XXVI SEMINARIO INTERNACIONAL DE DEFENSA

CIBERAMENAZAS Y RESPUESTAS

XXVI SEMINARIO INTERNACIONAL DE DEFENSA

CIBERAMENAZAS Y RESPUESTAS

Edición a cargo de
Miguel Ángel Aguilar y José María Ridao

Toledo, 24 y 25 de junio de 2014

Asociación de Periodistas Europeos

Cedaceros, 11; 28014 Madrid
Teléfono: 91 429 68 69
info@apeuropeos.org
www.apeuropeos.org

Coordinación
Juan Oñate

Edición y traducción de textos
Andrea Aguilar y Asociación de Periodistas Europeos

Fotografías
Diego de la Vega

Diseño y producción editorial
Exilio Gráfico

Impresión
Gracel

Impreso en España
Depósito legal: M-18842-2015

ÍNDICE

1. PRÓLOGO

Imagen del XXVI Seminario Internacional de Defensa

AVANCES Y VULNERABILIDADES EN LA RED

Reconozcamos que, al llegar a su vigesimosexta edición, el Seminario Internacional de Defensa promovido por la Asociación de Periodistas Europeos mantiene su fidelidad a los propósitos originarios de favorecer un espacio de reflexión intelectual y fomentar el contacto personal entre los actores implicados en este ámbito. Al iniciar estas tareas en las profundidades de 1983, los asuntos de la defensa y de las Fuerzas Armadas estaban fuera de la agenda de los medios de comunicación; se arrastraba la inercia del régimen franquista, durante el cual había 364 días de abstinencia y uno de empacho entusiasta y declamatorio para arropar el llamado «Desfile de la Victoria». Por aquel entonces, como la asignación de recursos se decidía a la manera autoritaria, nadie tomaba a su cargo presentar las necesidades de manera convincente ante la opinión pública.

En democracia, en cambio, es el Parlamento quien aprueba los Presupuestos Generales del Estado y sin el respaldo de la ciudadanía se hacía imposible allegar los dineros necesarios. Sucedía, además, que las Fuerzas Armadas españolas, en vez de formar parte de la defensa, eran percibidas como parte de la amenaza. En particular, los periodistas consideraban que todos los militares eran golpistas, mientras que los militares, instalados en una susceptibilidad muy acusada, tendían a pensar que todos los periodistas eran unos indeseables «hijos de puta». Fue en esos

tiempos de antagonismo radical cuando surgieron estos encuentros, que perseguían entre sus objetivos romper esas incompatibilidades en aras de un acercamiento que generase comprensión; siempre mediante una estrategia de aproximación indirecta, conforme la describe Liddell Hart. Por eso las diferencias mencionadas nunca figuraron de modo explicito en el orden del día de las jornadas, donde fueron preferidos asuntos en los que fuera posible la identificación de un interés compartido, aunque los ángulos de análisis fueran distintos.

En la tribuna del seminario se presentaron a lo largo de sus convocatorias notables anticipaciones, como la de Hélène Carrère d'Encausse al anunciar el derrumbe del gigante soviético por el que tan amenazados se sentían el presidente norteamericano Ronald Reagan y la primera ministra británica Margarita Thatcher. También Salomé Zourabichvili, asesora del Elíseo en materia de Defensa, afirmó en junio de 2001 que la que denominábamos *«guerra limpia»* –del todo asimétrica, combatida a distancia y capaz de causar un daño colosal al adversario sin sufrir bajas propias– tendría como respuesta la utilización del más sucio de los terrorismos. Una predicción clarividente, como se vio unos meses después con los atentados de las Torres Gemelas. Después de tantos años de protegernos de la amenaza de los poderosos –dijo entonces Zourabichvili–, convendría empezar a prepararnos para defendernos de los débiles. Otro momento estelar estuvo a cargo de Jiri Dienstbier, antiguo ministro de Asuntos Exteriores de la Checoslovaquia aún unida, quien predijo con más de un año de antelación la proclamación unilateral de independencia de Kosovo con el padrinazgo de Estados Unidos.

La amenaza del débil, identificada como riesgo creciente, aportaba una prueba más de la rapidez con que históricamente evolucionan los riesgos. Poco más de una década después se ha producido otro cambio, si cabe, aún más significativo referido al propio formato que adopta la amenaza. En efecto, la agresión urdida mediante estrategias cibernéticas se ha superpuesto a las

amenazas tradicionales, con sus características sutiles, su manejo a distancia y su peculiar economía, además del aliciente del anonimato y la reducción del uso de la violencia. Y todo ello multiplicando los daños. En palabras de Clausewitz: «El conquistador es siempre un amante de la paz que preferiría, sin duda, someter nuestro país sin tener que combatir». La cita del militar prusiano cobra vigencia ahora que las ciberamenazas ahorran combates y limitan ese derramamiento de sangre tan desprestigiado que caracterizaba la guerra tradicional, pero siguen horadando la seguridad sin distinguir entre combatientes de primera línea y población civil.

Sobre estas nuevas amenazas de muy difícil detección y sobre sus posibles respuestas versó la vigesimosexta edición del seminario. De sus sesiones pudo concluirse la esterilidad de una defensa nacional emprendida por cuenta propia y desconectada de alianzas geográficas y sectoriales. Se consideró imprescindible esta colaboración entre países y entre los sectores público y empresarial, pero también se demostraron fundamentales la inteligencia, en sus vertientes civil y militar, y una apuesta convencida por la investigación, el desarrollo y la innovación.

Se trata de protegernos, de proteger nuestra información, de proteger las infraestructuras críticas, pero también de proteger la intimidad y defender en ocasiones la opacidad, tal y como defiende Byung-Chul Han en *La sociedad de la transparencia*, donde el pensador coreano nos recuerda que «vivo de aquello que los otros no saben de mí. [...] Sin duda el alma humana necesita esferas en las que pueda estar en sí misma, sin la mirada del otro. [...] Está demostrado que más información no conduce de manera necesaria a mejores decisiones. La intuición, por ejemplo, va más allá de la información disponible y sigue su propia lógica. Hoy se atrofia la facultada superior de juzgar a causa de la creciente y pululante masa de información. Con frecuencia, un menos de saber e información produce un más. La negatividad de dejar y olvidar tiene no pocas veces un efecto productivo. La so-

ciedad de la transparencia no permite lagunas de información, ni de visión, pero tanto el pensamiento como la inspiración requieren un vacío. Y una sociedad que no admitiera ya ninguna negatividad de un vacío sería una sociedad invivible». Decía también nuestro autor que «la teoría está cerca de la ceremonia que separa a los iniciados de los no iniciados». Y, desde luego, en lo relativo a las ciberamenazas la separación entre iniciados y no iniciados es asombrosa; por eso le aconsejo, amigo lector, que se adentre en las reflexiones que contienen estas páginas y pase a ser uno de los iniciados en las ciberamenazas y sus respuestas.

Miguel Ángel Aguilar y José María Ridao
Madrid, mayo de 2015

2. LA NUEVA AMENAZA

GREG AUSTIN
Miembro Investigador del
East-West Institute (Australia)

Moderador
JAVIER FERNÁNDEZ ARRIBAS
Director de *Atalayar*


Javier Fernández Arribas y Greg Austin

Nos defendemos de las amenazas, pero las amenazas cambian de modo acelerado. Es menos frecuente que el cambio se produzca en el formato de la amenaza. Parece generalizada la idea de que ahora hay una nueva variable en la ecuación de la seguridad, cuya magnitud se acrecienta al ritmo de las nuevas tecnologías: se trata de la ciberseguridad, que en su aplicación al terreno militar, llamamos la ciberdefensa.

En un momento en que las amenazas han dejado de provenir tan sólo de naciones identificadas y tienen origen en Estados fallidos, grupos terroristas o incluso «lobos solitarios», el recurso a los ciberataques supone un medio rápido y ágil que, sin necesidad de grandes movilizaciones de efectivos, vulnera la seguridad de nuestros países de manera sensible. Este uso de estrategias cibernéticas tiene efectos letales y no requiere el empleo de grandes medios económicos. Además, se ampara en el anonimato y limita la visibilidad gráfica de los conflictos, reduciendo el uso de la violencia aun cuando se maximiza el daño. Se cumple así la máxima de Clausewitz, según la cual: «El conquistador es siempre un amante de la paz; que preferiría sin duda someter nuestro país sin tener que combatir».

En todo caso, parece claro que a partir de ahora todas las operaciones de guerra convencional estarán acompañas de operaciones en el ciberespacio.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

En esta primera ponencia del XXVI Seminario Internacional de Defensa hablaremos de «la nueva amenaza». Parece claro que, a partir de ahora, todas las operaciones de guerra convencional estarán acompañas de operaciones en el ciberespacio. Pensemos, sin ir más lejos, en las acusaciones que en los últimos tiempos se cruzan superpotencias como China y Estados Unidos en su pugna por la hegemonía internacional.

Para hablar de todo esto está con nosotros Greg Austin, investigador del East-West Institute de Nueva York, institución de la que ha sido vicepresidente del Área de Seguridad Global y de la que ahora es Miembro Investigador. Austin es autor y coautor de diversos estudios sobre las estrategias de China y Rusia, incluyendo todos los elementos de desarrollo militar y de estrategia. Asimismo, es especialista en lucha contra el terrorismo y crimen organizado en el marco del G-8. En 2003 lideró el equipo de asesoramiento del Gobierno británico para la prevención de conflictos y ha trabajado también para los gobiernos del Reino Unido y de Australia, país éste último del que es originario.

GREG AUSTIN
Miembro Investigador del East-West Institute

China, Rusia y Estados Unidos están de acuerdo en una cosa: la era de la información, la aplicación de tecnología militar avanzada, ha transformado la seguridad nacional. Hay un nuevo paradigma. Y estos países también estarían de acuerdo en que la tecnología, como los criminales que la explotan, avanza a una velocidad superior a la respuesta de los gobiernos. Durante mi intervención, trataré de apuntar algunas ideas sobre cómo podemos cerrar esa brecha entre la rápida transformación del ciberespacio y la lenta respuesta gubernamental. Para ello me cen-

traré en dos temas de gran amplitud: el panorama de las amenazas emergentes y el ambiente cambiante de las respuestas. Quiero ofrecer un adelanto sobre las conclusiones a las que nos conducirá mi charla. Presentaré tres ideas principales. La primera es que aumentan las amenazas a la seguridad del ciberespacio tanto en el terreno civil como en el militar. El año pasado la colaboración entre la comunidad internacional para tratar esas amenazas sufrió importantes reveses; algunos de ellos probablemente irrecuperables. Si las superpotencias no hablan de ciberespacio y ciberdefensa, ¿tenemos una crisis global de ciberseguridad?

Pero, antes de continuar, quiero presentarles el East-West Institute, para que entiendan por qué estoy aquí. El instituto representa una nueva forma de colaboración internacional en temas de ciberseguridad. En la presentación de estas jornadas se ha hablado del origen de este seminario y me gustaría añadir que en cuestiones cibernéticas es el momento de que los militares salgan de los barracones. No podemos permitirnos que los militares estén aislados de la sociedad civil y de los gobiernos en los trabajos de cooperación que se desarrollan para alcanzar una respuesta a las amenazas del ciberespacio. El East-West Institute fue fundado en 1980, durante uno de los momentos álgidos de la Guerra Fría. El proyecto trataba de canalizar consultas privadas entre oficiales de países miembros de la OTAN y de países pertenecientes al Pacto de Varsovia, así como entre expertos académicos de ambos lados. La idea era reunir a las partes para generar un diálogo en torno a la guerra y a la paz, y también catalizar el nuevo pensamiento que se generaba a ambos lados. El *modus operandi* se organizó con el fin de concentrarnos en dos áreas de actuación. Por un lado, el instituto facilitó encuentros privados y, por otro, trató de generar conocimiento e ideas. Tras la caída del muro –y después de que, en 1989, el Gobierno alemán reconociese el papel que en el fin de la Guerra Fría jugó el instituto y su presidente, John Morose– cambiamos el foco de trabajo hacia el nuevo contexto, centrándonos en la liberalización

política y económica del bloque de países de la antigua Unión Soviética. Pero nuestro *modus operandi* no cambió: seguimos reuniendo a gente para solucionar problemas y fomentando la generación de conocimiento e ideas entre todos.

En 2005 dejamos la región euro-atlántica y nos concentramos en China y en otros temas globales, como la lucha contra el terrorismo y la seguridad energética. De nuevo, mantuvimos los mismos principios fundacionales y nos volcamos en la diplomacia, mediante conversaciones privadas, y en la generación de ideas para fomentar el cambio político. El instituto empezó a trabajar en temas de ciberseguridad en 2010. Durante un par de años se realizaron consultas sobre temas de seguridad a oficiales de seguridad de los gobiernos de China, Rusia, India y Estados Unidos, para tratar de ver qué podíamos hacer. Después de recabar estas opiniones pusimos en marcha una serie de actividades y adoptamos la postura de que había algunas características comunes e inevitables en la respuesta de los gobiernos ante las ciberamenazas y la gobernanza del ciberespacio.

Supongo que muchos de ustedes saben esto, pero la respuesta ante las ciberamenazas tiene que ser colaborativa y multinacional, tiene que ser pública y privada, tiene que ser civil y militar y tiene que ser multidisciplinar. Ninguna organización tiene todos los efectivos, ni mucho menos todas las respuestas. Así que el instituto trata de contribuir modestamente a través, una vez más, de reuniones privadas y de la generación de conocimiento entre las partes en conflicto. Así, por ejemplo, hemos montado reuniones y grupos de trabajo entre miembros del Gobierno chino y estadounidense alrededor de temas como el *hacking* o el *spam*. En el futuro tenemos previsto celebrar sesiones con oficiales chinos para abordar temas como la protección de los menores en Internet y la defensa de la propiedad intelectual.

Quiero añadir que yo me formé en inteligencia de defensa. Pasé quince años trabajando con oficiales de inteligencia de Estados Unidos y el Reino Unido y acabo de terminar un libro

sobre ciberseguridad en China; algo de lo que podemos hablar en el turno de preguntas si quieren.

Volviendo al asunto de amenazas futuras, –y me disculpo si muchos de ustedes conocen parte de este material–, una manera de entender estas ciberamenazas futuras es fijándonos en cómo la cibersuperpotencia ve el asunto. Me refiero, por supuesto, a los Estados Unidos. Dado que España es un aliado de Estados Unidos, aquí no tienen que preparar una defensa contra las operaciones estadounidenses, pero no hay que olvidar que las operaciones estadounidenses determinan el ambiente de las ciberoperaciones a nivel global. La razón de esto es que si los adversarios de Estados Unidos tienen que vérselas con las ciberoperaciones, las cibercapacidades y la ciberplanificación de Estados Unidos, esos adversarios se centrarán en los aliados de la superpotencia para tratar de entender lo que hace y debilitar el valor de ese aliado para Estados Unidos. De manera notable, la alianza con Estados Unidos impone una carga en países aliados como España, porque este país, como otros, sufre las consecuencias de las ciberoperaciones globales de Estados Unidos. Antes, los aliados de Estados Unidos podían actuar en su territorio, pero ahora las implicaciones de ser un aliado de esta superpotencia es que estos países han saltado al escenario global en el ciberespacio. ¿Cuál es la perspectiva de Estados Unidos en las operaciones de inteligencia? A este respecto tenemos buenas fuentes de información. Hay un documento, conocido como la directiva presidencial, en el que encontramos una buena fuente de información sobre el punto de vista de Estados Unidos sobre las ciberoperaciones. Tenemos pues un documento de máxima seguridad de Estados Unidos que ha sido desclasificado, como es la directiva presidencial para el Gobierno dictada en octubre de 2012, y también tenemos el documento publicado en ese mismo momento conocido como el Manual para Operaciones Conjuntas en Ciberoperaciones. En estos papeles no se habla de ciberguerra, sino de ciberoperaciones, pero tenemos que matizar

cuál es la definición estadounidense de ciberoperaciones. La directiva presidencial PPD-20 no sólo habla de ordenadores, de Internet y de redes, sino que afecta también a servidores, redes de telecomunicaciones y administradores en cualquier sistema operativo que funcione con control remoto. Las ciberoperaciones en Estados Unidos buscan anular la confidencialidad, integridad o viabilidad de los sistemas, no sólo de las máquinas. Así que las operaciones están dirigidas a las máquinas, pero también a crear un impacto y distorsionar la información que se transmite. Los documentos oficiales antes mencionados hablan de la necesidad de acometer operaciones de ciberataque. Les voy a leer un extracto de uno de ellos, el PPD-20, que fue filtrado a la prensa y que dice que «las operaciones de ciberataque ofrecen una forma única no convencional de penetrar en lugares de todo el mundo con poco o ningún aviso, provocando efectos potenciales que pueden ir desde lo sutil a lo realmente dañino». Así que España, como Australia, como país aliado de Estados Unidos, está inevitablemente implicada en este ambiente de ciberoperaciones.

