero decir que, durante los últimos meses, el presidente del Gobierno firmó la Directiva de Defensa Nacional y yo edité el 4 de agosto la Directiva de Política de Defensa, que por primera vez es transparente. Se le ha dado publicidad –lo cual nunca se había hecho antes– precisamente para poner en valor esa apuesta de las Fuerzas Armadas españolas por el multilateralismo y esa apuesta que hacemos por la modernización de nuestras Fuerzas Armadas; así como por el apoyo a la industria de defensa española, que es esencial pues conlleva la creación de muchos puestos de trabajo. Tengo la satisfacción de decir que se van a crear 900 puestos de trabajo directos, y 4.500 indirectos, gracias a la industria de defensa española, que además favorece y protege a nuestras Fuerzas Armadas, lo cual es muy positivo. Precisamente estuve el lunes en Asturias visitando la fábrica de Santa Bárbara, donde se va a construir el blindado 8x8.

También es muy importante –y se lo quiero agradecer a la presidenta de Navantia, que está aquí hoy asistiendo a este seminario– el papel que está realizando Navantia en la construcción en

Ferrol de nuestras fragatas F-110 y de nuestro submarino S-80 en Cartagena. Es decir, apostamos por unas Fuerzas Armadas modernas que hacen una apuesta en industria, tecnología e I+D+i y, a la vez, ayudan a incrementar el tejido productivo y a crear puestos de trabajo.

Creo que es muy importante que se conozcan las dos directivas que les he mencionado anteriormente. También hemos hecho algo que creo que era absolutamente imprescindible, como es crear un marco normativo diferente, poner al día el marco normativo. Las directivas de las que estábamos hablando eran del 2012 y estamos en 2020, por lo que ésta era una labor absolutamente imprescindible.

También hemos creado un marco normativo nuevo. Se ha dictado un nuevo Decreto de Estructura de las Fuerzas Armadas y, derivado de ese decreto, que se editó hace pocos meses, se han ido dictando unas órdenes de desarrollo y de puesta en funcionamiento modernizado, tanto de Estado Mayor de la Defensa como de los tres Ejércitos, el Ejército de Tierra, la Armada y el Ejército del Aire.

Quiero poner aquí también en valor, precisamente porque está relacionado con el tema de este seminario, que dentro del Estado Mayor de la Defensa se ha constituido un Mando Conjunto nuevo, que es precisamente el Mando Conjunto del Ciberespacio, que sustituye el Mando Conjunto antiguo que había de ciberdefensa, más centrado en las telecomunicaciones. Ahora hemos puesto el foco en el ciberespacio, pues el ciberespacio es una amenaza real, que existe, y para la que hay que estar preparados.

Aunque habéis hablado en abundancia del tema de la modernización de las Fuerzas Armadas durante este seminario, quiero decir que somos muy conscientes de esa necesidad. De ahí todo lo que hemos hecho en estos últimos meses, tanto con el Decreto de Estructura de las Fuerzas Armadas como con la regulación específica del EMAD y de los tres Ejércitos, que no ha sido sino apostar por esa línea de modernización y de compromiso con la

sociedad. Hemos trabajado pues internamente en esa modernización, que es necesaria. Igual que hemos trabajado internacionalmente en todos los compromisos que tiene España.

Y hemos trabajado también contra ese enemigo terrible, silencioso, pero tan letal y nefasto, que está siendo el coronavirus y que, desgraciadamente todavía está ahí. Como ministra de Defensa es un honor y un orgullo y no tengo palabras suficientes para agradecer su labor a los hombres y mujeres de las Fuerzas Armadas que participaron en la Operación Balmis. Hablamos de exactamente 20.002 operaciones en las que han participado un total de 180.00 hombres y mujeres que han hecho de todo. Han llegado donde no llegaba nadie, con generosidad, con sacrificio y con entrega, haciendo desinfecciones de residencias y de infraestructuras públicas, trasladando cadáveres, no dejando solos a los muertos, lo cual es muy importante. Con generosidad, con espíritu de sacrificio, haciendo traslados de enfermos de unos hospitales a otros. Yendo a China a traer material en un traslado que implica más de 32 horas de vuelo. Hemos estado en infraestructuras críticas y en residencias de la tercera edad; no solamente desinfectando sino haciendo compañía a la gente. Y eso es algo que ha puesto a las Fuerzas Armadas en primera línea de conocimiento; es importante que la ciudadanía española las conozca y sepa de su eficacia, preparación y generosidad. Allí donde muchas veces no se llegaba estaban ellos. Allí estaba la sanidad militar. Ahí estaba el Hospital Gómez Ulla. Ahí estaba el Hospital Militar de Zaragoza. Estaban y están. Ahí estaban nuestros sanitarios y nuestros enfermeros haciendo pruebas.

Por eso hemos querido hacer algo simbólico, como ha sido la creación de la Medalla de Balmis, porque toda la ciudadanía tiene que saber que nuestras Fuerzas Armadas están siempre al pie del cañón. Ahora siguen al pie del cañón en la que hemos llamado Misión Baluarte, que no es sino el resultado del ofrecimiento que hizo en su momento el presidente del Gobierno a todas las comunidades autónomas para ofrecer rastreadores militares. Ayer mismo estuve con el ministro de Sanidad, Salvador Illa, visitando a los rastreadores en Madrid y quiero decir algo que me parece muy importante. La oferta del ejército a las comunidades autónomas no tiene ninguna connotación política. Es exclusivamente voluntad de servicio a los ciudadanos, vivan donde vivan, estén donde estén. No hacemos juicios de valor ni analizamos si una comunidad es más competente o menos. Hacemos el único juicio de valor posible, que es que tenemos que estar, que tenemos que ayudar, que el rastreo es esencial para prevenir los contagios. En este momento, trece comunidades autónomas y las dos ciudades autónomas nos lo han pedido. En muchos casos estamos ya trabajando *in situ*, por ejemplo aquí en Madrid. Y en otras comunidades estamos adaptándonos a los sistemas informáticos. Donde haga falta, cuando haga falta y como haga falta, estaremos rastreando. Estaremos en todas aquellas misiones en las que el Gobierno, en colaboración con las comunidades autónomas, entienda que las Fuerzas Armadas pueden prestar un servicio. Sin ninguna connotación política, exclusivamente con voluntad de servicio, ahí estarán nuestras Fuerzas Armadas. Y estarán como han estado siempre: con eficacia y con entrega, ayudando a los ciudadanos.

Yo creo que España ha demostrado que es un gran país en estos meses de la pandemia. Ha demostrado que los ciudadanos españoles son solidarios. Ha demostrado la capacidad de su personal sanitario, de los médicos y enfermeros. Ha demostrado tener unas fuerzas de seguridad del Estado que están a la altura de las circunstancias y, por supuesto, igual ha ocurrido con las Fuerzas Armadas. Como también han estado a la altura los transportistas, la gente que trabaja en los supermercados y tantos otros. Ésa es la gran España que tenemos. Y esa gran España que tenemos nos pide a todos los políticos unidad, arrimar el hombro, un esfuerzo conjunto. No debemos tirarnos el virus a la cabeza, porque el virus no distingue de ideologías, no distingue de partidos políticos, sino que ataca a las personas. Lamentablemente, lo ha-

ce especialmente con los más vulnerables, porque el virus tiene también unas connotaciones económicas que todos conocemos.

Por eso, a este virus hay que plantarle cara desde la unidad, sin hacer política. Lo digo muchas veces. Yo viví con dolor personal las críticas absolutamente injustas que se hacían cuando íbamos al Congreso de los Diputados y se pedía la prórroga del estado de alarma. Pero vamos a mirar al presente, al presente y al futuro. Esta batalla la tenemos que ganar. Y la tenemos que ganar desde la unidad; no desde la descalificación, no desde el tirarse los trastos a la cabeza, sino arrimando el hombro. Insisto, no hagamos política con ello. Y creo que la mejor manera, el mejor ejemplo, son nuestras Fuerzas Armadas y su comportamiento durante la Operación Balmis. Igual que lo están haciendo ahora en la Misión Baluarte, ejerciendo como rastreadores allá donde sea necesario.

Ayer, cuando estábamos en Torrejón observando a los rastreadores, pude ver el cariño y la empatía con los que los hombres y mujeres de la UME hablaban con aquellas personas que recibían la llamada y que lo estaban pasando mal. Ahí tenemos que estar a la altura de las circunstancias. Tenemos que ayudar a todo el que lo pasé mal, sin connotaciones políticas, con unidad y arrimando el hombro todos.

Cuando digo esto hablo en nombre de los 120.000 hombres y mujeres de las Fuerzas Armadas: en primera línea, donde haga falta, como sea necesario. Igual que están en el extranjero en misiones de paz, van a estar aquí, en España, luchando contra el coronavirus, sin ningún matiz político y con voluntad de servicio. Con voluntad de querer a nuestros ciudadanos y hacer de España un gran país, ese país que es de todos, que todos merecemos, comprometido con la justicia social, con los derechos y con las libertades desde hace muchos años. Ese compromiso con la justicia, con los derechos sociales, con una sociedad más abierta, lo representan por su voluntad de espíritu y de sacrificio nuestras Fuerzas Armadas. Así que mi homenaje a ellos, así como de nuevo mi agradecimiento, Miguel Ángel, a todos vosotros. Mi agradecimiento porque, en un momento como el que estamos viviendo, el papel de la prensa es esencial, fundamental, porque ahora más que nunca es necesario el rigor, la serenidad y el compromiso. Y sé que periodistas como tú, y como todos los que estáis hoy aquí –os conozco a muchos y sé que seguís materias de defensa–, se caracterizan siempre por el rigor, la serenidad y el compromiso. Sé que muchas veces renunciáis a un titular que a lo mejor sería más llamativo porque queréis dar la noticia real. Aquí el protagonista no es Miguel Ángel Aguilar, no es el Gobierno de la nación, no es Margarita Robles; es el esfuerzo de todos, que cada uno de los ciudadanos españoles tiene derecho a pedirnos; y es el protagonismo de todos y cada uno de los hombres y mujeres de las Fuerzas Armadas. Cuando alguien me pregunta si se están haciendo bien las cosas en Defensa, yo siempre digo que no, que los que están haciendo las cosas bien son los 120.000 hombres y mujeres de las Fuerzas Armadas.

Así que gracias de nuevo por organizar este seminario y darme esta oportunidad, este altavoz, para explicar nuestro compromiso con España y el objetivo fundamental en el que todos, sin excepción, sin hacer política, tenemos que estar comprometidos: vencer al virus y trabajar por la recuperación de nuestro país.

MIGUEL ÁNGEL AGUILAR
Moderador

Como sé que te va a gustar, te voy a resumir el telegrama que un buen amigo periodista va a lanzar en el programa «Hora 14» dentro de un rato. Dice así: «En resumen, las circunstancias obligan. Se acabó el recreo, el gusto por la bronca, la insolencia, el "y tú más", el gozarse con las dificultades del competidor político. Ha llegado el momento de la cooperación, de sumar recursos, de atender las necesidades de los ciudadanos, a los que no debe perjudicar el color político de las autoridades que estén al frente.

Basta ya de mirarse con encono y de creerse en posesión de la verdad y de negar todo a los rivales. Se impone abdicar de maniqueísmo y que prevalezca la buena voluntad. El público mira exigente, toma nota y pasará la cuenta».

Antes de dar paso a las preguntas, también quería decirte, a propósito de tu intervención, que es verdad que mucha gente ve el ámbito de la defensa con aprensión. Pero hay que saber que, si desaparecen los ejércitos, aparecen los señores de la guerra. Hay que volver a leer el libro *El honor del guerrero* de Michael Ignatieff. Hay que volver a leer también a Rafael Sánchez Ferlosio. Hay que saber que los militares obedecen no porque haya otro poder de coerción superior al suyo. Si se subleva el cuerpo de Correos, aparece la policía. Y, si se sublevara la policía, aparecerían las Fuerzas Armadas. Pero si se sublevan las Fuerzas Armadas no aparece nadie. Entonces, ¿por qué obedecen? No porque alguien tenga una fuerza mayor sino porque han empeñado su palabra. El sentido del honor es clave para la estructuración de las Fuerzas Armadas y, por eso, el respeto a esa actitud por parte de la ciudadanía resulta fundamental. El mundo ha progresado por la división del trabajo, porque algunos ciudadanos se especializaron en asumir la defensa de la totalidad de la población. Esto es muy importante y sé que tú lo sabes y que lo estás aplicando. Por eso mereces nuestra consideración.

A continuación, voy a trasladarte algunas de las preguntas que nos están llegando a través de *streaming*. La primera es de Gonzalo Babé, presidente de Renacimiento Demográfico: «¿Es sensible el Gobierno a la dotación presupuestaria que la defensa requiere?».

MARGARITA ROBLES
Ministra de Defensa

Lo único que puedo decir es que los presupuestos están en fase de elaboración y por tanto no hay aún una partida presupuestaria. Pero tengo que decir de una forma muy rotunda y clara que nadie dentro del Gobierno ha puesto nunca ningún inconveniente al presupuesto de Defensa. Nadie. Es importante decirlo porque creo que eso es ser justo con todo el mundo. El presupuesto de Defensa es necesario para tener esas Fuerzas Armadas modernas, esas Fuerzas Armada preparadas y que luchan por la paz. Durante la Operación Balmis –como bien sabe la secretaria de Estado que nos acompaña en este seminario–, el Ministerio de Defensa ha gastado 31 millones de euros, porque creíamos que hacerlo era bueno para los ciudadanos y también porque un presupuesto en defensa favorece la industria de defensa española y, por tanto, crea muchos puestos de trabajo. Antes he puesto el ejemplo de Asturias y aquí está presente la presidenta de Navantia, así que lo quiero decir con toda claridad: durante el tiempo que yo llevo aquí, no se ha puesto ningún obstáculo al presupuesto en Defensa.

Otra cuestión es la situación de los Presupuestos Generales del Estado en este país. Al hilo de la pregunta, diré que creo que es absolutamente imprescindible que haya unos presupuestos ya. No solamente por la defensa nacional, que también, sino porque, para su reconstrucción, este país necesita que haya unos presupuestos. Sinceramente, en un momento en el que la gente lo está pasando mal, cuando hay tantas personas vulnerables, nadie entiende que por razones puramente partidistas se pueda hacer una política muy menor, muy de corto vuelo, tratando de obstaculizar los presupuestos con la única finalidad de perjudicar al Gobierno. Porque si no hay un presupuesto de reconstrucción para España los únicos que salen perjudicados son los ciudadanos de la nació, no el Gobierno de la nación. Por eso es por lo que considero tan importante que todas las fuerzas políticas que crean en la democracia y que tengan sentido de Estado hagan lo necesario para que España, de una manera u otra, ya sea mediante su voto positivo o mediante la abstención, tenga de una vez los presupuestos que se merece.

MIGUEL ÁNGEL AGUILAR
Moderador

Ana Alonso, de *El Independiente*, pregunta qué teme más Margarita Robles como ministra de Defensa, si las amenazas, las ciberamenazas, etcétera.

MARGARITA ROBLES
Ministra de Defensa

Es complicado, pero me viene a la cabeza lo que decías antes de algo que para mí es tremendo, como es la desinformación y las noticias falsas. Esas amenazas también son muy graves, porque generan una situación de alarma con algo que no es verdad. Y eso no es fácil de combatir. Yo siempre digo que las cosas que son verdad, las guerras, los ataques reales, se pueden combatir. En cambio es muy difícil de combatir la desinformación y todo lo que hay detrás de ella, incluidos los que mueven esa desinformación. Por eso es tan importante, en un momento como el que estamos viviendo, el papel de los medios de comunicación. Yo soy una ferviente partidaria de los medios de comunicación, porque creo que la democracia en este país, la Transición, no se hubiera consolidado sin ellos. Creo que es muy importante que todos hagamos un esfuerzo para dejar en evidencia aquellas informaciones que son falsas y los intereses de muy distinto tipo que hay detrás de ellas.