La postura estadounidense en este dominio puede resumirse diciendo que el ciberespacio abarca la totalidad del mando y control estratégico, así como la diseminación de inteligencia de la que depende la seguridad militar. Y también abarca todos los sistemas digitales en uso que afectan a las infraestructuras críticas civiles. El ciberespacio no es un terreno ajeno a la guerra, sino precisamente el lugar donde la guerra moderna se libra y podrá ser perdida o ganada. En este sentido, es importante señalar que no sólo Estados Unidos tiene una doctrina sobre el dominio de información, sino que China también la tiene. Rusia no la tiene claramente definida, pero cabe asumir que tendrá las mismas aspiraciones de dominio.

Así que, aunque España no estuviera en primera línea en el enfrentamiento entre la OTAN y el Pacto de Varsovia durante la Guerra Fría, ahora está mucho más cerca de la línea de enfrentamiento en el ciberespacio. Quiero citar algunos ejemplos de

cómo España está involucrada en esta red global. España aloja desde hace una década en su territorio el servidor raíz 14, que es el destino de once de los más de cien cables submarinos de la red, que transportan el 95% de las comunicaciones transoceánicas, especialmente el tráfico de alta velocidad en Internet. España es pues un territorio crítico para los cables del oeste de África y para la mitad de los cables que comunican Egipto y el Golfo Pérsico con Europa y Estados Unidos. No hay duda de que la infraestructura de estos cables submarinos es uno de los elementos más vulnerables del ciberespacio. En cualquier conflicto militar, e incluso en los momentos previos a que el conflicto estallara, esta infraestructura de los cables de comunicación será un objetivo de alta prioridad. España también alberga en su territorio bases estadounidenses. El nuevo director de la Agencia Nacional de Seguridad de Estados Unidos, el Almirante Michael Rogers, cumplió servicio como responsable de Asuntos Relacionados con el Ciberespacio en la base de Rota. Así que debemos concluir que España, como aliado y socio de Estados Unidos, está en la primera línea del frente en lo que respecta a la protección de los sistemas globales de comunicación que sostienen el sistema económico y financiero de la comunidad global.

El tercer escenario del que quería hablarles no es exclusivo de la ciberguerra, pero sin duda es uno de los retos de la ciberseguridad. Me refiero a los aspectos no militares, que son igualmente importantes. Rápidamente, voy a hablar de tres organizaciones y de lo que han dicho de este tercer escenario posible. Hay un programa de la Unión Europea para la ciberseguridad que identifica diecinueve características en el panorama de posibles amenazas futuras. Yo les señalaré nueve. Habrá más ciberataques a vehículos armados y aparatos robóticos. Habrá más ataques a la infraestructura electrónica. Podemos esperar recibir ataques físicos en centros de datos, por no mencionar bases que conectan el cableado submarino. Debemos esperar un ascenso en la violencia cibernética que pretende penetrar sistemas para

manipularlos con el fin de que los aviones, las redes de transporte y las demás infraestructuras críticas se descompongan, causando muertes. Luego nos adentramos en áreas más complejas, como un sofisticado mercado de operaciones cibernéticas ilegales a través de *hackers*, robo de identidad cibernética de miembros destacados de la esfera política, y técnicas sofisticadas de manipulación. Hoy vemos destellos de todo esto, pero se espera que en el futuro todo esto ocurra de forma mucho más intensa, hasta el punto de determinar nuestro futuro teatro de operaciones.

Un marco más simple que puede servir para describir las posibles amenazas del futuro fue resumido por una organización australiana de una forma que creo simplifica la descripción de las amenazas al tiempo que explican la severidad de este ambiente de amenazas. Habla dicha organización de un creciente número de vectores de amenaza que evolucionan a través del *malware*. Ésta es una buena manera de presentar el asunto a los políticos encargados de legislar, pues las organizaciones encargadas de responder a las ciberamenazas tienen que recibir más recursos y hay que prestarles más atención. Éste es un dilema que afecta a todos los países.

Para hablar de las ciberamenazas de forma aún más sencilla, el Foro Económico Mundial celebrado en enero de 2014 habló del peligro que supone la total fragmentación de Internet y sugirió que es posible que la aparición de tan sólo una nueva tecnología disruptiva nos separe de que los atacantes logren sus objetivos e Internet deje de ser un medio en el que se pueda confiar para la comunicación. No todo el mundo está de acuerdo con esto; de hecho, la mayoría de la gente está en desacuerdo, pero es importante tenerlo en cuenta. Además, incluso la gente que se muestra crítica con esta visión cree que la acumulación de amenazas se vuelve relevante al hablar de la fragmentación de Internet y de una gradual pérdida de confianza.

¿En qué lugar nos deja esto en relación con la evolución de las respuestas? Las circunstancias varían de país a país, así que

es complicado generalizar, pero se pueden ofrecer algunas líneas generales sobre la legislación aprobada al respecto. Como no quiero aburrirles con mi opinión, citaré un informe del Departamento de Estado de Seguridad de Estados Unidos y su balance de la situación futura del teatro de operaciones. El primer punto alude a los nuevos paradigmas de seguridad y defensa. Esto es algo fundamental y por eso Estados Unidos creó el Mando Cibernético, como también lo ha hecho España. Pero, para entender el nivel de penetración de este cambio de paradigma, para ver cómo se desarrolla en distintos países, tenemos que hacernos la siguiente pregunta: ¿han transformado su paradigma suficientemente rápido todos los países?

El segundo punto es uno con el que ustedes ya están familiarizados y que tiene que ver con la necesidad de una sólida colaboración internacional. El Departamento de Estado también identifica el creciente volumen y sofisticación de las ciberamenazas; algo que demanda una mayor concienciación, así como la implementación de tecnología segura, una respuesta coordinada ante los incidentes y una resistencia probada en las funciones críticas. Todo esto suena a lo ya conocido, a algo que todo el mundo tiene ya, pero en algún momento habrá que comprobar si el nivel de respuesta está a la altura del nivel de la amenaza. El mencionado informe habla de la necesidad de contar con una plantilla profesionalizada de trabajadores, que es algo apremiante para responder a las ciberamenazas. No hay ningún país en el mundo que tenga suficientes profesionales dentro de sus fronteras como para protegerse de todos los ciberataques. Estados Unidos no tiene suficiente gente para hacerlo. China tampoco puede defender todo lo que quiere defender en el ciberespacio. Y países como Australia o España, de forma parecida, también se enfrentan a este enorme reto de cómo manejar a los trabajadores en el área de ciberseguridad.

El tercer punto del informe señala la creciente y cada vez más profunda dependencia de Internet para el intercambio de infor-

mación y el aumento del número de usuarios; el mundo se está haciendo cada vez más cibernético y la defensa tiene que enfrentarse a este incremento exponencial de uso y actividad. Para responder a esto –siempre según el informe– tenemos que volcarnos en aproximaciones que partan de la gestión de peligros y las respuestas serán distintas en los distintos países y organizaciones.

Retomo el proyecto 2020 de la Unión Europea que mencioné antes, pues identifica algunos aspectos interesantes del futuro. Algunas de las cosas ya las conocerán, como la idea de que surgirán nuevos poderes cibernéticos. También señala que la diplomacia cibernética y la diplomacia tradicional se convertirán en una sola cosa. Veremos si se produce un enfrentamiento entre dos países por alguna cuestión relativa a Internet y si eso también afectará a la seguridad y los intereses diplomáticos tradicionales. También habrá crecientes tensiones entre los gobiernos y las multinacionales, algo que ya es patente en Estados Unidos tras el caso Snowden. Y también veremos más presión sobre las infraestructuras críticas y cómo los ciudadanos exigirán tener más voz en estos asuntos capitales. Así que lo primero que se pude extraer de todo esto es que la respuesta colaborativa es algo esencial en la política de ciberseguridad de cualquier país.

Quiero volver a la pregunta que planteé al principio de mi intervención. ¿Estamos enfrentándonos a una crisis global en el ciberespacio? Estados Unidos y Rusia restablecieron el diálogo recientemente –durante la comisión presidencial de junio de 2013– para la colaboración oficial en asuntos cibernéticos, pero esto quedó suspendido en abril de 2014 por la anexión de Crimea. Este diálogo es de gran importancia. De hecho, ya en 1998, el presidente Yeltsin y el presidente Clinton celebraron una reunión y, entre otras muchas cosas, decidieron que era importante establecer un diálogo entre ambos países sobre el ciberespacio. Pero no se puso en marcha hasta 2009 o 2010. Así que hubo un retraso de unos trece años hasta que, finalmente, se reunieron y empezaron a negociar; alcanzaron un acuerdo relativo a una línea caliente de

comunicación pero, como les digo, todo esto ha quedado suspendido por la crisis de Crimea y ahora el ciberespacio vuelve a estar fuera de las mesa de diálogo entre Rusia y Estados Unidos.

Si nos fijamos en la situación entre Estados Unidos y China, resulta que la detención por parte de Estados Unidos de cinco PALs con cargos de ciberespionaje ha resultado en la suspensión de la colaboración recientemente inaugurada entre ambos países para asuntos relativos a la ciberseguridad. Así que en junio de 2013 China y Estados Unidos acordaron abrir un diálogo sobre este asunto y colaborar, pero hace un par de meses, ante las detenciones, las conversaciones han quedado rotas.

Quería hablar del caso de Edward Snowden y el potente impacto que los documentos que ha filtrado han causado en el nivel de confianza entre países en temas relativos al ciberespacio y la colaboración internacional. Podemos ver claramente los efectos que ha tenido en la relación de Estados Unidos y aliados claves, como Alemania o Brasil, pero además ha aumentado el deseo de Rusia y China de alcanzar a Estados Unidos e igualar sus capacidades en el ciberespacio. El Gobierno chino nunca ha sido ingenuo respecto de las capacidades de Estados Unidos en el ciberespacio, pero una vez que las declaraciones de Snowden se hicieron públicas reafirmó su deseo de igualar a Estados Unidos en el ciberespacio y, en febrero de 2014, declaró que pronto se convertirá en una potencia en el ámbito del ciberespacio. China jamás había dicho algo así antes. Hay una larga historia detrás de esta afirmación, que es de gran relevancia.

Otro efecto importante de las revelaciones de Snowden es un giro marcado de las multinacionales, alejándose de la colaboración voluntaria con el Gobierno estadounidense, pues las filtraciones de Snowden han alterado visiblemente las relaciones de confianza. Cualquier ejecutivo dirá abiertamente que su relación de confianza ha cambiado totalmente respecto al Gobierno de Estados Unidos; y un alto cargo del Gobierno chino diría exactamente lo mismo. También ha habido un cambio en la relación

de confianza de los ciudadanos para con las agencias de seguridad e inteligencia después de que salieran a la luz los papeles de Snowden. Así que creo que se puede decir que, efectivamente, tenemos una crisis global en el ciberespacio.

Al principio de mi intervención he planteado la idea de que quizá nos enfrentemos a una futura crisis global en el ciberespacio y de que sus efectos pueden ser irreversibles. Quiero decir que esa idea ha hecho que redoblemos nuestros esfuerzos en el East-West Institute. Seguimos adelante con nuestro trabajo con los gobiernos de China, Rusia y Estados Unidos, así como con multinacionales punteras, trabajando en estos temas, buscando una nueva forma de colaboración entre militares, civiles, multinacionales y gobiernos. Y, como ya he dicho, si los militares van a estar implicados en la ciberdefensa tienen que salir de los barracones, porque hay cosas que no se pueden hacer sólo en el ámbito puramente militar. El East-West Institute ha creado una serie de grupos para reunir a representantes de las Fuerzas Armadas, de las corporaciones, de los gobiernos y de la sociedad civil. En diciembre de 2014 celebraremos una cumbre en Berlín con los distintos grupos, en un evento organizado por el Ministerio de Asuntos Exteriores de Alemania. Necesitamos la colaboración de todos los gobiernos para poder presentar soluciones y conclusiones, y debo decir que hemos tenido una buena acogida por parte de gobiernos, corporaciones y militares.

Para terminar mi intervención sólo quiero volver a plantear la pregunta con la que arranqué: ¿nos enfrentamos a una crisis global en el ciberespacio?

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Hay muchos temas encima de la mesa y el papel de España nos plantea una situación interesante y también delicada. Abrimos ahora el turno de preguntas.

JENS WERNER MÜLLER
Agregado adjunto de Defensa de la Embajada
de Alemania

Quería preguntar acerca del trabajo de su instituto y su colaboración con China. Ha mencionado el documento de dominio de información elaborado por el Gobierno chino y ha dicho que China no tiene suficiente gente para protegerse, pero yo diría más bien que a China le falta gente para atacar todos los objetivos que se ha marcado a nivel global. Cuando el East-West Institute colabora con China en estos grupos de trabajo, ¿qué buscan exactamente? Para mí se trata de una situación que podría ser definida como «acostarse con el enemigo». No veo posible que logremos alcanzar un terreno común con China, porque sus objetivos son precisamente nuestros ministerios de Defensa y nuestras Fuerzas Armadas. ¿Cuál es la idea detrás de estas reuniones con China?

GREG AUSTIN
Miembro Investigador del East-West Institute

Gracias por su pregunta, que tiene muchas partes. Yo contestaré también por partes. El Gobierno chino, como el español o el estadounidense, tiene una serie de intereses económicos, de seguridad, políticos, sociales, etcétera. En efecto, está claro que existe una diferencia en la escala de valores entre Estados Unidos y China en casi todos estos campos, pero la prioridad política de ambos países, tanto de China como de Estados Unidos, es promocionar una colaboración económica pacífica, promover la prosperidad y evitar el conflicto. Las políticas de ciberseguridad de ambos gobiernos generan una intensa ansiedad en los gobiernos contrarios. Estados Unidos se toma muy en serio el uso de China del ciberespacio en dos dominios: uno es el tema de la supresión de los derechos humanos y el uso de Internet para lo-

grarlo; el otro es el ciberespionaje. Pero Estados Unidos no se toma tan en serio la capacidad militar de China en el ciberespacio.

Si miramos el caso de China, la situación es casi inversa. El Gobierno de ese país está muy preocupado por lo que considera que son acciones contra el poder del Gobierno chino procedentes de organizaciones estadounidenses, pues no se considera capaz de competir con Estados Unidos en aplicaciones militares en el ciberespacio ni en la guerra de la información. China ve a Estados Unidos como una superpotencia cibernética y considera que sus propias capacidades militares en el ciberespacio son muy bajas. Además, no hay que olvidar que Estados Unidos tiene entre treinta y cuarenta ciberaliados, mientras que China está sola y cuenta con pocas aplicaciones militares propias en el ciberespacio. ¿Qué haríamos nosotros si fuéramos China? Pues mucho ciberespionaje. Lo que intenta hacer el East-West Institute es reunir a estos dos países para que, juntos, aclaren los malentendidos que surgen entre ellos, pues las malas prácticas, que existen a ambos lados, pueden modularse. No es posible que Estados Unidos consiga todo lo que quiere de los chinos en el ciberespacio; si sigue empeñado en ese camino de hecho no conseguirá nada, como hemos visto al suspenderse las conversaciones entre Estados Unidos y China. ¿Qué intentamos hacer en el instituto? En el equilibrio entre asuntos militares y asuntos económicos y sociales en la relación China- Estados Unidos, los asuntos militares ocupan un lugar bajo en la lista de prioridades, pues la máxima prioridad es sin duda la relación económica entre los dos países. Y lo que vemos ahí es que, desde 1983, Estados Unidos se muestra dispuesto a proveer a China con casi todo lo que necesita este país para la modernización de sus tecnologías de comunicación. Hemos visto una llegada torrencial de multinacionales estadounidenses a China, que es hoy el primer país productor de ordenadores personales del mundo. Pero la tecnología de la información china depende mucho de la cooperación global, depende mucho de las multinacionales estadounidenses; asimismo, las exportaciones de estos productos

también dependen de estas compañías. Así que tenemos una situación en la que el ciberespionaje chino sigue adelante –pues todos estos ataques están ocurriendo, sin lugar a dudas–, pero, al mismo tiempo y desde 1983, los sectores de tecnología de Estados Unidos y China son totalmente interdependientes. Pero la dependencia de China es mayor y por eso Estados Unidos se puede permitir hacer cosas como acusar judicialmente a China.

Así pues, lo que intentamos desde el East-West Institute es tratar de imponer un cierto entendimiento y de fomentar determinadas acciones donde sea posible. Por eso tenemos estas conversaciones sobre *spam* y sobre *hacking*, además de conversaciones al alto nivel militar para ver que significa realmente el ciberespionaje. Pero, sin duda, es un proceso muy lento.

PEDRO GONZÁLEZ
Columnista de *ZoomNews*

Quería insistir en el tema que ha apuntado sobre el impacto que han tenido las revelaciones de Edward Snowden. El viernes pasado, la Cámara de Representantes de Estados Unidos aprobó, además del presupuesto militar para 2015, una enmienda para poner límite a la capacidad de recolectar datos y almacenarlos de la NSA. ¿Cree que este impacto puede llegar a más y que el Senado aprobará esta enmienda y el presidente la firmará? ¿Qué juicio político le merecen las revelaciones de Snowden, que han puesto patas arriba la lucha en el ciberespacio y han provocado una reacción por parte de los legisladores, que ven amenazada la libertad del ciudadano?

GREG AUSTIN
Miembro Investigador del East-West Institute

Gracias por su pregunta. No estoy familiarizado con el texto exacto de la resolución aprobada por el Congreso, pero he observado

que la actitud del Congreso y del presidente frente a la recolección de datos de la NSA ha cambiado dramáticamente desde que en junio del año pasado se hicieron públicas las revelaciones de Snowden. En enero de este año, el presidente Obama ha dicho que la historia ha demostrado que los gobiernos no son fiables a la hora de proteger las libertades civiles de los ciudadanos sin que haya los correspondientes controles, por lo que parece que siente que hay que poner punto y final a lo que estaba pasando. Su administración ha dejado claro que lo que estaba pasando era algo incompatible en gran medida con lo que es necesario y valioso y debe ser preservado. Así que creo que existe un fuerte apoyo en Estados Unidos a la hora de limitar el poder de la NSA. Y, como he dicho, también las multinacionales han cambiado su postura de cooperación voluntaria con las agencias de inteligencia; a partir de ahora harán lo que hacen en China, en España o en otros países, es decir, cumplirán estrictamente con la ley pero no ofrecerán voluntariamente ayuda que vaya más allá.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Quería pedirle que nos pusiera en más antecedentes sobre los riesgos que tiene España por ser un aliado de Estados Unidos.

GREG AUSTIN
Miembro Investigador del East-West Institute

Mientras conducía hacia Toledo venía pensando en lo lejos que está España de Rusia, de China y de Estados Unidos. ¿Está realmente España en la primera línea del frente de la ciberguerra? Pero piensen por ejemplo en el papel actual de los bancos españoles en la economía global. Además, España es miembro del G20. Desde luego no es un actor económico insignificante y su volumen de transacciones es importante para la seguridad del ci-

berespacio, pues existen todas estas interdependencias que he mencionado. Así que pienso que España es un jugador más, y lo pienso por varios motivos. No sólo porque sea una pieza de la infraestructura que debe ser protegida, o porque los bancos españoles participen en la economía mundial, sino que además hay una serie de actividades que pueden ocurrir en la jurisdicción española que son importantes para otros actores en la economía global. Pueden ser criminales actuando desde territorio español o pueden ser otro tipo de amenazas. El otro lado de la moneda es que, aunque no todos los países colaboren en el ciberespacio, todos ellos se verían afectados por una crisis en el ciberespacio. La habilidad, por ejemplo, de Estados Unidos a la hora de extraditar ciberdelincuentes de China nunca ha sido buena. Ha estado mejorando y ha habido algunos casos en los últimos años en que ha podido lograrlo, pero, en el ambiente actual, ¿es posible que Estados Unidos obtenga de Rusia o de China información por ejemplo sobre un ataque criminal contra un banco estadounidense? ¿Dónde queda España en todo esto? A medida que este país profundiza en sus alianzas con Estados Unidos en asuntos relacionados con el ciberespacio, ¿cómo afecta eso a la posibilidad de entablar un diálogo importante en asuntos de ciberespacio? Todos formamos parte de un mundo global.

JAVIER FERNÁNDEZ ARRIBAS
Moderador

Entiendo que eso incluye el acuerdo sobre el escudo antimisiles.

GREG AUSTIN
Miembro Investigador del East-West Institute

No sé mucho sobre este tema, pero sé que es importante. No obstante, la posibilidad de un enfrentamiento entre China y Estados Unidos es muy pequeña. Lo mismo ocurre en el caso de

Rusia. Pero esto no quiere decir que los servicios de inteligencia de estos países no estén muy activos. El ciberespacio es el dominio principal donde tendrá lugar la guerra de la información. He hablado de los cables submarinos de alta velocidad de transmisión de datos, pero en términos militares lo más importante para Estados Unidos son los satélites. Sin satélites Estados Unidos perdería su superioridad ciberespacial. China lo sabe y se mueve rápidamente para desarrollar sus propias capacidades en el ámbito de los satélites. Dicho esto, desde luego, la participación en algo como el escudo antimisiles expone a un aliado al ciberespionaje. Puede que no sea tan importante, pero sin duda es una de las muchas facetas.

FELIPE SAHAGÚN
Miembro del Consejo Editorial de *El Mundo*

Hace muchos años, en 1992, asistí a un seminario sobre el final de la Unión Soviética con la participación de John Morose, que contaba con la colaboración de Aleksei Varvatov. Estaba pensando si la red con la que ustedes trabajan actualmente en su instituto incluye también a personas con fuentes de información, capacidad y conocimiento, como Varvatov, que fue presidente del comité de defensa de la Duma. ¿Sigue trabajando el East-West Institute con personal local?

Por otro lado, anteayer escuché hablar –no sé si en la BBC o en la CNN– a la ministra de Exteriores alemana. Le preguntaban cómo se estaba resolviendo el conflicto tras el caso Snowden. Ella decía que, entre aliados, estas cosas son cuestiones de familia. No dio detalles, pero reconoció que los americanos se habían excedido y que las cosas no podían seguir igual; las reglas de juego debían cambiar. Quería preguntarle si usted tiene algún dato que indique cómo está ahora la relación entre Alemania y Estados Unidos, si se está encarrilando en una buena dirección. Además, no sé si usted tiene una opinión acerca de

por qué en España la reacción ha sido tan silenciosa, pues prácticamente no ha habido reacción.

Ha dicho que todos nuestros instrumentos y recursos humanos resultan escasos para atender esta amenaza, pero al mismo tiempo vemos que se han ido creando en los últimos años –especialmente en Estados Unidos– departamentos prácticamente independientes y cuerpos nuevos para atender este desafío. Me da la impresión de que se está perfilando un instrumento independiente, con una responsabilidad de supervisión, pero separado del resto de la administración. Yo, sin ser un experto, siento que el problema parte de la infraestructura y de la burocracia. Esto de crear divisiones de las Fuerzas Armadas especializadas en estas amenazas parece menos eficaz que si se planteara como algo que tiene que estar dentro de todo el cuerpo social, industrial y burocrático. Quizá, desde este punto de vista, las cosas no se están haciendo bien y puede que sea algo que paguemos caro en el futuro. Aunque, claro, puedo que me equivoque.

Por último, y volviendo a Snowden. Hace meses escuché al presidente de la Comisión de Justicia criticar lo que representaban para las libertades las revelaciones de Snowden. Como usted sabe, los directores de los medios de comunicación que han trabajado con este tipo de documentos –primero con Wikileaks y luego con Snowden– han estado sometidos a una persecución y a una presión tremendas, como bien han contado los de *The Guardian* y *The New York Times*. ¿Cree que los medios han actuado correctamente? ¿Piensa que nos quedamos cortos? ¿Cómo se puede reconducir esta grave crisis entre la seguridad, el aparato que tiene que administrarla y los medios de comunicación?

GREG AUSTIN
Miembro Investigador del East-West Institute

Le voy a contestar rápida y brevemente. Sí trabajamos con expertos como Varvatov; de hecho, él formó parte de nuestra jun-

ta directiva durante algún tiempo. Sobre el asunto de Alemania, las cosas nunca volverán a ser iguales en lo que respecta a los términos de confianza entre Estados, pero eso no significa que Alemania deje de ser un aliado fiel militarmente. Aunque insisto en que la confianza del público alemán respecto a Estados Unidos nunca volverá a ser igual. Sobre la NSA y la burocracia, Estados Unidos ha creado muchas agencias burocráticas, mientras que otros gobiernos han desechado esa opción. Así que, en efecto, creo que hay un margen para preguntarse si Estados Unidos podría haber elegido un camino distinto al de crear agencias especializadas. Sobre Snowden, creo que son los propios medios quienes deben juzgar si hicieron lo correcto, pero yo pienso que fueron unas relevaciones muy importantes –hasta tal punto que han cambiado la política–, por lo que, personalmente, apoyo que salieran a la luz.

JUAN CUESTA
Director de *Europa en Suma*

Quería comentar dos aspectos. Uno tiene que ver con la defensa que los Estados hacen de sus sistemas de información y del contenido de esa información; hay mucha gente buscando soluciones para esto. Otro aspecto es la defensa que los ciudadanos deberíamos tener frente a la voracidad, o la insaciabilidad, de los Estados en su afán por controlar la información que circula entre los ciudadanos. ¿De qué manera podríamos acotar o controlar la barra libre de los Estados a la hora de controlar la información de los ciudadanos?

GREG AUSTIN
Miembro Investigador del East-West Institute

Buena pregunta. Le daré una respuesta injustamente breve. Yo trabajé durante un tiempo en agencias de inteligencia y tengo

cierta confianza en lo que la NSA y otras agencias hacen con esa información, pero estoy de acuerdo con el presidente Obama en que los gobiernos no son fiables si no se les aplican una serie de controles. En el ciberespacio, la mayor amenaza para usted o para mí es la que suponen los criminales, no de gobiernos; ni el estadounidense ni español ni el alemán. Por tanto, incluso aceptando que estos gobiernos hacen cosas en el ciberespacio que están mal, me preocupa mucho más lo que hacen los delincuentes. Y nuestra inhabilidad global para atajar la ciberdelincuencia es algo grave. Volviendo a su pregunta, creo que el escrutinio de las agencias de información es algo fundamental. Lo que hizo Snowden es importante y también lo es que haya un debate público al respecto, pero en última instancia creo que las agencias de seguridad nos protegen, aunque cometan errores de vez en cuando. Desde luego, hay que cosas que deben acometerse.

ANTONIO REGALADO
Colaborador de *ABC*

¿Qué papel pueden jugar los drones a la hora de prevenir las ciberamenazas? ¿O son en sí mismos los drones otra amenaza?

GREG AUSTIN
Miembro Investigador del East-West Institute

Mirando hacia delante, creo que todos nos debemos plantear el uso que estos drones pueden tener. Estoy seguro de que habrá muchos ejemplos en el futuro de cómo los drones pueden ser usados para violar nuestra intimidad y para cometer actividades ilegales. Pero los drones son sólo un ejemplo de la tecnología robótica; algo que en futuro será muy relevante y que, además, se controla desde el ciberespacio. Sin duda, esta tecnología robótica también estará sujeta a ataques y manipulaciones. Sí, debemos preocuparnos por los drones.

3. LA CIBERDEFENSA EN ESPAÑA

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto
de Ciberdefensa

JAVIER CANDAU
Jefe de Área de Ciberseguridad,
Centro Criptológico Nacional

FRANCISCO LÓPEZ LUQUE
Presidente de Everis Aeroespacial
y Defensa

Moderador
JOSÉ ANTONIO GUARDIOLA
Director de «En Portada», TVE

José Antonio Guardiola, Francisco López Luque, Javier Candau
y el General Carlos Medina

Las nuevas amenazas aparecen más vinculadas a ataques cibernéticos que convencionales. Una estrategia de ciberdefensa para España parece irrenunciable. Para ello, en febrero de 2013 el Ministerio de Defensa creó el nuevo Mando Conjunto de Ciberdefensa. Este mando, dependiente del Jefe del Estado Mayor de la Defensa (JEMAD) y dotado de unos 150 efectivos, surge con el cometido de garantizar el libre acceso al ciberespacio que resulta imprescindible hoy en día para cualquier misión de las Fuerzas Armadas, tanto en nuestro territorio como en las intervenciones exteriores, con el fin de protegerlo de amenazas e intromisiones. Su cometido es básicamente prevenir, defender y recuperarse de posibles ataques a los sistemas de información, así como desarrollar la capacidad de explotación, estrechamente vinculada con labores de inteligencia, para facilitar el acceso a los sistemas adversarios y adquirir una cierta capacidad de ataque para neutralizar total o parcialmente dichos sistemas.

¿Cuáles son las amenazas reales en materia de ciberdefensa? ¿Qué objetivos concretos pretenden alcanzar esos ataques? ¿Estamos preparados para repelerlos? ¿Podemos proteger nuestras infraestructuras críticas de esos ataques? ¿Ha supuesto la aparición de este nuevo riesgo un cambio en la formación y la articulación de los miembros de las Fuerzas Armadas españolas?

JOSÉ ANTONIO GUARDIOLA
Moderador

Hace unos años decidí hacer un reportaje en televisión sobre algo que me parecía innovador: la ciberguerra, que más adelante se convirtió en ciberamenaza, adquiriendo un concepto más amplio. Recurrí entonces a algunos expertos que están aquí presentes. Y resulta que lo yo pensaba que iba a pasar ya estaba pasando, o ya había pasado. Vi dos ejemplos claros. Uno de ellos fue el ciberataque a Estonia originado en Rusia. Digo en Rusia porque una cosa es saber desde dónde se lanza un ataque y otra saber si fue lanzado por rusos; un tema que entra en la atribución de *casus belli* en ciberdefensa. Gracias a aquel reportaje también vi cómo se desarrollaba entonces un virus tan «fantástico» como el Stuxnet, que logró bloquear el programa nuclear iraní. Y también comprendí que la ciberdefensa se estaba desarrollando también en España y que era un asunto que había que tratar.