MIGUEL ÁNGEL AGUILAR
Moderador

Pedro González, de la revista *Atalayar* pregunta: «¿Ha testado el Ministerio de Defensa si después del esfuerzo desplegado por las Fuerzas Armadas en toda España ha crecido la empatía hacia ellas en el País Vasco y en Cataluña?».

MARGARITA ROBLES
Ministra de Defensa

Yo no hago diferencias, porque este virus no distingue de comunidades autónomas. Nuestras Fuerzas Armadas han estado allí donde ha hecho falta. Han hecho desinfecciones en el País Vasco, han construido un hogar para los sin techo en la Fira de Barcelona, han construido un hospital de campaña en Sabadell, han desinfectado residencias de personas mayores en Cataluña y en el resto de España. Lo que sí que puedo decir, y ahí están las últimas encuestas, es que los ciudadanos aprecian nuestras Fuerzas Armadas. Voy a decir una cosa que me parece una obviedad pero que hay gente a la que no le resulta tan obvia. Los 120.000 hombres y mujeres que forman las Fuerzas Armadas son personas como nosotros, trabajadores con sus propios problemas familiares. Algunos no llegan a final de mes porque los sueldos... Ojalá fueran superiores. Muchos de ellos están en situación de aislamiento por el coronavirus. Y, aun así, tienen una única voluntad, que es el servicio a los ciudadanos. Así que yo animaría a aquel que todavía tenga dudas a que los conozca un poco más.

MIGUEL ÁNGEL AGUILAR
Moderador

Javier Fernández Arribas, también de la revista *Atalayar*, pregunta si es necesaria una mayor intervención española y europea en el Sahel para atajar la expansión de grupos terroristas que podría desestabilizar esa región estratégica.

MARGARITA ROBLES
Ministra de Defensa

El Sahel es un sitio esencial, fundamental. Por eso tiene España ese compromiso en Malí. En esta materia trabajamos con la UE,

como socios serios y fiables que somos. Damos nuestro máximo apoyo al Alto Representante, a Josep Borrell, y a todas aquellas misiones que la Unión Europea considera que son buenas para este fin. Vamos a estar allí donde nos llamen. Por eso estamos en Malí. La situación en el Sahel nos preocupa mucho y España debe tener protagonismo.

España es un país que no puede vivir aislado. A muy pocos miles de kilómetros de nosotros, en este momento hay guerras, hay violaciones de derechos humanos, hay agresiones sexuales, hay muchos muertos... No podemos mirar para otro lado. España no sería una democracia si nos pusiéramos de perfil ante los dramas que estamos viviendo en el mundo. Ahí, en primera línea, con empatía, con compromiso con la paz, están muchos hombres y mujeres de las Fuerzas Armadas, ayudando a determinados países. Y, además, con algo muy importante que tienen nuestros contingentes españoles: mucha empatía. Yo he estado en Líbano y he visto como enseñan español, como enseñan a los niños el idioma. Por ejemplo, hemos firmado un convenio con el Instituto Cervantes para que el idioma español pueda estudiarse por ese canal en Líbano. Siempre digo que el idioma es un instrumento para la paz y el español es un magnífico idioma, uno magnífico idioma para la paz.

MIGUEL ÁNGEL AGUILAR
Moderador

Decirte que durante el seminario el General Dacoba ha puesto de manifiesto el comportamiento impecable que han tenido nuestros contingentes en Líbano. Toquemos madera, porque donde hay mucha gente siempre puede haber un exceso. Hemos visto asuntos muy duros por parte de contingentes de otros países, de Estados Unidos, de Holanda..., relacionados con abusos, etcétera. Y España está a salvo. El comportamiento de los nuestros ha sido realmente ejemplar. Sintamos eso como algo muy valioso.

Quería decir otra cosa, que es que los españoles vemos al rey como el primer soldado de la nación. Tal vez ahora ha crecido algo más el republicanismo al calor de algunos acontecimientos pero, como ha dicho muy bien el presidente del Gobierno, y has repetido tú incluso con más fuerza, esto tiene un trámite. Si ustedes quieren cambiar esto, ahí está la Constitución y sus mecanismos para cambiarlo. No se puede hacer de otra forma. Éste es un país maduro en el que eso podría pasar. ¿Habrá una Tercera República? El tiempo lo dirá. O puede que la monarquía vuelva a ganarse, si cabe con más fuerza, la adhesión de los españoles y su respeto.

La cuestión realmente peligrosa es que algunas intervenciones de algunos de los promotores de la República terminen no diciendo «Viva la República» sino diciendo «Vivan las repúblicas», como si estuviéramos en trance de la balcanización de la Península Ibérica. Viviremos con la República si eso es lo que decidiésemos los españoles mediante el procedimiento naturalmente establecido, pero el abismo de ver nuestro país fragmentado es una cosa que yo creo que a muchos nos conmueve muchísimo, porque si España terminase siendo ocho repúblicas cada uno de los españoles valdríamos un octavo de lo que valemos.

MARGARITA ROBLES
Ministra de Defensa

Yo creo profundamente en el espíritu de la Transición. Creo en nuestra Constitución; creo en el pacto constitucional del que hablaba el presidente del Gobierno. Quizá porque hay gente que no vivió la dictadura, que no sabe lo que es la privación de derechos y de libertades, a lo mejor no se valora suficientemente la Constitución. Es la Constitución lo que permite que todos nosotros podamos expresarnos, opinar libremente y defender aquello en lo que creemos. Creo que, durante estos cuarenta años, la Constitución nos ha permitido desarrollarnos como país. Es muy im-

portante salir al mundo. A veces uno no viaja suficientemente pero, cuando uno viaja a muchos países y va a organismos internacionales, ve cómo se valora a España en todo el mundo. España habla hoy de igual a igual con Estados Unidos o con cualquier otro país. Y eso ha sido posible gracias a nuestra Constitución. A veces los españoles tenemos una vena que nos hace pensar que todo lo nuestro es malo. Habrá cosas malas, pero la inmensa mayoría de nuestras cosas son muy buenas. Como ese espíritu que ha tenido la sociedad española en la lucha contra la COVID, ese espíritu tan importante. Nuestra Constitución es un marco de libertades, un marco de democracia, de convivencia, de tolerancia y de respeto. No se puede pedir más.

MIGUEL ÁNGEL AGUILAR
Moderador

Querida ministra, muchísimas gracias por habernos acompañado en la clausura de esta XXXII edición del Seminario Internacional de Seguridad y Defensa. Gracias también a todos los que nos habéis acompañado, tanto de manera presencial como *online*, y a quienes habéis colaborado con vuestras preguntas.

MARGARITA ROBLES
Ministra de Defensa

Gracias a vosotros. Muchas gracias.

MIGUEL ÁNGEL AGUILAR

Licenciado en Física por la Facultad de Ciencias de la Universidad Complutense de Madrid y graduado en la Escuela Oficial de Periodismo de Madrid, inició su aproximación al periodismo en el diario *Madrid*, donde fundó la Sociedad de Redactores meses antes de que el periódico fuera cerrado por el Gobierno del General Franco en noviembre de 1971. En los inicios de la Transición dirigió *Diario 16* hasta ser destituido por publicar una información sobre el intento de golpe que gestaba el General Torres Rojas al frente de la División Acorazada nº 1. Por ello le fue incoado un Consejo de Guerra, mientras el General en cuestión culminaba con otros colegas el golpe que intentarían el 23-F, un año más tarde. Ha sido corresponsal político y diplomático, miembro del comité editorial de *El País* y director de Información de la Agencia EFE, además de dirigir el diario *El Sol* y los informativos de madrugada y del fin de semana de Telecinco. Desde su establecimiento en 1981, es secretario general de la Asociación de Periodistas Europeos. Actualmente colabora en *Vozpópuli*, la Cadena SER y Antena 3.