Sobre esto vamos a hablar con los tres invitados a esta mesa, pues cada uno de ellos cumple una función clave en este proceso. El General Carlos Medina, del Mando de Ciberdefensa, representa a la parte militar. También nos acompaña Javier Candau, del Centro Criptológico Nacional, el organismo que vela por que el sistema informático de la administración sea lo menos vulnerable posible. Y, finalmente, Francisco López Luque, que representa a Everis, empresa que se dedica a asesorar sobre el buen uso de los sistemas informáticos en las empresas.

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

Lo primero que pensé al ver el título de este panel, «La ciberdefensa en España», es si era necesario argumentar que esa ciberdefensa es necesaria en nuestro país, pero creo que esto me lo puedo saltar. Quiero centrarme en varias ideas. En primer lugar,

quiero tratar la Estrategia Nacional de Seguridad. Luego, quiero hablar de la Estrategia de Ciberseguridad Nacional, deteniéndome en el Consejo de Ciberseguridad. Y, por último, hablaré del Mando Conjunto de Ciberdefensa.

La Estrategia Nacional de Seguridad se aprobó el 31 de mayo de 2013 y fue una de las primeras acciones del Consejo de Seguridad Nacional. En ese documento –disponible en la web de Presidencia de Gobierno– se identifican doce amenazas y riesgos. Y el tercero de esos riesgos son las ciberamenazas. Esto llama la atención, porque en esa lista aparecen otras amenazas en las que indudablemente interviene de forma fundamental la ciberseguridad, pero se le ha querido dar el protagonismo que merece presentándola también en solitario. La Estrategia Nacional de Seguridad determina que la manera de defenderse de esas ciberamenazas –que afectan al sector público, al sector privado y, en general, a todos los ciudadanos– es ni más ni menos que la ciberseguridad. Incluso plantea varias líneas de acción estratégica para obtener esa protección. Quedaba claro pues que para tratar esas amenazas era necesario desarrollar una estrategia propia de ciberdefensa. Ése era un proceso que ya se había iniciado antes, pero que llegó a buen fin en diciembre de 2013, con su aprobación por parte del Consejo de Seguridad Nacional.

La Estrategia establece un objetivo global y seis objetivos específicos. Para situarnos, voy a leerles. El objetivo global consiste en tratar de «asegurar que España tenga un uso seguro de sus sistema de comunicación y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques». Como ya he dicho, ese objetivo global tiene seis objetivos específicos, y luego la Estrategia identifica ocho líneas de acción para alcanzarlos. Esas líneas engloban desde la seguridad de los sistemas de comunicación y telecomunicaciones que soportan las administraciones púbicas hasta el fomento de los conocimientos y competencias, el I+D+i, o aumentar la cultura de ciberseguridad.

Así planteada, la estrategia podría convertirse en una relación de buenos deseos si no abordara el punto de vista práctico o de eficacia. Pero se plantea un mecanismo, una organización, para llevar esto a la práctica: ese organismo es el Consejo de Ciberseguridad Nacional, que celebró su primera reunión el 25 de febrero de 2014; hace apenas unos meses. Se trata de uno de esos comités especializados que está previsto que apoyen al Consejo de Seguridad Nacional. Su misión no es ni más ni menos que velar por la correcta implantación de la Estrategia de Ciberseguridad Nacional. Tiene doce vocales permanentes: diez que representan a ministerios y dos que representan al CSID y al Departamento de Seguridad Nacional. Los ministerios incluyen Exteriores, Interior, Industria y Defensa, pero también Hacienda, Educación o Justicia. Y actualmente lo dirige el director del Centro Nacional de Inteligencia (CNI). Así es la organización que vela por la implantación de la Estrategia de Ciberseguridad. Para cumplir su cometido coordina todo el impulso de la administración y, además de los vocales permanentes, puede convocar a otros actores, de la administración o del sector privado, que puedan aportar información de interés para la implantación de la estrategia.

Y en este maremágnum, ¿cómo nos repartimos las responsabilidades? ¿Cómo defendemos España desde el Mando Conjunto? Ésta es una tarea de muchos jugadores. De forma simplista –no rigurosa pero sí clarificadora–, les diré que el Ministerio del Interior es responsable de las infraestructuras críticas y, por supuesto, de los ciberdelitos y del ciberterrorismo. El Centro Criptológico Nacional –dependiente del Centro Nacional de Inteligencia– se ocupa de las Administraciones Públicas. El Ministerio de Industria tiene la enorme tarea de apoyar a las empresas tanto públicas como privadas. Y en el Ministerio de Defensa tenemos dos tareas. La primera tarea es defender nuestros sistemas, los propios del Ministerio de Defensa; los sistemas de información y la red de telecomunicaciones. Pero también tenemos otra tarea más ambigua, y muy ambiciosa, que consiste en hacernos cargo

de cualquier sistema importante para la defensa nacional que se nos pueda asignar.

¿Hay realmente una necesidad operativa para el Mando Conjunto de Ciberdefensa, teniendo en cuenta cuál es nuestra responsabilidad? Como ustedes sabrán, en las Fuerzas Armadas somos extraordinariamente ciberdependientes; somos como la sociedad que nos rodea, pero más. Las tres fases de nuestra actuación son el planeamiento de operaciones, la dirección y la ejecución, y las tres son claramente ciberdependientes. Nos apoyamos permanentemente en sistemas de información y de telecomunicaciones; no necesariamente Internet, aunque en ocasiones sí.

Cómo habrán oído ustedes, el ciberespacio constituye ese quinto dominio: tierra, mar, aire, espacio y ciberespacio. No hay ninguna duda de que cualquier conflicto moderno conlleva acciones en el ciberespacio. Y, al igual que ocurre en los otros dominios, también en el ciberespacio se pueden planear, dirigir y ejecutar operaciones militares. De ahí que, una vez establecida esa necesidad operativa, el Mando Conjunto se creara en febrero de 2013. Ahora mismo tenemos año y medio de edad. Como he dicho, se crea para responder a unas amenazas ya existentes y a unos riesgos que van aumentando progresivamente.

Dentro de la estructura de la fuerza conjunta, el Mando Conjunto de Ciberdefensa ya es el quinto mando que compone la doctrina conjunta planteada por el Jefe del Estado Mayor de la Defensa: tierra, mar, aire, operaciones especiales y «cíber». Yo, como jefe del Mando Conjunto, dependo directamente del JEMAD, lo cual tiene muchas ventajas. Desde nuestro punto de vista la solución, como fórmula para defender esos intereses, es algo eficaz y eficiente. Una pregunta que me hacen con frecuencia es si vamos hacia un cuarto ejército dedicado a la ciberactividad. Mi respuesta es que no, por distintos motivos.

Creemos que el Mando Conjunto es la opción más eficiente para hacer frente a esa necesidad. Entre nuestros cometidos está la protección de redes y sistemas conjuntos de las Fuerzas Arma-

das. Coordinamos las acciones defensivas de los ejércitos y las Fuerzas Armadas, que son a su vez responsables de sus sistemas específicos. Somos responsables de las acciones ofensivas de responder –como dice la orden de mando– a ciberataques de forma oportuna, legítima y proporcionada. Tenemos la tarea de liderar la formación y concienciación sobre la ciberdefensa en el ministerio; de asumir la representación nacional e internacional del ministerio en temas de ciberdefensa; y de prestar apoyo, en caso necesario, cuando estén comprometidos los intereses nacionales. Estamos ubicados en la población madrileña de Pozuelo de Alarcón, en la antigua sede del cuartel general de OTAN, en la base de Retamares, y alcanzamos nuestra capacidad operativa inicial en septiembre de 2013.

¿Cuáles son nuestros objetivos? Voy a presentarles dos bloques. El primer bloque son los objetivos a corto y medio plazo. Nuestra primera intención es entrar en operación de forma más intensa. En colaboración con el Mando de Operaciones y el Centro de Inteligencia de las Fuerzas Armada –conocido coloquialmente como CIFAS–, pretendemos poner en práctica el plan y programa de concienciación, formación y adiestramiento de todo el Ministerio de Defensa –es decir 120.000 personas–, para llevar a cabo la dirección y coordinación de las capacidades defensivas de los tres ejércitos, o, mejor dicho, de los dos ejércitos y de la Armada. También debemos adecuar los recursos de personal a las necesidades operativas, porque estamos iniciando una actividad en un dominio que es nuevo y tenemos que hacer un ajuste permanente en las capacidades que se nos piden y que tenemos que aportar, así como en recursos de personal. Por supuesto, debemos alcanzar las capacidades operativas finales –final es una palabra demasiado radical en el espacio cibernético; digamos capacidad operativa completa–, tanto en defensa como en explotación y ataque. Un objetivo de gran importancia que hay que plantearse todos los años es obtener la aprobación del presupuesto para el año siguiente. Por otra parte, tenemos que cola-

borar en la consecución de los objetivos que se establecen en la Estrategia de Ciberseguridad Nacional, que, además de lo que ya he señalado, establece que hay que coordinarse con organismos de la administración pública. Debemos impulsar todo lo que esté en nuestra mano el desarrollo industrial y reforzar el sistema de I+D+i colaborando con empresas y con universidades; un elemento tremendamente importante. También aumentar la cultura de ciberseguridad, y promover y sostener el compromiso con organizaciones internacionales y con las naciones aliadas, es decir, con la OTAN y la Unión Europea y las Fuerzas Armadas de las naciones aliadas.

Los objetivos a largo plazo –que yo considero permanentes porque siempre van a estar ahí– incluyen temas como el desarrollo de las capacidades de defensa, explotación y respuesta; algo que siempre estará en evolución permanente. Por el mismo motivo, también hay que evolucionar el plan de formación y adiestramiento. Entendemos que siempre habrá una Estrategia de Ciberseguridad en vigor. Hoy tenemos ésta y dentro de unos años entendemos que será otra versión, pero tendremos que colaborar en la consecución de los objetivos establecidos.

JOSÉ ANTONIO GUARDIOLA
Moderador

Ha dicho que, por el momento, no es partidario de crear un cuarto ejército, un ciberejército.

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

Hasta donde yo alcanzo a ver creo que no es necesario. Igual dentro de 25 años, por ponerles una escala tal vez algo exagerada, se llegue a la conclusión de que deben plantearse las cosas de otra manera.

JOSÉ ANTONIO GUARDIOLA
Moderador

Gracias, General. Ahora hablará Javier Candau, jefe del Área de Seguridad del Centro Criptológico Nacional.

JAVIER CANDAU
Jefe de Área de Ciberseguridad, Centro Criptológico Nacional

Voy a hablarles sobre la situación de la ciberseguridad en España y sobre el papel del Centro Criptológico Nacional. En la parte dedicada a esta sesión en el programa de estas jornadas se plantean cinco preguntas. «¿Cuáles son las amenazas reales en materia de ciberdefensa? ¿Qué objetivos concretos pretenden alcanzar esos ataques? ¿Estamos preparados para repelerlos? ¿Podemos proteger además nuestras infraestructuras críticas de esos ataques? ¿Ha supuesto la aparición de este nuevo riesgo un cambio en la articulación y la formación de los miembros de las Fuerzas Armadas españolas?». Trataré de responder a todo menos a la última cuestión, que le corresponde al General.

A modo de introducción general, cabe decir que el principio del que partimos para acercarnos a esta cuestión es que atacar o infectar una red es algo relativamente sencillo. Tenemos tres niveles en la red. El primer nivel es al que acceden los usuarios; éste es el nivel más bajo. Luego, está el siguiente nivel, donde se almacenan los datos, que está formado por bases de datos y servidores de correo electrónico, además de otra serie de servidores miembros. Y, por último, tenemos lo que, dentro del dominio Windows, llamamos los controladores de dominio, que es donde están los administradores administrando ese controlador de dominio. En este tercer nivel es realmente donde se da derecho a los usuarios para obtener información o no. Un atacante siempre manda un correo electrónico o un enlace que el usuario tiene la libertad de descartar o no. Por desgracia, nuestra experien-

cia indica que muchos usuarios realmente abren ese correo electrónico. Con que haya tan sólo un usuario que lo abra, o que pinche un enlace, el ataque avanza, el usuario pasa a estar infectado y el atacante recolecta credenciales, privilegios de acceso y contraseñas. Así va progresando por la red hasta que, en un determinado momento, llega a un equipo que tiene unas credenciales especiales, que son las de administración. Eso le permite llegar al controlador de dominio y convertirse entonces en administrador de la red y, por lo tanto, colonizar la red. A este tipo de ataques se les llama «amenaza persistente avanzada», porque no están asociadas a un tipo específico de *malware*.

Me gustaría hablar brevemente de algunos conceptos en torno a la ciberseguridad. Desde la década de 1980 hasta el año 2000 hemos hablado de *compusec* (*computer security*, o seguridad de ordenadores), de *netsec* (*net security*, o seguridad en red) y de *transec* (*transmission security*, o seguridad de transmisión), toda una serie de conceptos que quedaron englobados en el concepto de *infosec*, que defiende que tenemos que proteger la información en sus tres dimensiones: confidencialidad, integridad y disponibilidad.

Todos estos principios de ciberdefensa, que se han mantenido hasta el año 2000, sostenían que teníamos que poner muchas medidas de seguridad en la valla, en la defensa de las redes. Quiero aclarar que estas ideas no han pasado de moda. Así que, hoy en día, cuando tenemos un organismo infectado volvemos a repetir que si se hubieran aplicado las precauciones y medidas de seguridad adecuadas no sería un objetivo blando, sino duro y difícil de atacar.

A partir del 2000 pasamos al concepto de *information assurance*, que propone que además de estas dimensiones debemos proteger la autenticidad y el no repudio. Éste no repudio se ha traducido en nuestro esquema de seguridad nacional en el concepto de trazabilidad.

Tras del atentado de las torres gemelas y la invasión de Irak en 2003, cambian las amenazas que empezaron a barajarse y entra un nuevo concepto, que es el del ataque a las infraestructuras críticas. En este frente lo que nos preocupa es la dimensión y disponibilidad, es decir, que el servicio se caiga. Hay que destacar un aspecto importante en lo relativo a las infraestructuras críticas y es que el 80% pertenecen al sector privado. En las administraciones públicas es fácil regular, podemos dar un esquema y obligar a que se cumpla, pero en la relación con las empresas el asunto es un poco más complicado.

A partir de 2003 surge el concepto de ciberterrorismo y, ya a partir de 2006, todos estos conceptos se engloban dentro de lo que llamamos ciberdefensa y ciberseguridad. Entonces se empieza a hablar también del ciberespionaje de los gobiernos. De 2008 en adelante todas las naciones empiezan a publicar estrategias con el fin de darle cuerpo legal a la nueva aproximación a la ciberseguridad. En 2013 y 2014 se habla de ciberresilencia, de defensa activa y de ciberguerra, conceptos todos ellos que son subconjuntos de los anteriores. Quiero destacar esto porque considero que muchas veces, al manejar parcialmente los conceptos, propiciamos que nuestro acercamiento al problema de la ciberseguridad sea también parcial. Eso es algo que me parece importante subrayar.

¿Qué es el Centro Criptológico Nacional (CCN)? En primer lugar, forma parte del Centro Nacional de Inteligencia (CNI). Recibe su cuerpo legal en la ley 11/2002 y desarrolla sus funciones en la ley 421/2004. A partir de 2005, el Gobierno de España le encomienda al CNI, y específicamente al CCN, una postura más proactiva en la defensa de las redes. Actuamos intentando proteger las administraciones públicas, pero también fruto de la misión del CNI, según la ley 11/2002, de actividad de contrainteligencia, intentando proteger la propiedad intelectual e industrial de las empresas que se consideran estratégicas. Para esto, lo que se hace desde el CCN es desplegar sensores que permitan identificar pa-

trones de ataque de determinado *malware* o atacante. Los organismos que están cubiertos son todas las administraciones del Estado. A partir de 2013 se empezó a desplegar también en comunidades autónomas y, ahora mismo, hay ocho adscritas al servicio. El despliegue también ocurre cuando hay un riesgo crítico en empresas estratégicas y ahora también empezaremos a ponerlo en marcha en grandes ayuntamientos y diputaciones.

Así podremos informar sobre incidentes y catalogarlos según la guía 817 de nuestro portal. Hay incidentes críticos muy altos, bajos y medio-altos. Entre los críticos, sólo registramos incidentes que se notifican con recursos propios, es decir, no contabilizamos los incidentes que nos aportan otras administraciones. En 2013 se reportaron unos 7.300 incidentes y, a junio de 2014, ya llevamos contabilizados unos cinco mil este año. Así que seguramente llegaremos a la barrera de los 10.000, gestionando miles de incidentes cada mes.

Si nos fijamos en la cripticidad, en 2013 se registraron mil y pico incidentes muy altos y treinta y tantos críticos. Ese número se ha duplicado en 2014. Así que, efectivamente, nos atacan. Pero que tampoco hay que dramatizar. Lo que hay que hacer es defenderse y vigilar.

¿Quién nos ataca? En nuestro informe anual de amenazas y tendencias –que en unos meses será de dominio público– establecemos quién nos puede atacar. Nuestra aproximación a este asunto parte de algo importante que no conviene olvidar: nos atacan porque es muy rentable hacerlo y es rentable porque no nos protegemos tan bien como deberíamos. Como ya se ha dicho en la primera sesión de este seminario, la ingeniería es fácil y no resulta descabellado recibir un correo o un enlace por las redes sociales y abrirlo. Reaccionamos ante un hecho ya ocurrido, pero no nos adelantamos a las acciones del atacante.

Tenemos poco personal dedicado a esta seguridad, y además muy fragmentado. Normalmente, en las administraciones públicas los departamentos informáticos son muy verticales, según

las funciones de los ministerios y de los distintos organismos. Así que hay muchos equipos de seguridad muy pequeños, en lugar de existir un servicio de seguridad horizontal más potente y eficiente. En el caso del sector privado, las empresas son muy reacias a comunicar incidentes, porque esto puede reflejarse en su cuenta de resultados o afectar su valor en bolsa. Además, saber quién ha atacado es realmente muy difícil.

Todo esto crea el escenario ideal para un atacante, porque infectar inicialmente a una empresa o un organismo es algo relativamente sencillo. La empresa Mandiant realizó un estudio que afirma que, de media, las infecciones ocurren en apenas unas horas, mientras que el defensor puede tardar meses o años en detectarlas. Por otro lado, nos enfrentamos a profesionales del robo de la propiedad intelectual: no se trata de identificar un *malware* y destruirlo, sino que nos enfrentamos a unos atacantes que tienen como misión robarnos información. Por eso, limpiar una red nos llevará meses o, si no se hace bien, incluso años.

Un informe de 2013 de otra empresa analiza cuántas familias de *malware* se han encontrado y cómo esas familias están asociadas a los distintos sectores (sector energético, bancario o de la administración del Estado) y han atacado a distintos países. Según estos datos, Estados Unidos ha recibido ataques en más de veinte sectores y en España se han detectado ataques en quince sectores. Todos los países de Occidente e Iberoamérica, algunos países asiáticos y, por supuesto, los países relacionados con la producción petrolífera han sido atacados. Si nos fijamos en las familias de *malware*, ¿qué sectores han sido atacados? Pues las administraciones públicas han recibido ataques de más de ochenta familias de *malware*.

Así pues, somos objetivo de ataques y muchas veces no estamos debidamente protegidos Hay auténticos profesionales del ataque. Los principales atacantes son China, Rusia, Irán, etc., y normalmente, estas capacidades para el ciberataque competen a las Fuerzas Armadas a los servicios de inteligencia.

Volviendo al informe, el segundo motivo de preocupación es el ciberdelito, el cibercrimen, así como el robo de propiedad intelectual. El tercer punto en la lista de preocupaciones es el hackeractivismo, es decir, la existencia de grupos que son un poco, digamos, «antisociales»; y digo esto porque cualquier expresión en las redes es respetable salvo aquello que va contra los derechos de los ciudadanos, como la publicación de información privada de particulares, o la difusión de información clasificada o sensible. Finalmente, el cuarto motivo de preocupación es el uso de Internet por terroristas, o ciberterrorismo. Quiero apuntar que, dentro de los grupos terroristas, la capacidad de ciberterrorismo es escasa, aunque sí hacen un uso extensivo de Internet para sus comunicaciones y propaganda, entre otras cosas. El ataque ciberterrorista a infraestructuras críticas es escaso, pero este tipo de ofensiva surge más claramente en caso de conflicto o de guerra entre Estados. Es el Estado quien tiene mayor capacidad para realizar ataques contra infraestructuras críticas.

Todos estos agentes y ataques se apoyan en los usuarios internos. Hay usuarios especialmente privilegiados, como los administradores de la red. En las empresas y administraciones públicas, éstos ocupan dentro de la jerarquía real unos puestos muy bajos, tanto en salario como en categoría. Así que estos usuarios, que reciben un salario de digamos 20.000 o 40.000 euros brutos, son fácilmente manipulables y pueden abrir las puertas a cualquier atacante.

En 2013, los dos primeros motivos de preocupación apuntados se han incrementado de manera notable y los otros dos se han mantenido como estables o incluso se han reducido. Ese año la campaña de ciberespionaje conocida como Octubre Rojo, que atentaba contra administraciones públicas y empresas, afectó de lleno a España. Tanto es así que varios ministerios fueron infectados por este *malware*. En un informe sobre APT1, Mandiant cita como primer ejemplo un ataque de un grupo específico con origen en China que afectó a 154 empresas, en su mayoría esta-

dounidenses. Hay otros casos de amenazas persistentes avanzados el año pasado, pero no afectaron de manera directa a España. Si en 2013 tuvimos cuatro ejemplos claros de ataques persistentes en el dominio público avanzados, en 2014 ya llevamos ocho en el mes de junio. Uno de ellos, Energetic Bear, tiene posiblemente su origen Rusia y ha afectado a muchas empresas y administraciones públicas.

Nos roban mucho. ¿Se puede hacer una estimación real de cuánto? En España no lo hemos plasmado en dinero, pero en el Reino Unido se ha calculado cuánto costaba el ciberespionaje, los ataques y el no tener ciberseguridad. La cifra a la que llegaron fue de 27.000 millones de libras. El robo de propiedad intelectual y el ciberespionaje ascendía a entre 8.000 y 9.000 millones de libras. Es especialmente alto el robo en empresas aeroespaciales, de software o farmacéuticas, porque los atacantes tratan de reducir su brecha tecnológica en estas áreas respecto a los países industrializados.

Hay sectores que reciben un impacto considerable fruto del ciberespionaje que resulta en pérdida de contratos y demás. Pero si hablamos de infraestructuras críticas en España, en este grupo quedan englobados los sectores energético, de industria nuclear, la administración, etc. Y, si cotejamos esta lista con los sectores que reciben más ataques, sólo hay cinco que coinciden: el energético, la administración, el financiero, la industria química y las comunicaciones. Pero hay un montón de sectores –como el aeroespacial, el de defensa o el farmacéutico, la minería o el naviero– que no están considerados como infraestructuras críticas y, sin embargo, reciben muchos ataques contra su propiedad intelectual e industrial. Por lo tanto, necesitamos una aproximación bastante global para solucionar este problema. Algo que creo que nos va a proporcionar la Estrategia Nacional de Ciberseguridad.

Sobre el robo de información, ¿qué hace el CCN o qué posible solución ve? Nuestra postura en esto se establece a partir de tres ejes. En primer lugar, la defensa de redes: intentamos detec-

tar los ataques y asesoramos a las administraciones para que implementen las mejores medidas de seguridad. El Esquema Nacional de Seguridad establece hasta 75 medidas que, si fueran implementadas, nos permitirían dejar de ser objetivos blandos y pasar a ser objetivos duros. El segundo eje es el intercambio de información. Nosotros tenemos varios programas –el de las administraciones públicas lo tenemos bastante rodado y ahora estamos con empresas– para poder intercambiar información. No obstante, normalmente la gente es bastante reacia a intercambiar información –recibe mucho e intercambia poco– y, cuando hablamos de incidentes, a no ser que se trate de algo que no sean capaces de resolver, el intercambio de información es escaso. El tercer punto de nuestra actuación es la capacidad de inteligencia que pretende tratar de conocer al agresor. Para esto usamos el diagrama del diamante y, partiendo de las víctimas, tratamos de llegar a los atacantes. Este planteamiento se asimila a una carrera de fondo. El atacante nos infecta con relativa facilidad, pero una vez que está dentro de nuestra red hace mucho ruido. Yo estoy defendiendo mi fortaleza y él sólo tiene que aprovechar un agujero o fallo en mi seguridad para entrar dentro, pero, una vez que está ahí y empieza a evolucionar dentro de la red, si tenemos capacidades de vigilancia dentro de las redes, lo podremos detectar y expulsar. Si tenemos capacidades de vigilancia, como ocurre ahora en muchas administraciones públicas y empresas, el atacante lo tendrá más difícil. Así que, en conclusión, podría decirse que tenemos que intercambiar mucha información para dificultar la actividad de los atacantes e intentar evitar el robo de propiedad intelectual y de información clasificada o sensible de empresas.

JOSÉ ANTONIO GUARDIOLA
Moderador

Me ha surgido una pregunta. Ha dicho que en lo que va de año hemos sufrido treinta incidencias críticas. ¿Son críticas por la

globalidad del ataque o porque han logrado su objetivo? ¿Cómo se clasifica esto?

JAVIER CANDAU
Jefe de Área de Ciberseguridad, Centro Criptológico Nacional

Un incidente se clasifica como crítico cuando hay evidencia de que ha habido filtración de información. Es decir, no implica que haya infectado a varios organismos o empresas; es posible que haya afectado a siete o a uno sólo.

JOSÉ ANTONIO GUARDIOLA
Moderador

Gracias. Ahora tiene la palabra Francisco Luque.

FRANCISCO LÓPEZ LUQUE
Presidente de Everis Aeroespacial y Defensa

Después de oír a Javier Candau es complicado no entrar a hablar del mundo de la tecnología y dar un poco más de información sobre ese tema, pero yo voy a hablar sobre cuál creo que debería ser la implicación de las empresas privadas en la ciberdefensa. En el mundo actual, este mercado presenta una confluencia del ámbito militar con el civil en tecnologías de uso doble. Y, si vamos a la ciberseguridad, esto es aún más acusado. Es complicado distinguir entre ciberdefensa y ciberseguridad. De hecho, cuando hablo de ciberdefensa como concepto a nivel país, habría que poner la coletilla de nacional. También quiero abordar otro concepto que está empezando a aparecer en los informes especializados. Se trata de la llamada *Smart Defense* (defensa inteligente). Estamos en una era en que todo es *smart*, desde nuestras redes eléctricas (*smart grid*) hasta nuestras ciudades, porque rara es la que no se considera una *smart city*. Creo que básicamente

se trata de un cambio de paradigma. Tenemos que poner en un mismo entorno colaborativo a múltiples actores, tanto públicos como privados, para que, ante el uso intensivo de las tecnologías de la información, se pueda dar un servicio a la sociedad; un servicio que hasta este momento era algo inimaginable.

Antes se pensaba que la administración pública necesitaba mantener unos niveles de servicio sin hacer unas inversiones a priori que no pudiera asumir. Por otro lado, a las empresas privadas les interesa tener una vinculación fuerte y una relación a largo plazo con la administración pública a través de un negocio sostenible. Pero, al hablar de seguridad, creo que el término colaboración es algo que se queda corto. No estamos hablando de una concesión, sino más bien de una implicación pública-privada, donde la motivación de las empresas no es tanto el negocio como el beneficio común; su compromiso no sé si es con la soberanía nacional o con la ciberdefensa nacional.

El sector privado es muy amplio, así que lo he segmentado en tres grupos. En el primer grupo están las grandes empresas y, en especial, los operadores de infraestructuras críticas. Obviamente, en las grandes empresas la preocupación por la seguridad informática no es algo nuevo; llevan años invirtiendo en ello. En el pasado, tal y como ha señalado Javier Candau, estas grandes empresas se concentraban en la protección de perímetro. Es decir, trataban de proteger sus infraestructuras tecnológicas, sus redes y sus servidores intentando que no entrara nadie, que no llegara nadie hasta allí. Esta postura sigue vigente, pero ya no es el principal vector en la ciberseguridad de las grandes empresas. El siguiente paso son los datos, porque la amenaza en aquel momento no era tanto que los datos fueran robados como que fueran modificados, una acción que puede tener un efecto fuerte en los clientes; y esto es un riesgo que una empresa privada grande no se puede permitir. Ahora hemos subido un escalón más, porque ya no se trata de las redes ni de los datos ni de la relación con los clientes, sino que estamos hablando de un problema sisté-

mico de continuidad del negocio, de la capacidad inherente a una empresa de poder competir y proveer servicios. Así que la amenaza es aún mayor. Es por esto que estas grandes empresas han hecho fuertes inversiones para dotarse de recursos de protección. Sus sistemas de protección han ido evolucionando, con más o menos éxito, y se ha llegado a un punto en el que el nivel de interoperatividad es tal que no basta con que estas empresas estén protegidas; sus clientes, sus subcontratistas, sus proveedores o sus socios tienen que tener un nivel equivalente. Así que una gran empresa tiene motivos más que suficientes para participar en un incremento general y global de la ciberseguridad, simplemente porque esto tiene una repercusión directa en su propia seguridad.

Como apuntaba antes Javier, existe también el problema de la reputación. Es decir, es muy, muy complicado que una gran empresa levante la mano y diga que ha sido atacada y no ha sido capaz de controlar la situación durante un tiempo. Así que es necesario crear mecanismos legales para que se apruebe una ley de protección de datos estratégicos, porque estos datos son necesarios. Hay que crear pues un ambiente propicio y unas garantías para que las empresas sean capaces de compartir sus experiencias ante ciberataques.

En las infraestructuras críticas los sistemas, en su día, estaban aislados. Es natural pensar que si uno está aislado está protegido, pero es un error. Es como si considerásemos que una isla, sólo por serlo, está protegida; aunque no haya un puente, más vale tener fortificaciones y sistemas de defensa, unos procedimientos de vigilancia, y más vale también que seamos capaces de prever qué posibles atacantes hay en el exterior. Cualquier isla es un objetivo y es susceptible de ser invadida, y con los sistemas de las infraestructuras críticas pasa exactamente lo mismo. En las plantas de producción, los sistemas estaban aislados, porque las tecnologías que se manejaban eran diferentes a las que se usaban fuera. Tanto el *hardware* como el *software* y los

sistemas operativos eran específicos, dirigidos a esa infraestructura en particular. Por eso su nivel de vulnerabilidad era bajo. Pero esto se acabó desde que existen unas necesidades inevitables de interconexión entre las empresas. Una planta de producción tiene que hablar con el sistema de toma de decisiones y con le departamento de contabilidad de la compañía, con lo cual ahí tiene que haber una conexión estable. Además, el proceso de abaratamiento de costes ha hecho que muchas tecnologías que en su momento eran específicas se hayan trasladado a tecnologías de consumo. Los sistemas operativos, el *hardware*, que hoy se maneja es mucho más cercano, y por lo tanto mucha más gente tiene capacidad para acceder a ellos. Hoy en día hay muchos más sistemas; está el de producción puro y el de gestión de la infraestructura, pero existen otros muchos sistemas de soporte.