GENERAL MIGUEL ÁNGEL BALLESTEROS

General de Brigada de Artillería, es diplomado en Investigación Operativa y en Estado Mayor y doctor por la Universidad Pontificia de Salamanca. Especialista en geopolítica y estrategia de seguridad, prevención del terrorismo y yihadismo, entre 1995 y 2012 fue profesor asociado en la Universidad Pontificia de Salamanca y, desde octubre de 2015, en la Facultad de Ciencias Políticas y Sociología de la Universidad Complutense. Ha dirigido diversos cursos de verano en universidades de todo el territorio español y actualmente es profesor colaborador en el master de Prevención del Terrorismo de la Universidad Rey Juan

Carlos. Fue el primer jefe del centro de satélites Centro Principal Helios Español. Entre 2002 y 2008 ocupó el cargo de Jefe del Departamento de Estrategia y Relaciones Internacionales de la Escuela Superior de las Fuerzas Armadas del Centro Superior de Estudios de la Defensa y en 2009 fue nombrado General Director del Instituto Español de Estudios Estratégicos, cargo que desempeña hasta su nombramiento en 2018 como director del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno.

GENERAL FRANCISCO JOSÉ DACOBA

General de Brigada de Infantería, es diplomado de Estado Mayor, así como en Alta Gestión de Recursos Humanos por el CESEDEN, en Altos Estudios Internacionales por la Sociedad Española de Estudios Internacionales y por el Colegio de Defensa de la OTAN en Roma. Como Oficial del Estado Mayor ha sido analista en la División de Planes del Estado Mayor del Ejército y Jefe de la Sección de Planes y Organización de la misma. En al ámbito operativo, ha sido Jefe de la Unidad de Inteligencia de la División Mecanizada y miembro del Estado Mayor de dicha división. En sus sucesivos empleos ha estado al mando de unidades acorazadas y mecanizadas y ha participado en numerosas actividades de ámbito internacional en el marco del Eurocuerpo y de otros Cuarteles Generales de la Alianza. En 1994 formó parte del contingente español en la Misión de Naciones Unidas UNPROFOR, en Bosnia Herzegovina, en 2003 fue miembro de la Coalition Provisional Authority para la reconstrucción de Irak, y en 2013 y 2014 desplegó su Brigada en Líbano, haciéndose cargo del mando de la Brigada Multinacional del Sector Este de UNIFIL y ejerciendo como Comandante de dicho Sector de la Misión de Naciones Unidas en el sur de Líbano.

ROSA DÍAZ

Licenciada en Ciencias Exactas por la Universidad Autónoma de Madrid, amplió su formación con un Programa de Dirección General por el IESE. Con una sólida experiencia en el sector TIC, ha ocupado diferentes cargos directivos en empresas como Sage, Santander Elavon y Panda Security, donde fue Country Manager en España y Portugal durante cuatro años. Tras ocupar el cargo de subdirectora de Apoyo a Empresas e I+D+i, actualmente es directora general de INCIBE. Asimismo, pertenece a diferentes grupos que tienen como objetivo dar visibilidad a la mujer en puestos de liderazgo dentro del mundo de los sectores de la tecnología y, específicamente, en el sector de la ciberseguridad.

MONTSERRAT DOMÍNGUEZ

Licenciada en Periodismo por la Universidad Complutense de Madrid y máster en Periodismo por la Universidad de Columbia de Nueva York, donde vivió entre los años 1989 y 1990, comenzó su carrera periodística en la Agencia EFE. Tras trabajar en Canal+, Telecinco y Antena 3, donde presentó y dirigió informativos y coberturas especiales, presentó los programas «La Mirada Crítica» y «Ruedo Ibérico» y 2008 se hizo cargo de «A vivir que son dos días» de la Cadena SER. En 2012 fue nombrada directora de *El Huffington Post* y en junio de 2018 pasó a ser la nueva subdirectora de *El País*. Montserrat Domínguez es vicepresidenta de la Asociación de Periodistas Europeos y ha recibido sendas Antenas de Oro por su trabajo en radio y televisión, así como el premio Carmen Olmedo Checa de la Junta de Andalucía por su compromiso igualitario a lo largo de su trayectoria profesional, y el Premio de Periodismo Europeo Salvador de Madariaga.

MARIO ESTEBAN

Investigador principal del Real Instituto Elcano y profesor titular del Centro de Estudios de Asia Oriental de la Universidad Autónoma de Madrid, es doctor en Ciencia Política y Relaciones Internacionales por la Universidad Autónoma de Madrid y máster en Política Asiática por la School of Oriental and African Studies de Londres. Además, es investigador principal de proyectos financiados por la Korea Foundation y los ministerios de Economía, Industria y Competitividad y Asuntos Exteriores. Como analista sobre China, ha colaborado con el Parlamento Europeo, la Comisión Europea y el Ministerio de Defensa. Asimismo, ha ejercido como profesor visitante en la Universidad de Lenguas Extranjeras de Pekín y en la Universidad de Turku, en Finlandia y, como investigador visitante, en la Academia de Ciencias Sociales de China y en la Universidad Nacional de Chengchi.

PAZ ESTEBAN

Nacida en Madrid en 1958, Paz Esteban es licenciada en Filosofía y Letras por la Universidad Autónoma de Madrid. En 1983 ingresó en el Centro Superior de Información de la Defensa, donde se especializó en Inteligencia Exterior, realizando sus primeros informes en relación con la permanencia de España en la OTAN de cara al referéndum de 1985. Siempre dentro de este ámbito, desempeñó diversos cargos hasta que Félix Sanz Roldán la nombró Jefa de su Gabinete Técnico en 2010. En junio de 2017 fue nombrada secretaria general del Centro Nacional de Inteligencia y en febrero de 2020 se convirtió en la primera mujer en la democracia española en desempeñar el cargo de directora del CNI. Actualmente, además de secretaria de Estado como directora del Centro Nacional de Inteligencia, es directora del Centro Criptológico Nacional, de la Autoridad Nacional de Inteligencia y Contrainteligencia y de la Autoridad Delegada para la Seguridad de la Información Clasificada, además de presidenta del Consejo Nacional de Ciberseguridad.

JAVIER FERNÁNDEZ ARRIBAS

Licenciado en Periodismo por la Universidad Complutense de Madrid, entre los años 1979 y 1991 trabajó en la Cadena COPE, primero como redactor y posteriormente como jefe de la sección de Internacional. Entre febrero y noviembre de 1991 trabajó en el diario *El Independiente* y, en el año 1992 empezó a trabajar en Onda Cero como subdirector de los Servicios Informativos. Más adelante, entre 1998 y 2004, fue subdirector de la agencia de noticias Colpisa y, posteriormente, fue director de los servicios informativos de Punto Radio durante seis años. Actualmente es director de la revista *Atalayar* y colabora como analista político en la Cadena COPE y colabora con Colpisa, RTVE y *Diariocrítico*. Ha sido galardonado con el Premio de Periodismo Europeo Salvador de Madariaga y es vicepresidente internacional de la Asociación de Periodistas Europeos.

CORONEL CARLOS JAVIER FRÍAS

Coronel de Artillería, es diplomado en Estado Mayor y doctor en Paz y Seguridad Internacionales por el Instituto Universitario General Gutiérrez Mellado, además de máster en Seguridad y Defensa y en Estudios Estratégicos y Seguridad Internacional por la Universidad de Granada. Colabora habitualmente en la revista *Ejército*, en publicaciones del Instituto Español de Estudios Estratégicos y en los *Cuadernos de Estrategia* del Centro Superior de Estudios de la Defensa Nacional.

GENERAL RAFAEL GARCÍA HERNÁNDEZ

Tras su paso por la Academia General del Aire en julio de 1983 fue destinado al Ala 78 y, posteriormente, a la Academia General del Aire, donde ejerció como profesor. En 1986 ascendió a Capitán y fue destinado al Centro de Adiestramiento de Seguridad y Defensa y, en 1991, al Ala de Alerta y Control, donde permaneció hasta su ascenso a Comandante. Tras su destino entre 1994 y 1998 en el Gabinete del Jefe del Estado Mayor del Ejército del Aire, fue destinado a SHAPE, donde prestó servicio en la División CIS para el programa ACCS de Mando y Control Aéreo. Posteriormente pasa al Grupo Central de Mando y Control como Jefe de Operaciones. En 2004 fue nombrado Agregado Aéreo de la Embajada de España en Londres y, en 2007, fue destinado al Cuartel General del Mando Aéreo de Combate. Posteriormente, fue nombrado Jefe del Grupo Central de Mando y Control y, en 2015, Jefe de la Secretaría General del Estado Mayor Conjunto. Un año después, ya como General de Brigada, fue nombrado Jefe del Sistema de Mando y Control del Mando Aéreo de Combate, destino que ocupó hasta 2018, cuando ascendió a General de División y fue nombrado Comandante del Mando Conjunto de Ciberdefensa.