Otro concepto que conviene tener en cuenta es «el Internet de las cosas», pues cada vez va a haber más tráfico; todos hemos oído hablar de los cincuenta mil millones de dispositivos conectados a Internet por su cuenta, interactuando entre ellos por su cuenta. Esto nos lleva desde el torno de control de acceso de una central hasta el último monitor de una oficina de mando y control, y cada uno tiene su *software* específico, susceptible de ser alterado y con capacidad de acceso directo a Internet, por lo que también son accesibles desde el exterior. Las cosas, por tanto, se complican.

El mandato más etéreo que tiene el Mando Conjunto de Ciberdefensa es el de proteger. Aquí hay un paralelismo con las Fuerzas Armadas tradicionales, cuando se habla de la protección o la ayuda, con organismos públicos y privados, siempre que los intereses nacionales estén en peligro. Obviamente, un ciberataque contra una infraestructura crítica pone estos intereses en peligro. Pero ese mandato es complicado de ejecutar si no hay un trabajo previo. Tiene que haber intercambio de información y simulacros, de manera que en caso de un ataque o una crisis a nivel nacional los organismos públicos encargados de actuar pue-

dan hacerlo. Es necesario pues un proceso de colaboración previo al día de la crisis.

Ahora voy a hablar del segundo grupo de empresas: las proveedoras de servicios de seguridad. Everis forma parte de este grupo y la estrategia de ciberseguridad casi nos marca el camino por dónde tenemos que hacer negocio, porque ése es nuestro mercado. Todos los objetivos que ahí se marcan son para nosotros líneas de servicio y de negocio. Este negocio se hará en el entorno estándar entre cliente y proveedor, más allá del socio a largo plazo, pero debe estar regido por el libre mercado. ¿Qué ocurre entonces? Que esto va un poco más allá, porque esas empresas, tanto tecnológicas como proveedoras de servicios de seguridad, tienen recursos que en algún caso pueden ser interesantes, pues son complementarios y deberían poder integrarse en una gestión de crisis global. No obstante, para tenerlos localizados habría que inventariarlos y no sé hasta qué punto tenemos inventariadas las capacidades estratégicas de nuestras empresas tecnológicas.

Sé que se está avanzando no sólo en ciberseguridad, sino también en otros ámbitos, porque al final se trata de ser capaz de poner encima de la mesa nuestra capacidad de industria militar y de seguridad. También hay que localizar de forma individualizada a expertos y personal; algo que nunca sobra en los organismos que tienen que gestionar la seguridad y que en un momento dado es necesario que puedan colaborar en una gestión. Eso no puede estar dentro del ámbito de un contrato y de una contratación pública, con los procesos que eso implica. Es algo que tiene que definirse de otra manera, a partir de un protocolo, y que, como he dicho, no puede dejarse para el día de la crisis. Hay que tener suficiente intercambio de información y conocimiento mutuo previo para que, en caso de necesidad, se pueda ayudar.

Otro aspecto que forma parte de la Estrategia Nacional de Ciberseguridad es el desarrollo de capacidades. Es decir, nuestro país tiene que desarrollar capacidades diferenciales que nos

permitan elevar la posición que tenemos a nivel internacional en ciberseguridad. Creo que tenemos la materia prima: empresas de tecnología e ingenieros capaces de desarrollar esas tecnologías que nos hagan diferentes. Y es cierto que esas compañías están acostumbradas a hacer I+D, pero el I+D en ciberseguridad tiene que estar muy orientado hacia la colaboración de empresas de tecnología con centros de investigación pública que puedan complementar sus capacidades. Las empresas grandes de tecnología pueden ejercer de motores de ese equipo, obviamente vinculado con una definición de especificaciones, con unos requisitos marcados por los organismo públicos encargados de la ciberdefensa, y erradicando un problema que tenemos en otros ámbitos del I+D. Porque el I+D nunca es un fin en sí mismo, es un medio, y debe crear un producto que pueda ser interesante para la seguridad interna o para el mercado internacional. Somos un país donde, cada vez que se crea una norma, inmediatamente surgen empresas para beneficiarse de ella. En el I+D esto ha pasado. Hay muchas empresas de I+D cuya aportación real de soluciones, de productos, es muy baja. Eso es algo que no sólo se arregla con tutela.

Finalmente quiero hablar de un tercer grupo de empresas, la mayoría de las cuales son PYMES muy pequeñas que están situadas al mismo nivel que la ciudadanía en cuestiones de ciberseguridad y que necesitan campañas de concienciación, promovidas por organismos públicos y por grandes empresas, sobre los riesgos inherentes al ciberespacio. Probablemente necesiten ayuda para definir procedimientos y métodos, para protegerse, y también necesiten incentivos para que esos métodos se pongan en marcha y eleven su nivel de protección. El área de defensa y seguridad de Everis trabaja desde hace más de dos años con diversas PYMES de tecnología en seguridad; somos socios pero no las hemos comprado. Y en este tiempo ninguna de ellas ha planteado siquiera que tenga un procedimiento para controlar el acceso a sus redes. Supongo que la mayoría tienen un antivirus, pero poco

más. Y algunas desarrollan trabajos para el Ministerio de Defensa y crean productos que se venden en España y fuera, por lo que deberían ser susceptibles de protegerse. Nos falta pues concienciación, tanto a nivel de la ciudadanía como en las PYMES.

Cuando estaba preparando esta intervención, me di cuenta de que, cuando se llega al final, es difícil resistirse a señalar las cosas que son urgentes. No es el momento de apuntar una larga lista de temas acuciantes, pues cada uno de los actores tiene sus problemas y se está moviendo. Pero tenemos que aceptar el estatus, porque estamos en una sociedad en la que la capacidad de acceso a la información entre personas es exagerada. Y eso tiene unas servidumbres y unos beneficios de lo que todos disfrutamos. Nos tenemos que proteger; igual que cuando se crearon las ciudades surgieron más problemas de seguridad en los centros urbanos que en los pueblos, pero eso no hizo a la gente regresar al campo. La escalada se va a mantener. Y en ese incremento de ciberseguridad la implicación público-privada tiene mucho que decir.

ENRIQUE PERIS
Excorresponsal de TVE en Londres

Clausewitz escribió que la guerra es una continuación de la política por otros medios. ¿Se podría decir que la ciberguerra y el robo de propiedad intelectual, tanto a empresas como a Estados, es también una continuación de la guerra, de los negocios y de la actividad económica general por otros medios? ¿Por eso los ejércitos tienen un papel esencial en esa defensa? Como prolongación a estas preguntas, y considerando que en el espionaje tradicional hay una enorme interacción entre lo que se llama el espionaje y el contraespionaje –entre el MI5 y el MI6, por ejemplo–, supongo que gran parte de la actividad de defensa respecto de los ciberataques consistirá en anticiparse, en proceder a una actividad de ataque más o menos abierta. ¿En qué medida la defensa frente a los ciberataques del enemigo implican también

una actividad en este sentido? ¿En qué medida una nación como España desarrolla actividades de ciberespionaje respecto a otros países, no tanto por el interés de recopilar información como para prevenir o anticipar ataques? ¿Desarrollamos nosotros también una actividad de ciberespionaje fuera de España?

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

Sobre su primera pregunta, la clave es que el ciberespacio es un dominio nuevo. Tenemos una actividad en ese ámbito que inicialmente tiene utilidades para la humanidad, pero donde también se descubre que hay un espacio del que pueden aprovecharse determinados grupos. Cuando el hombre empieza a explorar las aguas que le rodean y aprecia que el mar y los ríos son fuentes de riqueza, porque facilitan el transporte, a renglón seguido aparecen los piratas. Lo que vivimos es esencialmente lo mismo, aunque con el matiz de que Internet nace con unas premisas de uso generalizado, con un nivel de regulación disminuido y poco motivado por la seguridad. Esto ha favorecido estas actividades delictivas, que pretenden sacar ventaja de los usuarios del ciberespacio. No es que sea la continuación de la política por otros medios, sino que hay quienes tratan de aprovecharse de una realidad que hace 25 años no existía y cuya ausencia, hoy, en el primer mundo, resulta inconcebible. No podemos volver a los pueblos y abandonar las ciudades, sino que tenemos que seguir adelante y usar los desarrollos tecnológicos. Pero hay que añadir algo que probablemente hace unos años no era tan crítico como lo es ahora: la seguridad.

En cuanto a la segunda pregunta, eso de que la mejor defensa es un ataque es algo que se cumple en muchos casos. España, igual que nuestros aliados, cuenta con unas Fuerzas Armadas por varios motivos. Ojalá que no haya que usarlas nunca, pero si hubiera que hacerlo ahí están. Lo mismo digo res-

pecto de la ciberdefensa: hay que estar preparados para todo, para lo más probable y también para lo más peligroso. Puede que nunca haya que usarla, pero si hubiera que hacerlo debemos estar preparados.

JAVIER CANDAU
Jefe de Área de Ciberseguridad, Centro Criptológico Nacional

Quisiera comentar sobre los temas de espionaje y los ciberataques y sobre si el defensor tiene derecho a atacar. Si nos quedamos en la trinchera y el atacante entra en nuestras redes, si nos dedicamos sólo a una defensa dentro de las redes, nuestra capacidad de actuación y de aprendizaje de lo que pueden ser los siguientes pasos de un ataque queda muy mermada. Siempre hay que considerar lo que se llama la defensa activa, pero el problema es que ésta tiene implicaciones legales. Por eso tiene que ser llevada a cabo por organismos que cuenten con las autorizaciones pertinentes. No se puede en ningún momento renunciar a esa capacidad de defensa, a intentar meterse en los sistemas del enemigo y aprender muchísimo más de él. Se trata de algo que normalmente va a ser competencia de los servicios de inteligencia y de las Fuerzas Armadas, pero es algo a lo que no se va a renunciar nunca.

ARANTZA MARTÍN
Responsable de Interior y Defensa de Onda Cero Radio

Parece que siempre que hablamos de ciberdefensa y ciberespacio se reitera la necesidad de la colaboración internacional. ¿Qué peso tiene la colaboración con nuestros aliados y qué peso tiene la defensa o la protección frente a nuestros aliados? Es evidente que tenemos que colaborar con los aliados y trabajar conjuntamente, pero ¿cuánta protección nos exige eso?

JAVIER CANDAU
Jefe de Área de Ciberseguridad, Centro Criptológico Nacional

La colaboración con los aliados en el marco de la OTAN es fundamental. En el ciberespacio hay amenazas muy definidas y el intercambio de información interesante sobre muestras de *malware* muy específicas ante una serie de ataques es algo muy saludable y muy eficaz. Por desgracia, eso no quiere decir que se pueda compartir todo. Cada uno decide en última instancia qué quiere compartir y qué no, pero los aliados pueden recibir unos mismos ataques y ese intercambio puede ser muy productivo. Nosotros, por ejemplo, colaboramos en el programa de inversión en seguridad de la OTAN, el NSIP, para el intercambio de información de ataques. Igual que lo hacemos con el resto de países europeos, como pueden ser Alemania, Reino Unido, los países escandinavos, Hungría o Francia. Esto no quiere decir que estés libre de cualquier tipo de ataque de otras naciones, pero permite que, ante amenazas comunes, tengamos una respuesta coordinada.

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

La clave está, como decía Javier Candau, en determinar niveles de importancia, no sólo en lo relativo a este tipo de información de ciberdefensa, sino en el intercambio de cualquier tipo de información. Hay que fraccionar la información en función de su importancia. Algunos niveles son perfectamente intercambiables, porque benefician a ambas partes, y otros no lo son.

JOSÉ MANUEL VERA
One Magazine

Las Fuerzas Armadas están pensadas, por ejemplo, para protegernos de una invasión, pero en el ciberespacio las invasiones se

producen todos los días. Lo que quiero preguntar al General es si en este año y medio ha habido alguna actuación militar por parte del mando frente a una amenaza real. Hablamos de ataques militares en el ciberespacio, que al final es un poco lo básico para el mando, aunque haya otras cosas. ¿Se ha actuado ya? ¿Ha habido algún combate en el ciberespacio durante este año y medio?

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

No, no lo ha habido.

JUAN ANTONIO GÓMEZ BULE
Presidente de S21sec

Quería hacer dos preguntas. La primera es para el General. ¿Se han encontrado grandes ventajas a la hora de establecer un entorno colaborativo entre el Mando de Operaciones, el Mando de Ciberdefensa y el Centro de Inteligencia de las Fuerzas Armadas? La segunda pregunta es para Francisco López Luque. Estoy totalmente de acuerdo con él en lo que es la definición del acuerdo marco, abierto a la parte pública y a la privada, para desarrollar una detección temprana de necesidades. ¿Cree que, a la hora de llevar a cabo un cambio en la política industrial de seguridad y defensa, un planeamiento industrial a largo plazo sería una de las herramientas adecuadas para poder solventar esa deficiencia que tenemos en tecnología?

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

La colaboración en este año y medio está siendo perfecta. Ese trabajo con ellos era el primer objetivo y a corto y medio plazo

es muy beneficioso para nosotros, porque tienen experiencia real en operaciones desde hace muchos años y nos ayudan muchísimo a focalizar nuestros esfuerzos y centrar nuestros recursos. Quiero aprovechar para decir que no sólo dentro del Estado Mayor de la Defensa, sino también dentro del propio ministerio, pues la colaboración es muy buena con los ejércitos y la Armada. Estamos trabajando en varias tareas con calado importante, como la concienciación y formación del personal que va a estar directamente implicado en la ciberdefensa. Velar por su adiestramiento es una de las tareas en las que trabajamos conjuntamente y el resultado está siendo muy bueno.

FRANCISCO LÓPEZ LUQUE
Presidente de Everis Aeroespacial y Defensa

Sobre la evolución en industria, creo que ése es el camino: la integración entre pequeñas empresas tecnológicas y empresas motrices que puedan poner esas capacidades en el mercado; es decir, que puedan llevarlas allí donde no llegan las PYMES, promoviendo una integración fuerte con los organismos públicos. Todo eso en el largo plazo. Yo no creo en otros conceptos que se han manejado en el pasado en la industria española, porque no todo es aplicable. No creo en la idea de que hay un *champion* nacional y que lo mejor es que todo cuelgue de él. Nosotros, si apostásemos por esta idea, tendríamos todas las de perder, porque nuestro «campeón» nacional es tan sólo un pequeño competidor en el mercado global.

Tenemos capacidades estratégicas en muchos ámbitos de defensa. Puedo hablar de algunas que están dentro del grupo de empresas con las que trabajo: comunicaciones de satélites a nivel mundial, drones –en España hay una empresa que ha fabricado más de doscientos–, biometría facial, etc. Hay una pequeña empresa de Barcelona que es capaz de competir con grandes multinacionales japonesas en soluciones de este tipo. Tenemos que

primero intervenir el mercado, en el sentido de detectar estas compañías, de separar el grano de la paja, y ver qué capacidades son realmente estratégicas y diferenciales. Hay que potenciar esas capacidades desde la administración pública y desde las grandes compañías. Esto sólo se puede hacer desde la voluntad de las empresas y desde la voluntad del Ministerio de Defensa o del Interior. Así se confluirá en un ente que no será un gran «campeón», sino múltiples compañías que para España sean referencia en ese ámbito de tecnología, cada una de ellas con un trazado claro a largo plazo. Lo mismo se aplica en ciberseguridad.

CORONEL JACINTHO MAIA NETO
Agregado de Defensa de la embajada de Brasil en España

Quiero felicitar a los ponentes por las ideas que han expuesto. Aprovechando la respuesta que acaba de dar Francisco López Luque, ¿qué pueden hacer las empresas dedicadas al I+D en temas de ciberdefensa para recibir apoyo del Estado? Ha dicho anteriormente que pensaba que debían ser tuteladas. Quería saber cuáles son sus ideas sobre cómo podría articularse esto.

FRANCISCO LÓPEZ LUQUE
Presidente de Everis Aeroespacial y Defensa

Lo principal es ver cuáles son susceptibles de esa tutela y tener en cuenta que ésta no es tanto de índole económica. En el pasado nos hemos equivocado cuando hemos buscado subvencionar y subvencionar, porque se restan capacidades de aprovechar bien esa financiación. Obviamente, lo que más nos aportan los organismos públicos a las empresas es requerimientos, necesidades. Lo primero es explicitar éstas; ya se buscarán luego los medios. A veces éstos volverán a la administración, pero lo harán con un objetivo claro. Las PYMES normalmente son pequeñas y facturan un millón o dos millones de euros, y con eso no puedes in-

vertir o lanzarte a participar en el mercado global. Debemos conseguir que esas pequeñas empresas crezcan y la manera en que pueden hacerlo, o al menos ése es nuestro modelo, es con la tutela de empresas grandes, que las complementamos en cinco cosas: capacidad financiera, gestión, acceso al mercado, internacionalización y producción en serie. Si se habla con cualquier PYME y se pone esto sobre la mesa, la respuesta es «sí, sí, sí, no y no». Es decir, al menos tres de estos asuntos les preocupan. En cambio, para una gran compañía al menos cuatro de estos puntos están resueltos; no porque sean más espabiladas sino porque tienen más recursos. He visto muchos concursos en los que PYMES españolas intentan ganar el mercado brasileño y poner allí una bandera española y o son engañadas o no son capaces de medir el mercado. Porque uno va a Brasil y piensa que el mercado es fácil –por la amabilidad de la gente– y que todo va a ser un éxito. Pero el hecho de que haya empresas españolas con presencia allí desde hace quince años, que las pueden ayudar acogiéndolas dentro de sus infraestructuras, es básico. Creo que es muy fácil hacerlo, aunque haya que renunciar un poco al beneficio a corto plazo, pensando en el largo.

JUAN CUESTA
Director de *Europa en Suma*

Esta mañana, en la primera sesión, Greg Austin recordaba el perfil bajo, el *relax* con el que algunos países se toman la necesidad de protección de sus sistemas de información. «Objetivos blandos», como decía López Luque. Mi pregunta es para el General. ¿Cómo nos catalogan nuestros aliados, y en concreto Estados Unidos? ¿España es un objetivo blando, medio, duro? Puesto que se trata de una seguridad compartida, ¿qué hacen nuestros aliados, qué hace Estados Unidos? ¿Controlan, auditan, chequean o nos asesoran sobre lo que debe hacerse para no poner en peligro la seguridad común?

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

No sé cómo nos considera Estados Unidos. Sólo puedo decirle cómo nos consideramos nosotros. Me preguntaron en unas jornadas sobre ciberdefensa cómo estábamos en el *ranking* mundial y yo utilicé un símil que es muy gráfico y que, aunque resultó un poco polémico y no sé si es apropiado, creo que nos puede ayudar. Si pensamos en términos de fútbol, podríamos decir que no jugamos en la Liga de Campeones, pero creo que hacemos un buen papel en la UEFA. Eso sí, pretendemos jugar en la Champions.

ANTONIO REGALADO
Colaborador de *ABC*

Mi pregunta es para el señor Candau. Sabemos que hay una falta de colaboración grande en educación o sanidad entre el Estado y las comunidades autónomas, pero ¿qué grado de colaboración hay entre el Gobierno y las comunidades en ciberdefensa? ¿Se les facilita información sensible a las comunidades autónomas?

JAVIER CANDAU
Jefe de Área de Ciberseguridad, Centro Criptológico Nacional

Sí, se facilita información sensible y el grado de colaboración es bastante alto. Ante un problema importante para todos, la capacidad de colaboración tiene que ser alta. Tenemos unos grupos de trabajo específicos de ciberseguridad en los que participan comunidades autónomas, diputaciones, ayuntamientos y universidades, donde se intercambia información limitada y confidencial, no del grado más secreto, pero sí a nivel de difusión. Muchas veces a una comunidad autónoma no le hace falta saber quiénes son los atacantes o cuáles son sus estructuras; sólo tiene que saber cómo puede detectar el ataque en sus sistemas. En ese sentido el in-

tercambio de información es fluido, aunque por desgracia hay más información que va de nosotros a ellos que a la inversa. Pero es verdad que, cuando hay indicios de infección sobre algo que les hemos remitido, nos informan. Otra cosa más importante ocurre cuando identifican el *malware*, y esto nos lo pasan.

MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación de Periodistas Europeos

En este asunto de la defensa parece que los agentes naturales son los Estados, pero luego aparecen otros grupos sin esa definición y sin esas responsabilidades que a veces generan peligros mayores. Mi pregunta es sobre las religiones ¿Son generadoras de ciberamenazas? ¿Son objetivo de ciberamenazas?

GENERAL CARLOS MEDINA
Jefe del Mando Conjunto de Ciberdefensa

Nos encontramos en un dominio, el ciberespacio, donde las relaciones son asimétricas. Para enfrentarse a un Estado en este dominio no es necesario ser otro Estado. Un grupo organizado, numéricamente irrelevante en otros términos, puede tener unos resultados extraordinarios, desde el punto de vista de eficacia, en el ciberespacio. Y ese principio puede aplicarse a lo que quiera. Cualquier grupo organizado, sea cual sea su propósito, tiene a su favor estas características propias del ciberespacio.

JOSÉ ANTONIO GUARDIOLA
Moderador

El General comentaba antes que uno de los objetivos era aumentar la cultura de la ciberseguridad y creo que nuestros tres ponentes han contribuido a ello esta mañana. Gracias a todos.

4. ¿ALIADOS ENTRE LOS CIBERATAQUES?

CARLOS MIRANDA
Embajador. Exrepresentante Permanente de España en el Consejo de la OTAN

SULEYMAN ANIL
Miembro del Centro de Ciberdefensa de la OTAN en Mons (Turquía)

DAVID RAMÍREZ MORÁN
Analista Principal del Instituto Español de Estudios Estratégicos

GREG AUSTIN
Miembro Investigador del East-West Institute (Australia)

Moderadora
GEORGINA HIGUERAS
Periodista *freelance*.
Excorresponsal de *El País* en Asia

Georgina Higueras, Carlos Miranda, Suleyman Anil, Greg Austin
y David Ramírez Morán

Los 28 países que componen la OTAN coinciden en considerar los ciberataques como una amenaza cada día más grave y en que la Alianza debe dotarse de la capacidad suficiente para darles respuesta. Sin embargo, a la hora de compartir las tecnologías que permitieran a cada aliado defenderse a sí mismo, surgen algunas diferencias, sobre todo en el terreno presupuestario, ya que mientras Estados Unidos, Reino Unido, Francia o Alemania vienen destinando sumas significativas para protegerse de los riesgos del ciberespacio, otros apenas han invertido aún en esa protección y buscan amparo en el concepto de solidaridad, tan vigente en la OTAN desde su fundación. Por su parte, la Alianza Atlántica mantiene que la ciberdefensa es una cuestión nacional y que cada socio debe ser autosuficiente, aunque la OTAN pueda contribuir compartiendo información y métodos e incluso realizando ejercicios conjuntos.

¿Superará la OTAN ese concepto de la autosuficiencia nacional? ¿Se puede llegar a una mayor de cooperación entre los aliados? ¿Es tan desequilibrada la contribución de unos y otros? ¿Hasta qué punto ese desequilibrio es un problema insalvable? ¿Tendría sentido la creación de un equipo de respuesta rápida para asistir a quien padeciera un ataque concreto?

GEORGINA HIGUERAS
Moderadora

Empezamos una nueva sesión en la que vamos a tratar el asunto de los aliados. Después de las revelaciones de Edward Snowden, hablar de aliados en materia de seguridad en el ciberespacio parece casi una ironía. Aun así, la OTAN tiene claro que los ciberataques son una amenaza que cada día cobra mayor importancia y que, para afrontarla, es imprescindible que exista cooperación entre países. No obstante, la OTAN está compuesta por 28 países y cada uno de ellos tiene una voluntad distinta a la hora de compartir los avances tecnológicos propios. Los gobiernos de la OTAN son conscientes, como lo son los de la Unión Europea, de que hoy en día sus dispositivos tecnológicos necesitan esa alianza y cooperación, pues sin ellos tienen pocas posibilidades de resistir a las ciberamenazas. No obstante, en una alianza donde se están poniendo en cuestión temas de relevancia y donde –tal y como ha mostrado Edward Snowden– se puede pinchar el teléfono de Angela Merkel –supuesta gran aliada y miembro de la OTAN–, parece difícil definir si realmente nuestros países son aliados y si nuestra alianza es fiable o no lo es. La otra gran cuestión es el asunto presupuestario. ¿Qué piensan países como Estados Unidos el Reino Unido, Francia o Alemania, que invierten enormes sumas en ciberseguridad, de que otros países consideren que por el mero hecho de pertenecer a un club que de una forma u otra dirige Estados Unidos ya están cubiertos por el grupo?

Tenemos con nosotros a cuatro expertos que nos van a hablar de si de verdad hay una alianza, de si se puede hablar realmente de cooperación en materia de ciberseguridad. Analizaremos si de verdad es posible compartir y coordinar las acciones derivadas de esta información cibernética, que está estrechamente ligada al espionaje. Estados Unidos, por ejemplo, considera que la ciberseguridad debe depender de cada uno de los países, aunque luego, en el marco de la OTAN, pueda haber una cier-

ta cooperación. En primer lugar intervendrá Carlos Miranda, que ha sido embajador de España ante la OTAN en dos ocasiones y es diplomático desde 1969.

CARLOS MIRANDA
Embajador. Exrepresentante Permanente de España en el Consejo de la OTAN

Voy a empezar recordando una anécdota sobre la confianza en los demás. En los acuerdos firmados en Reikiavik al final de la Guerra Fría, Gorbachov puso pegas a Reagan sobre el tema de la verificación y el presidente estadounidense dijo una frase que se hizo muy famosa: «*Trust but verify*». Es decir, «confía pero verifica». Hay que confiar pero también hay que asegurarse de que los demás le dicen a uno la verdad.

Antes de seguir permítanme expresar mi agradecimiento por haber sido invitado a participar en este importante seminario, que es un faro en temas de seguridad y defensa y que resulta especialmente importante en un país como España, que en general no presta suficiente atención a estos temas. Es posible que la clase política, cuando oye truenos y rayos, se fije más, pero en general falta el aspecto didáctico respecto a la seguridad y la defensa.

En el ámbito del ciberespacio estamos en una etapa inicial. A medida que se conquistan espacios –como en el pasado ocurrió con el aéreo– se amplían las zonas a las que todo el mundo puede acceder: los Estados y también los ciudadanos. Esto implica la necesidad de una reglamentación. Por otro lado, estos nuevos espacios siempre han provocado un interés por proteger los propios recursos: otros tienen ahora la capacidad de atacar tus recursos, del mismo modo que tú también tienes capacidad para acceder a los recursos de otros. Así que creo que, en este ámbito, hay tres aspectos que hay que cubrir. Por un lado la defensa de los propios recursos; por otro, la capacidad de acceso a los demás; y, por último, las reglamentaciones. En este aspecto,

creo que estamos en un área en la que se interrelaciona lo público y lo privado, así como lo nacional y lo internacional.

El ciberespacio se ha vuelto determinante para todos los sectores de un país, de tal forma que la disrupción de estos espacios puede resultar desastrosa, incluso catastrófica. Por otro lado, la interrelación dentro de las redes, que es precisamente su razón de ser, las hace vulnerables. Es decir, tal y como yo lo veo, el problema es que todo el mundo comparte este espacio y que todo el mundo puede hacerte algo, por lo que tienes que poder defenderte. En términos generales creo que hay un primer plano nacional de defensa o de reglamentaciones. También hemos aprendido que nada es invulnerable; lo que tenemos que hacer es tratar de reducir el nivel de vulnerabilidad. Hay pues un principio de fatalidad, porque incidentes siempre va a haber. De ahí que sea importante estar en condiciones de defenderse, de minimizar los efectos de un ataque y de recuperar la situación previa al ataque. Todo esto requiere la concertación, en el ámbito nacional, entre el Estado y las empresas, como se ha explicado anteriormente. De hecho, en muchas ocasiones las empresas son más fuertes que el Estado a este respecto. En la relación entre el sector privado y el Estado, tal y como ha apuntado Georgina, hace falta establecer unas reglas, porque no puede ser que el más fuerte sea capaz de acceder a la información del más débil. Y, como ya he dicho, el fuerte no tiene porque ser el Estado. No nos gusta que nadie se meta en nuestros ordenadores, así que se impone garantizar el respeto al ámbito privado y que las cosas se hagan según marca la ley, con las oportunas órdenes judiciales.

En el aspecto más centrado en la OTAN, hay en la mesa gente que está más al día que yo, que me marché en 2012, cuando los temas cibernéticos apenas llegaban al Consejo. Ahora me consta que sí que son muy relevantes. La OTAN tiene un Centro de Excelencia en Estonia que fue objeto de un ataque importante que se atribuyó a Rusia. Ahora, y tras un importante ejercicio de ciberseguridad, dicho tiempo dispone de su propio centro de

respuesta. Es evidente que, en el marco de la OTAN, hay una necesidad de coordinación para proteger no sólo las propias redes de la Alianza, sino también las de los países aliados. Aquí entramos en el tema de las diferencias. Yo creo que hay que ayudar a defender las redes de los socios, pero me da la impresión de que la OTAN está más en la idea de ser un lugar donde se coordinan las cosas y donde se aporta información, un mercado donde todo el mundo se interrelaciona, pero sin ir más allá. Por tanto resulta pertinente la pregunta de si lo que hace la OTAN es suficiente o si debe dar más pasos.

El marco OTAN es un marco de referencia pero no es el único; también está la Unión Europea. España tiene que protegerse y regular desde el punto de vista nacional pero, en el plano internacional, hay dos marcos de referencia importantes para nosotros, como son la OTAN y la UE, donde también desarrollamos operaciones militares. Cabe preguntarse hasta qué punto se ha avanzado de la misma manera en los dos marcos, si la coordinación en uno de ellos es más avanzada que en el otro. Esto me lleva a señalar las limitaciones que tiene la coordinación dentro de estos marcos, especialmente en la OTAN. Me da la impresión de que no todos los países realizan los mismos esfuerzos. No todos los países dedican el mismo dinero ni personal y, por lo tanto, no todos los países están al mismo nivel. Esto produce en algunos países cierta renuencia a compartir determinadas cosas, porque, cuando uno se ha gastado su dinero y ha hecho un esfuerzo, el que llega pidiendo ayuda se suele encontrar con cierta resistencia. Esto implica la necesidad de que inviertan más los países que invierten menos –entre los que creo que está el nuestro–, hasta llegar a la media de lo que invierten los demás.

Otro elemento son los factores de seguridad que limitan la capacidad de actuación; entramos en ese terreno del «si yo le doy a usted y usted me da a mí, ¿cómo se mete después en lo mío?». Por eso he dicho que hay que verificar lo que a uno le dicen. Ya no es posible ser un anacoreta ni vivir en una isla de-

sierta; estamos obligados a vivir en comunidad y eso comporta unos riesgos que hay que saber enfocar.