JAVIER GARCÍA VILA

Licenciado en Periodismo por la Facultad de Ciencias de la Información de la Universidad Complutense de Madrid, ha desarrollado toda su carrera profesional en la Agencia Europa Press, a la que se incorporó en junio de 1987 y donde fue nombrado jefe de Cierre en 1989 y jefe de la sección de Economía en 1990. Posteriormente pasó a desempeñar el cargo de redactor jefe de Economía, desde el que creó y desarrolló el Servicio Económico de Europa Press. En 1999 fue nombrado

subdirector de la agencia y, año y medio después, en 2000, director de Internet, cargo desde el que se ocupó de la creación de una «factoría» especializada en el desarrollo e integración de contenidos específicos para internet. Desde 2002 es director de gestión del Grupo Europa Press, con responsabilidad directa sobre las áreas de Desarrollo de Negocio, Comercial, Comunicación, Internet y Servicios Informativos de Televisión. En 2008 sustituyó a Ángel Expósito como director de Europa Press, cargo que sigue desempeñando en la actualidad, al igual que el de vicepresidente segundo de la Asociación de Periodistas Europeos.

MARÍA ELENA GÓMEZ CASTRO

Licenciada en Derecho por la Universidad de Salamanca y diplomática, ha estado destinada en las representaciones españolas en Costa de Marfil, República Democrática del Congo y ante la Unión Europea. Ha ejercido como experta nacional, destacada en la dirección general, para cuestiones de defensa de la Secretaría General del Consejo de la Unión Europea. Asimismo, ha sido asesora para Asuntos Internaciones de la ministra de Defensa y subdirectora general de Seguridad en el Ministerio de Asuntos Exteriores y de Cooperación. Antes de ser nombrada Directora General de Política de Defensa (DIGENPOL), cargo que ocupa actualmente, fue representante permanente adjunta de España ante el Consejo del Atlántico Norte.

ÁNGEL GONZALO

Licenciado en Ciencias de la Información por la Universidad Complutense de Madrid en 1982, es jefe del área Internacional de Onda Cero desde su creación en 1990, cargo en el que ha cubierto acontecimientos internacionales como el primer alto el fuego del IRA, la victoria electoral de Nelson Mandela o el restablecimiento de las relaciones cuba-

no-estadounidenses. En 2000 le fue impuesta la Cruz de la Orden de Isabel la Católica y en 2008 recibió el Premio de Periodismo Europeo Salvador de Madariaga.

GEORGINA HIGUERAS

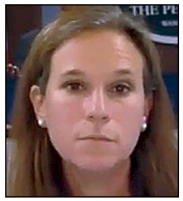
Licenciada en Ciencias de la Información por la Universidad Complutense de Madrid, estudió chino y cursó un máster en la Universidad de Pekín sobre Historia de las Relaciones Internacionales de China: de la Guerra del Opio a la Liberación (1840-1949). Entre 1982 y 1987 trabajó para la Agencia EFE, donde fue delegada en Pekín y Estrasburgo y corresponsal diplomática en Washington. En 1987 entró a formar parte de la plantilla de *El País*, donde, como corresponsal en Asia-Pacífico, cubrió los conflictos de Oriente Próximo, Camboya-Vietnam y Afganistán. En 1997 fue nombrada corresponsal de la Cadena SER en Moscú y en 2001 volvió a *El País*, donde, entre otros puestos, ocupó el de directora general de Comunicación de la Defensa entre 2009 y 2010. Es autora de los libros *China: la venganza del dragón* (2003), *El despertar de Asia* (2005) y *Haití: una apuesta por la esperanza* (2011).

LUIS JIMÉNEZ

Teniente Coronel en situación de Servicios Especiales, es especialista criptológico y máster en Dirección de Sistemas de Tecnologías de la Información y las Comunicaciones por el Instituto Nacional de Administración Pública y la Universidad Politécnica de Madrid. Actualmente es subdirector general del Centro Criptológico Nacional, vocal del Consejo Nacional de Ciberseguridad de España, representante nacional en los Comités de Seguridad de la Información y Ciberseguridad del Consejo de la Unión Europea y de la OTAN y miembro del Comité Ejecutivo de la Comisión de Estrategia TIC de la Administración General del Estado. Entre los principales cometidos de su actual puesto de trabajo se encuentran el impulso y desarrollo de la Estrategia Nacional de Ciberseguridad, el apoyo a la implementación del Esquema Nacional de Seguridad en las administraciones públicas, la mejora de las capacidades de respuesta ante incidentes de seguridad y la mejora de las capacidades de evaluación y certificación.

ALMIRANTE JUAN FRANCISCO MARTÍNEZ NÚÑEZ

Ingresó en la Escuela Naval Militar en 1972 y recibió el despacho de Alférez de Navío en el año 1977. Ha estado embarcado en las fragatas *Asturias* y *Baleares* y ha mandado el patrullero *Deva*, la corbeta *Infanta Cristina*, la fragata *Reina Sofía* y el buque escuela *Juan Sebastián de Elcano*. Es diplomado de Estado Mayor por la Escuela de Guerra Naval y diplomado del Curso de Guerra Marítima en el Reino Unido por el Colegio de Defensa de la OTAN, además de estar titulado en Ciencias Físico-Matemáticas. Entre 1993 y 1994, participó en las operaciones combinadas de mantenimiento de paz de la OTAN y la UEO en el Adriático durante el conflicto de Bosnia-Herzegovina, lo que le convirtió en el primer oficial español que se integró en el Estado Mayor de la Fuerza Naval Permanente de la OTAN en el Atlántico. En su hoja de servicios, cuenta 2.400 días de mar, embarcado en buques nacionales y aliados. Ha ocupado los cargos de consejero del secretario de Estado de Defensa para el programa de las fragatas F-100, Jefe del Gabinete del Almirante Jefe del Estado Mayor de la Armada, Jefe de la División de Planes del Estado Mayor de la Armada y Jefe de la División de Planes y Estrategia del Estado Mayor de la Defensa. Actualmente, el Almirante Martínez Núñez es Secretario General de Política de Defensa (SEGENPOL).



MADELINE MORTELMANS

Directora Principal para Política de Ciberseguridad del Departamento de Defensa de Estados Unidos, ha trabajado en la Oficina del Secretario de Defensa desde 2004, ocupando distintos cargos, incluyendo el de asistente especial de dos subsecretarios en calidad de asesora sobre estrategia y presupuestos. Antes de unirse a la Oficina de Ciberseguridad, estuvo asignada a la misión de Estados Unidos ante la Organización para la Seguridad y la Cooperación en Europa, donde ejerció como asesora del embajador sobre cuestiones de defensa y participó en las negociaciones para la construcción de medidas de confianza en el ciberespacio. Anteriormente, también fue contratista de la Agencia de Reducción de Amenazas de Defensa dentro del Programa Cooperativo de Reducción de Amenazas.

RAFAEL PANADERO

Licenciado en Ingeniería Superior de Telecomunicaciones por la Universidad Politécnica de Madrid y máster de Periodismo UAM-EL PAÍS, desde 2007 es jefe de Internacional de la Cadena SER, donde empezó su andadura en el año 2003. Como enviado especial ha cubierto procesos electorales en Estados Unidos (2008-2016), Alemania, Italia, el Reino Unido, Grecia o Serbia; el referéndum del Brexit; la sucesión de Raúl Castro en Cuba; la crisis de Grecia entre 2010 y 2015; el bloqueo de los refugiados en Idomeni; el proceso de independencia en Escocia; la muerte de Nelson Mandela; la independencia de Kosovo; la realidad política y social en el Sáhara Occidental; el terremoto de México de 2017 o la situación en la región de Nagorno Karabaj. Desde su puesto actual ha tenido la oportunidad de entrevistar, entre otros, al ex primer ministro británico Tony Blair, al secretario general de la ONU Ban Ki-moon, al expresidente de Brasil Lula da Silva o al presidente del Parlamento Europeo, Martin Schulz. También ha dirigido y presentado los programas «In Pod We Cast» (política y sociedad en Estados Unidos en tiempos de Trump) y «A cierta distancia» (análisis monográfico de asuntos de actualidad internacional). En 2009 participó en el International Visitor Leadership Program, organizado por el Departamento de Estado de Estados Unidos, y en 2014 fue galardonado con el XX Premio de Periodismo Europeo Salvador de Madariaga por su enfoque europeísta y su apuesta por convertir la información europea en una cobertura cotidiana y cercana.

IGNACIO RAMOS

Es licenciado en Filosofía por la Universidad Pontificia Comillas de Madrid y en Teología por la Hochschule Sankt Georgen, así como doctor en Filosofía por la Goethe-Universität, ambas en Frankfurt. Profesor en el Departamento de Relaciones Internacionales y delegado para Asuntos Chinos de la Universidad Pontificia Comillas, vivió cerca de tres años en Taiwán y pasa temporadas en China continental entregado a su labor académica, siempre relacionada con el encuentro con la cultura. Es autor de varios libros y diversos artículos en el ámbito de las humanidades y ha investigado y publicado sobre la figura de Diego de Pantoja, pionero del encuentro con China desde el ámbito iberoamericano. En la actualidad comisaría el proyecto de la Unión Europea *2019-2020 Cultural Routes of Europe Itinerant Exhibition*, presentado en diversas ciudades chinas.

MARGARITA ROBLES

Licenciada en Derecho en la Universidad Central de Barcelona, ingresó en la Carrera Judicial en la 27 Promoción de Jueces y Fiscales. Desempeñó los cargos de juez y magistrada en Balaguer, San Feliú de Llobregat y Bilbao antes de acceder a la Audiencia Provincial de Barcelona en 1981, convirtiéndose en la primera mujer en ocupar un órgano colegiado en España. Entre 1991 y 1993 fue presidenta de la Audiencia Provincial de Barcelona y, un año después, fue nombrada subsecretaria del Ministerio de Justicia. En 1994 fue nombrada secretaria de Estado de Interior, cargo que desempeñó hasta que, en 1996, pasó a ejercer como magistrada de la Sala de lo Contencioso Administrativa de la Audiencia Nacional. En 2004 fue nombrada magistrada de la Sala de lo Contencioso del Tribunal Supremo y, entre 2008 y 2014, ejerció como vocal del Consejo General del Poder Judicial. En 2016 fue elegida diputada por Madrid, presidiendo hasta 2017 la Comisión de Justicia del Congreso de los Diputados y ejerciendo como portavoz del Grupo Parlamentario Socialista en el Congreso hasta que, en 2018, fue nombrada ministra de Defensa.

CARMEN ROMERO

Subsecretaria general adjunta de Diplomacia Pública de la OTAN, división que se encarga de coordinar la comunicación de la Alianza Atlántica, es la mujer española con el cargo de mayor jerarquía dentro de la OTAN. Periodista de profesión y con una extensa carrera internacional, durante más de tres años fue corresponsal de la Agencia EFE en Bruselas, antes de convertirse en portavoz adjunta de la OTAN. Previamente, trabajó en las delegaciones de la Agencia EFE en París (1997-2001), Moscú (1994-1997) y Ginebra (1989-1994).

Como portavoz adjunta de la OTAN, ha trabajado con tres secretarios generales de la Alianza: el actual titular, Jens Stoltenberg, y sus predecesores en el cargo, Anders Fogh Rasmussen y Jaap de Hoop Scheffer.

GENERAL FÉLIX SANZ ROLDÁN

Ingresó en la Academia General Militar en el año 1962, recibiendo el despacho de Teniente de Artillería en julio de 1966. Ha ocupado diferentes destinos, incluyendo el de Jefe de Batería, Oficial de Plana Mayor y Agregado Militar Adjunto en la Embajada de España en Washington, hasta ser designado a la División de Planes del Estado Mayor del Ejército. Ya como Coronel, en 1997 se incorpora a la Dirección General de Política de Defensa como Jefe del Área OTAN/Unión Europea. En 2004 fue nombrado Jefe del Estado Mayor de la Defensa, ascendiendo al empleo de General de Ejército. Durante su etapa como JEMAD se aprobó la Directiva de Defensa Nacional y las leyes de Defensa Nacional y de Tropa y Marinería. En 2008 fue designado Alto Representante para la Presidencia Española de la Unión Europea en Asuntos Propios Relacionados con la Defensa, con dependencia directa del presidente del Gobierno y con rango de secretario de Estado. En 2009 fue nombrado secretario de Estado Director del Centro Nacional de Inteligencia, cargo que ostentó hasta julio de 2019.

11. RELACIÓN DE ASISTENTES

El XXXII Seminario Internacional de Seguridad y Defensa se celebró en la sede de la Fundación Diario Madrid de manera semipresencial y con un aforo reducido, acorde con las medidas establecidas a causa de la pandemia, y fue emitido por streaming *a través de distintas redes sociales. En la relación de asistentes figuran únicamente los que acudieron físicamente al seminario.*

La secretaria de Estado de Defensa entre los asistentes al seminario.

El Contralmirante Alfonso Pérez de Nanclares
y el General Rafael García Hernández.

AGUILAR, MIGUEL ÁNGEL
Secretario general de la Asociación Periodistas Europeos (APE)

ALONSO, ANA
Redactora de *El Independiente*

ANDREU JIMÉNEZ, EMILIO
Corresponsal de defensa de RNE

BABÉ, GONZALO
Presidente de la Fundación Renacimiento Demográfico

BALLESTEROS, MIGUEL ÁNGEL
General. Director del Departamento de Seguridad Nacional

CAMPUZANO, ANTONIO
Gerente de la Fundación Diario Madrid

CANTÓN, EVA
Colaboradora de *El Periódico*

CARRASCO, ANTONIO
Asociación de Periodistas Europeos (APE)

CASTELEIRO, ESPERANZA
Secretaria de Estado de Defensa

CUBEIRO CABELLO, ENRIQUE
Capitán de Navío. Jefe de Sistemas de Satelitales
y Ciberdefensa

DACOBA, FRANCISCO JOSÉ
General. Director del Instituto Español de Estudios
Estratégicos (IEEE)

Carmen Romero interviniendo desde Bruselas.

Georgina Higueras, Carlos Miranda y la DIGENPOL, María Elena Gómez Castro.

La secretaria de Estado de Defensa, Esperanza Casteleiro, la ministra de Defensa, Margarita Robles, y el secretario general de la APE, Miguel Ángel Aguilar.

DÍAZ, ROSA
Directora general del Instituto Nacional de Ciberseguridad (INCIBE)

DÍAZ DE VILLEGAS, VICENTE
Asistente del Secretario General de Política de Defensa

DOMÍNGUEZ, MONTSERRAT
Vicepresidenta de la Asociación de Periodistas Europeos y subdirectora de *El País*

ESTEBAN, MARIO
Investigador principal del Real Instituto Elcano y profesor titular del Centro de Estudios de Asia Oriental de la Universidad Autónoma de Madrid

ESTEBAN, PAZ
Directora del Centro Nacional de Inteligencia (CNI)

FERNÁNDEZ ARRIBAS, JAVIER
Director de la revista *Atalayar*

FRÍAS, CARLOS JAVIER
Coronel. Doctor en Paz y Seguridad Internacional. Colaborador del Instituto Español de Estudios Estratégicos (IEEE)

GARCÍA HERNÁNDEZ, RAFAEL
General. Comandante del Mando Conjunto del Ciberespacio

GARCÍA VILA, JAVIER
Director de Europa Press

GÓMEZ CASTRO, MARÍA ELENA
Directora General de Política de Defensa (DIGENPOL)

La directora del CNI, Paz Esteban, conversa con el General Miguel Ángel Ballesteros, director del Departamento de Seguridad Nacional.

El General García Hernández, Rosa Díaz y Ángel Gonzalo durante la sesión «¿Quién promueve los ataques cibernéticos?».

El SEGENPOL charla con los periodistas Emilio Andreu y Miguel González.

Mario Esteban (en pantalla), el Coronel Frías, Ignacio Ramos
y Georgina Higueras analizando el rol de China.

Carmen Romero (en pantalla), el General Dacoba, María Elena Gómez Castro
y Rafael Panadero en la sesión sobre la desinformación.

GONZÁLEZ, MIGUEL
Responsable de Defensa de *El País*

GONZÁLEZ, PEDRO
Analista internacional de la revista *Atalayar*

GONZALO, ÁNGEL
Jefe de Internacional de Onda Cero

GUALDA, BELÉN
Presidenta de Navantia

HERNÁNDEZ, EUGENIA
Directora del Observatorio de Política Internacional de la Universidad Francisco de Vitoria

HIGUERAS, GEORGINA
Excorresponsal de *El País* en Asia-Pacífico

JIMÉNEZ, LUIS
Subdirector general del Centro Criptológico Nacional (CCN-CERT)

JUAN, JOSÉ VICENTE DE
Director de la Fundación Diario Madrid

LÓPEZ GIL, MAR
Jefa del equipo de Ciberseguridad de la Presidencia del Gobierno

MARTÍNEZ NÚÑEZ, JUAN FRANCISCO
Almirante. Secretario General de Política de Defensa (SEGENPOL)

Aspecto del aula magna de la Fundación Diario Madrid durante el seminario.

La DIGENPOL y el SEGENPOL conversan con la presidenta de Navantia, Belén Gualda.

MIGUEL SANTOS, MARÍA DE
Consejera técnica de Ciberseguridad de la
Secretaría de Estado de Telecomunicaciones
y para la Sociedad de la Información

MIRANDA, CARLOS
Exembajador de España ante la OTAN

MORTELMANS, MADELINE
Directora principal para Política de Ciberseguridad
del Departamento de Defensa de Estados Unidos

OÑATE, JUAN DE
Director de la Asociación de Periodistas Europeos (APE)

PANADERO, RAFAEL
Jefe de Internacional de la Cadena SER

PERAL ALONSO, DANIEL
Europa en Suma

PERALTA, PEPI
Asociación de Periodistas Europeos (APE)

PÉREZ, CARLOTA
Analista internacional de la revista *Atalayar*

PÉREZ DE NANCLARES Y PÉREZ DE ACEVEDO, ALFONSO
Contralmirante. Subdirector general
de Programas del Ministerio de Defensa

RAMOS, IGNACIO
Profesor de Relaciones Internacionales y delegado para
Asuntos Chinos en la Universidad Pontificia de Comillas

La directora principal para Política de Ciberseguridad del Departamento de Defensa de Estados Unidos, Madeline Mortelmans (en pantalla), analiza los retos de la seguridad para el siglo XXI con Javier Fernández Arribas.

La directora del CNI, Paz Esteban, conversa con Montserrat Domínguez.

Asistentes al XXXII Seminario Internacional de Seguridad y Defensa, que fue transmitido a través de *streaming*.

Momentos de la clausura del XXXII Seminario Internacional de Seguridad y Defensa.

REQUENA, PILAR
Reportera de Internacional de TVE

ROBLES, MARGARITA
Ministra de Defensa

ROCA RIVEIRO, JAVIER
2º Comandante del Mando Conjunto del Ciberespacio

ROMERO, CARMEN
Subsecretaria general adjunta de Diplomacia Pública
de la OTAN

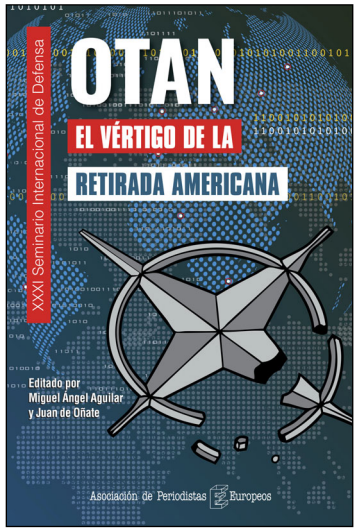
RUIZ JIMÉNEZ, ROCÍO
Redactora de la revista *Atalayar*

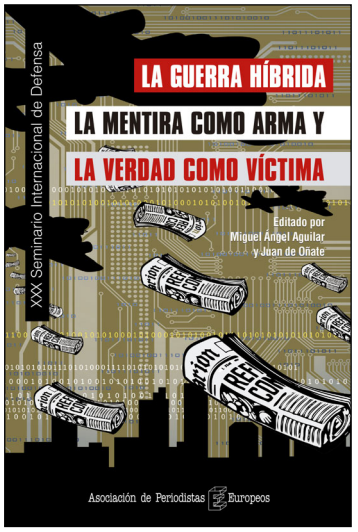
SANZ ROLDÁN, FÉLIX
General. Jefe del Estado Mayor de la Defensa (JEMAD)
entre 2004 y 2008 y director del Centro Nacional de
Inteligencia (CNI) entre 2009 y 2019

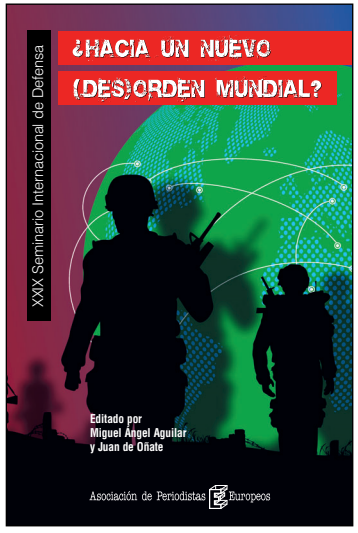
SOLER TOMÉ, ROSARIO
Colaboradora de la revista *Atalayar*

La ministra de Defensa, Margarita Robles, atendiendo a la prensa.

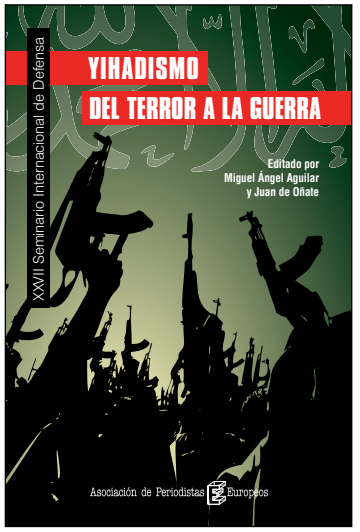
ALGUNAS EDICIONES ANTERIORES
DEL SEMINARIO INTERNACIONAL
DE SEGURIDAD Y DEFENSA


XXXI Seminario Internacional de Defensa
OTAN
EL VÉRTIGO DE LA
RETIRADA AMERICANA
Editado por
Miguel Ángel Aguilar
y Juan de Oñate
Asociación de Periodistas Europeos

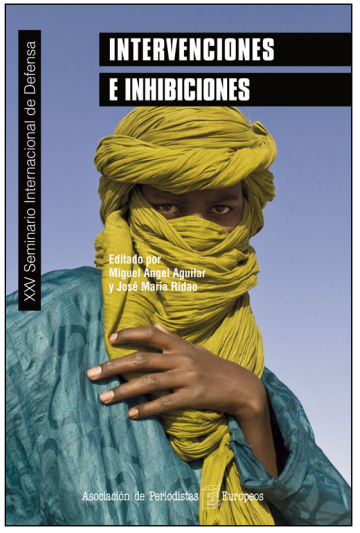

XXX Seminario Internacional de Defensa
LA GUERRA HÍBRIDA
LA MENTIRA COMO ARMA Y
LA VERDAD COMO VÍCTIMA
Editado por
Miguel Ángel Aguilar
y Juan de Oñate
Asociación de Periodistas Europeos

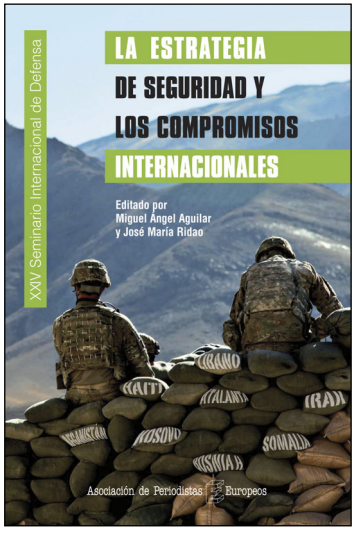

XXIX Seminario Internacional de Defensa
¿HACIA UN NUEVO
(DES)ORDEN MUNDIAL?
Editado por
Miguel Ángel Aguilar
y Juan de Oñate
Asociación de Periodistas Europeos


XXVIII Seminario Internacional de Defensa
EUROPA AMEDRENTADA
LA AMENAZA DEL YIHADISMO
Editado por
Miguel Ángel Aguilar
y Juan de Oñate
Asociación de Periodistas Europeos

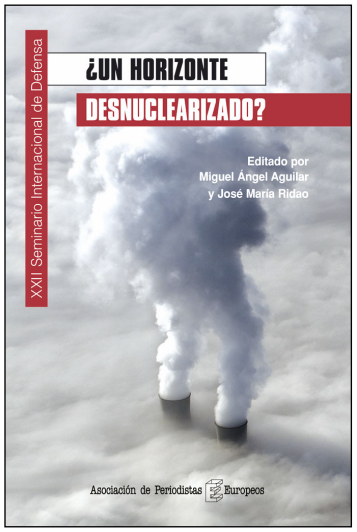

XXVII Seminario Internacional de Defensa
YIHADISMO
DEL TERROR A LA GUERRA
Editado por
Miguel Ángel Aguilar
y Juan de Oñate
Asociación de Periodistas Europeos


XXVI Seminario Internacional de Defensa
CIBERAMENAZAS
Y RESPUESTAS
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

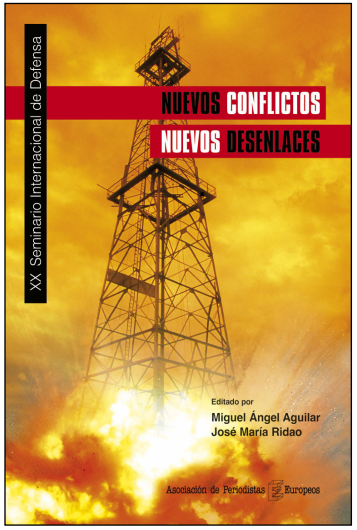

XXV Seminario Internacional de Defensa
INTERVENCIONES
E INHIBICIONES
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

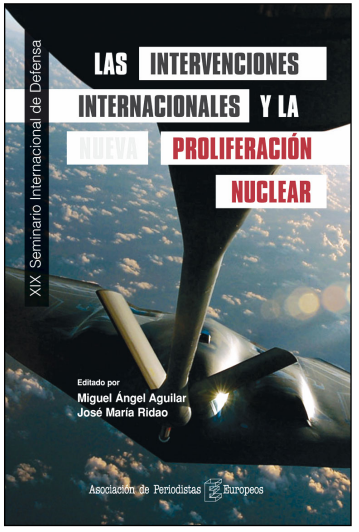

XXIV Seminario Internacional de Defensa
LA ESTRATEGIA
DE SEGURIDAD Y
LOS COMPROMISOS
INTERNACIONALES
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

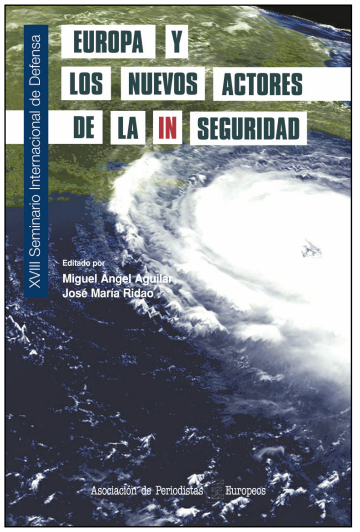

XXII Seminario Internacional de Defensa
NUEVOS PARADIGMAS
DE DEFENSA Y SEGURIDAD
Editado por
Miguel Ángel Aguilar y José María Ridao
Asociación de Periodistas Europeos

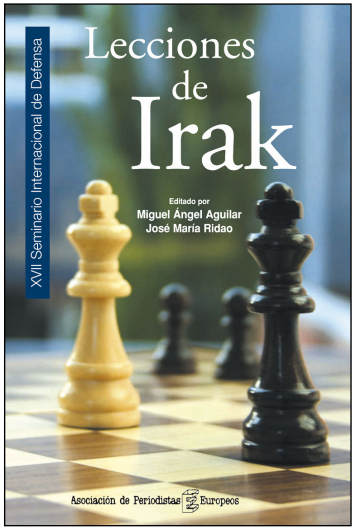

XXII Seminario Internacional de Defensa
¿UN HORIZONTE
DESNUCLEARIZADO?
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos


XXI Seminario Internacional de Defensa
LAS MIRADAS DE EUROPA
Y SU VOZ FRAGMENTADA
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

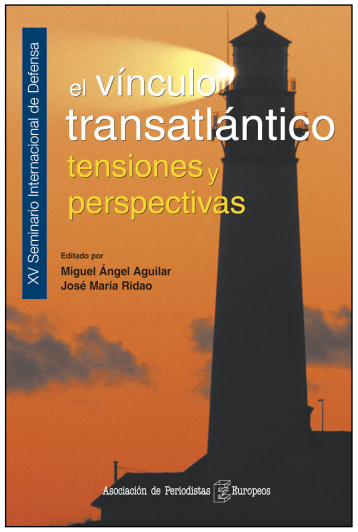

XX Seminario Internacional de Defensa
NUEVOS CONFLICTOS
NUEVOS DESENLACES
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos


XIX Seminario Internacional de Defensa
LAS INTERVENCIONES
INTERNACIONALES Y LA
NUEVA PROLIFERACIÓN
NUCLEAR
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos

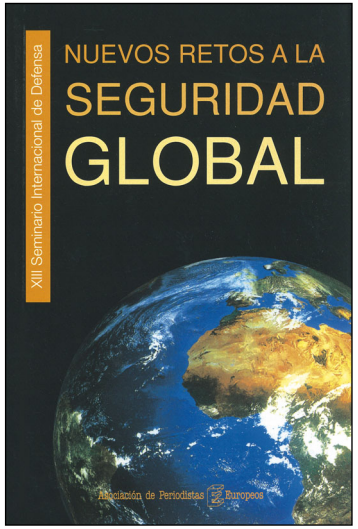

XVIII Seminario Internacional de Defensa
EUROPA Y
LOS NUEVOS ACTORES
DE LA IN SEGURIDAD
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos

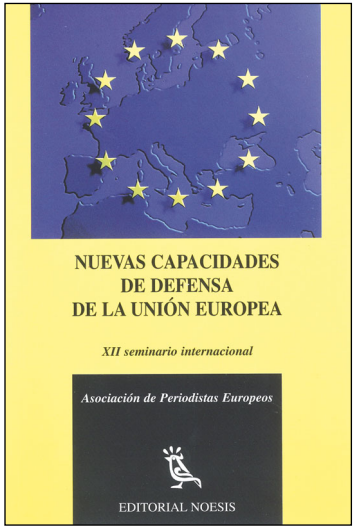

XVII Seminario Internacional de Defensa
Lecciones
de
Irak
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos


XVI Seminario Internacional de Defensa
Conceptos para
la seguridad
en el siglo XXI
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos


XV Seminario Internacional de Defensa
el vínculo transatlántico
tensiones y perspectivas
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos


XIV Seminario Internacional de Defensa
el terrorismo una amenaza del siglo XXI
Miguel Ángel Aguilar
José María Ridao
guerra sin enemigo
paz sin seguridad
Asociación de Periodistas Europeos


XIII Seminario Internacional de Defensa
NUEVOS RETOS A LA SEGURIDAD GLOBAL
Asociación de Periodistas Europeos


NUEVAS CAPACIDADES
DE DEFENSA
DE LA UNIÓN EUROPEA
XII seminario internacional
Asociación de Periodistas Europeos
EDITORIAL NOESIS