Luego está el tema de si en la OTAN se debe ir más lejos del mero intercambio y cooperación, si existe, o si debe existir, una integración en la que los países pongan en común algo a ser liderado y regulado por la propia OTAN desde Bruselas. Desde luego, parece que todo aquello que todos ponemos en común y en lo que se trabaja de forma integrada sale más barato y funciona mejor. Lo vemos en los programas de armamento, en el *Smart Defense*; todo sale mejor. Lo que ocurre es que, si nos salimos del ámbito de las empresas y los mercados de defensa y entramos en otros conceptos, encontramos que algunos países han aportado mucho más que otros. Si yo pongo en común mis cosas con los otros y a mí me ocurre luego algo que no me cubre la OTAN, por la razón que sea, ¿cómo recupero eso? Si es algo que no se pueda extraer, ¿cómo me aseguro yo de que una GS vaya a vigilar bien el territorio que yo necesito vigilar fuera de los pactos? Aquí entramos pues en situaciones complicadas de gestionar. Todo esto me lleva a pensar que hay que buscar equilibrios entre los intereses nacionales y los colectivos, porque interés colectivo es interés nacional también. No obstante, también hay intereses nacionales identificables y hay que ver cómo se protegen.

Una incógnita que se plantea es cómo afecta todo esto al artículo 5 del Tratado de la OTAN y la verdad es que no sabría dar respuesta. Antiguamente, si se quería atacar a un país lo primero que se pedía era que se destruyeran las defensas antiaéreas para obtener el dominio del espacio aéreo. Me da la impresión que hoy en día se empezaría por un ciberataque. ¿Un ciberataque se podría concebir como algo aislado que levantara el artículo 5? No lo sé. Si está combinado con otras actuaciones parece más claro, pero si no lo está...

Hay otra dificultad en el ciberespacio, como es el tiempo que se tarda en identificar a un atacante; tengo la impresión de que es un tiempo largo. Estamos acostumbrados a los combates aéreos

y me pregunto si existen también los combates cibernéticos. Y también me pregunto, en línea con las dudas sobre el artículo 5, sobre la difuminación del Estado. No está claro que quien te ataque sea forzosamente un Estado; pueden ser particulares que trabajan para ese Estado o una agencia, etcétera. Tras la caída del muro, la OTAN vivió la conceptualización de su utilidad y de ahí surgió que la Alianza pudiera actuar fuera de su ámbito original: de ahí los Balcanes, Asia, Libia, las operaciones antipiratería en el Índico, etcétera. Y el ciberespacio está claramente fuera de ese ámbito.

Para terminar diría que los planes de defensa nacional son imprescindibles, que la cooperación es necesaria, que hace falta reglamentación internacional y que los países de la OTAN tienen que alcanzar una cooperación eficiente –no sólo para los recursos de la organización sino también para los aliados y los países socios– en un marco equilibrado. Pero cuando hablo de países socios también hay una escala, pues hay socios y socios. Por ejemplo, la OTAN tiene un Consejo OTAN-Rusia. ¿Vamos a tener los mismos niveles de confianza con Rusia que con otros aliados? Hay pues que tener en cuenta también las asimetrías. Me parece necesario un mayor esfuerzo en inversiones en tecnología por parte de los aliados que invierten menos. Eso creo que facilitaría la cooperación en el seno aliado de la OTAN y de la Unión Europea. Éste es un campo de colaboración entre estas dos organizaciones y ahí hemos tenido problemas por la asimetría de los miembros, pero es evidente que una colaboración entre ambas entidades es necesario y, además, factible.

GEORGINA HIGUERAS
Moderadora

Muy interesante. Me quedo con la necesidad de una gobernanza mundial cibernética después de los ataques que hemos visto realizarse desde China o Rusia, o el que hicieron Estados Unidos e

Israel para ralentizar el programa nuclear iraní. Parece que está clara la necesidad de esa gobernanza mundial. Me preguntaba, embajador, si hay más posibilidades de cooperación en la OTAN que en la Unión Europea.

CARLOS MIRANDA
Embajador. Exrepresentante Permanente de España en el Consejo de la OTAN

No lo sé, porque yo me he dedicado más a la OTAN que a la Unión Europea. Aun así, me da la impresión de que son temas que no deben ser muy distintos y que se podría lograr una colaboración entre los dos. Desde mi perspectiva –me considero federalista europeo–, aspiro a una Unión Europea de verdad, pero mientras no la tengamos no tendremos una defensa europea de verdad y, por lo tanto, la única defensa europea seguirá siendo la OTAN. Por eso me parece absolutamente necesario que la Unión Europea –siempre se critica y se dice que debiera ser más, pero si nos fijamos en lo que era cuando se firmó el Tratado de Roma se ve que se ha avanzado mucho– y la OTAN cooperen.

GEORGINA HIGUERAS
Moderadora

Tiene ahora la palabra Suleyman Anil, miembro del equipo de defensa cibernética de la OTAN y jefe del equipo de respuesta a incidentes cibernéticos, además de responsable de la coordinación internacional.

SULEYMAN ANIL
Miembro del Centro de Ciberdefensa de la OTAN en Mons

En mi intervención haré una descripción de las amenazas, tal y como lo vemos desde la OTAN, y plantearé cómo asistimos a los

Estados miembros en el asunto de las ciberamenazas y las ciberemergencias. También diré algo brevemente sobre la próxima cumbre de la OTAN, que se celebrará en septiembre en Cardiff.

Las amenazas quedaron definidas en la OTAN en 2010, un año importante tanto por la Cumbre de Lisboa como porque se aprobó el plan estratégico para 2010-2020. Antes de la elaboración de este plan se encargó un informe a un grupo de diplomáticos y políticos experimentados dirigido por Madeleine Albright. En ese informe se identificaban amenazas estratégicas a las que los aliados harían frente en la siguiente década y, entre éstas, aparecían el terrorismo internacional y las amenazas cibernéticas. Como digo, esto quedó reflejado en el plan estratégico que se aprobó en la Cumbre de Lisboa de 2010. No se decía que la ciberdefensa podía ser algo colectivo pero sí que las ciberamenazas podían suponer una amenaza tanto para la seguridad nacional como para la seguridad transatlántica. La postura de la OTAN respecto de las ciberamenazas parte pues de ahí.

Me gustaría compartir con ustedes algunos parámetros en términos de amenazas. Antes se hablaba de conflictos del futuro, pero ahora hablo de conflictos del presente, porque todos los conflictos a los que hacemos frente hoy en día tienen un componente cibernético a distintos niveles. Lo que ha ocurrido en Ucrania, por ejemplo, ha tenido varios elementos cibernéticos. Otro parámetro es el servicio de ataque, que se está expandiendo rápidamente, pues los puntos en los que se conectan las redes son blancos de ataque. Es éste además un conflicto asimétrico, pues alguien con pocos recursos puede alcanzar las capacidades necesarias para un ciberataque. En la parte más positiva de la moneda está no obstante el hecho de que la inversión en ciberdefensa también es asimétrica: las inversiones en ciberdefensa son bastante modestas si se comparan con las que se hacen en otro tipo de defensas, pues proteger las redes de la OTAN cuesta casi lo mismo que un helicóptero. Esto es el lado positivo de la asimetría.

¿Dónde somos más vulnerables? Sin duda en las infraestructuras críticas. Allí y en nuestro comercio. Para hincar de rodillas a un país basta con cortar el suministro eléctrico, que hoy en día además está interconectado en los países desarrollados. Otro ejemplo del aspecto económico de esta amenaza es que, según dijo una nación, un ataque determinado contra un grupo empresarial costó seis millones de euros en pérdidas, además de tres mil puestos de trabajo. Este paisaje de amenazas es lo que hace que el ciberespacio sea diferente a otros dominios.

La acción de la OTAN en el ciberespacio tiene dos partes. Una de las cosas que no son muy conocidas de la OTAN es que, como organización, posee sus propias infraestructuras de comunicación. Esto la diferencia de la Unión Europea y de la ONU. La OTAN gestiona sus propias infraestructuras con personal de la OTAN, en una red que va de Noruega a África, de América a Afganistán. De hecho, esta infraestructura es prácticamente la única cosa que la OTAN tiene, porque no posee ni siquiera los edificios en los que trabajamos, que son propiedad de los países en los que están emplazados. Por eso la OTAN reaccionó antes que otras organizaciones ante las ciberamenazas, pues en las operaciones de finales de los noventa en los Balcanes nos dimos cuenta de la debilidad de nuestros sistemas de mando, control y comunicación. Aquélla fue la primera vez que actuábamos fuera de nuestro territorio y sufrimos muchos percances. Hubo un informe al respecto, con consecuencias políticas; de ahí que en 2002, en la Cumbre de Praga, el comunicado hablara ya de ciberamenazas.

La principal función de la OTAN es su misión de asegurar la seguridad colectiva, la gestión de crisis y la seguridad cooperativa. Tenemos pues que asegurarnos y ocuparnos de que las redes de la OTAN funcionen y de que no estén sujetas a los problemas del ciberespacio. Ése es nuestro principal objetivo en la división. Como en el resto de los dominios, en tierra, aire y mar, también en el ciberespacio, cuando un Estado miembro sufre

una amenaza a su seguridad nacional, la OTAN tiene que ofrecer una defensa colectiva. En nuestro ámbito, este papel de ayudar a los Estados miembros tiene que entrar en efecto cuando la seguridad nacional está comprometida –como en el resto de los dominios– y sólo cuando el Estado afectado pide ayuda.

¿Cómo lo hacemos? Bueno, respecto a la primera tarea trabajamos muy duro para reforzar la seguridad de nuestras redes. Recientemente logramos reforzar nuestras capacidades tecnológicas tras un periodo conflictivo, llegando a un acuerdo el 23 de mayo de este año. Podemos proteger 51 puntos de la red de la OTAN desde los cuarteles generales en Bruselas, donde tenemos un equipo de más de un centenar de expertos que, con la tecnología disponible, pueden detectar incidentes –ya sea en la red en Afganistán, en algún país miembro o en los cuarteles– y pueden responder a estos ataques. También tenemos los medios necesarios para trasladar a un equipo si se necesita asistencia en un lugar en concreto. Y nos hemos integrado en todos los procesos de la OTAN. Por ejemplo, el desplazamiento de recursos para una operación militar actualmente tiene siempre un componente cibernético. En un momento se discutió si debía haber otro departamento distinto, pero se llegó a la conclusión de que era mejor y más eficaz integrar la ciberdefensa en todas las otras áreas. Invertimos mucho en recursos.

Sobre la defensa de nuestros aliados, ésta es la parte que afecta más a España, que ha sido uno de los campeones en la ciberdefensa debido a los avances de los dos últimos años. Hay tres áreas en las que la OTAN ayuda a los Estados miembros en ciberdefensa. La ciberdefensa se discute no sólo a nivel ministerial, entre los encargados de defensa, sino también en minicomités. Así que los 28 países miembros se reúnen y hablan sobre cualquier aspecto del ciberespacio, técnico o de inteligencia, sobre el sector privado o sobre lo que sea. Este enfoque común centrado en la ciberdefensa ha mejorado el progreso de los Estados en esta materia.

La segunda forma de asistencia es mediante el desarrollo de capacidades específicas. La OTAN tiene dos mecanismos para acometer esta tarea. Uno es nuestro tradicional o antiguo diseño de plan de defensa, o EDP. La OTAN define objetivos de capacidad en distintas áreas, ya sea aire, tierra o mar, y desde 2013 también en ciberdefensa. Y el último año todos los Estados miembros aceptaron esos objetivos y acordaron que los cumplirían en distintos calendarios, pero que todos llegarían a ellos en 2019. No se trata de nada mágico sino de tener en orden las normas, las leyes, los entrenamientos, las estructuras, los equipos, etcétera. Es decir, los requisitos mínimos y esenciales.

También tenemos el concepto del *Smart Defense*. Como en la OTAN somos muy buenos en temas burocráticos, tenemos tres fases en ciberdefensa y *Smart Defense*, que implican que no todos tienen que estar en la misma situación. Es decir, si cinco o seis naciones están interesadas en desarrollar una determinada capacidad en ciberdefensa, pueden seguir adelante sin que se financie con el fondo común. Así somos más flexibles y, además, otras naciones pueden ser invitadas a participar.

El tercer área en la que la OTAN ayuda los aliados es en la construcción de capacidades y el entrenamiento. Las dos escuelas de la OTAN cada vez incluyen más entrenamiento en ciberdefensa. De hecho, está previsto que la escuela radicada en Italia se traslade a Portugal y, cuando esto ocurra, tendrá un foco especial en ciberdefensa y se llamará Escuela de Ciberdefensa. También los ejercicios militares de la OTAN incluyen escenarios de ciberdefensa; hay un ejercicio sobre las cibercoaliciones en el que el año pasado participaron en Tallin más de cuatrocientos expertos de los distintos países.

Para concluir me gustaría hablar de la próxima cumbre que se celebrará en septiembre en Cardiff. En ella, la OTAN anunciará un paquete de medidas de ciberdefensa, cinco o seis puntos que explicarán la postura de la organización en el campo de la ciberdefensa y su disposición a implementarlas. Además, se ha

aprobado ya por los ministros de Defensa el tercer documento de política de ciberdefensa. Los dos anteriores, de 2007 y 2010, fueron elaborados en respuesta a determinados hechos, pero en esta ocasión se trata de la declaración práctica y madura a la que ha llegado la OTAN para dar respuesta al ciberespacio.

Finalmente quiero decir que el ciberespacio es un dominio distinto a los demás, con sus propios parámetros y características, la más importante de las cuales es que es muy joven comparado con otros. Mis hijas veinteañeras no pueden creer que cuando ellas nacieron no hubiera Internet. Nos llevó siglos construir las normas internacionales que rigen otros dominios y, claro, aún no hemos llegado a ese punto con el ciberespacio. Quizás en una década veremos cuáles son las amenazas y las respuestas oportunas. Pero tampoco hay razón para mitificarlo, porque toda nuestra sabiduría y nuestro conocimiento sobre seguridad se aplican igualmente al ciberespacio. Así pues, no hay que volver a inventar la rueda al tratar la ciberseguridad. El principal mensaje que quiero compartir con ustedes es que debemos tirar hacia adelante y ponernos a trabajar, porque el trabajo entre los aliados puede crear un ciberespacio que sea seguro. Hay oportunidades para ello.

No olvidemos que, desde la invención de la máquina de vapor no habíamos tenido una nueva tecnología que nos permita avanzar y compartir tanto.

GEORGINA HIGUERAS
Moderadora

Hay varias cosas que me han llamado la atención de lo que ha dicho. Por ejemplo, que la OTAN sea, sobre todo, una estructura de información, que lo básico de la OTAN sea esa estructura de información. ¿Cómo se comparte esa información? ¿Todo lo que hay dentro de la OTAN se comparte entre los 28 miembros? ¿Qué niveles hay?

SULEYMAN ANIL
Miembro del Centro de Ciberdefensa de la OTAN en Mons

Claro que hay varios niveles. Hay un Comité de Inteligencia y otros comités, como en todas partes. Para contestar de forma general, a nivel político la OTAN no puede levantar un dedo contra los países miembros; son ellos los que deciden. En el área del ciberespacio nos hemos enfrentado a ciertos retos en lo relativo a compartir información, especialmente en asuntos técnicos, porque hay temas delicados. Pero estamos trabajando en ello y tenemos el Civilian Intelligence Committee y un panel sobre ciberespacio. También hemos celebrado un taller en Madrid que reunió al Comité de Ciberinteligencia y al Comité Técnico para intercambiar información. Y celebramos otro en Bucarest con unas cien personas. Además, este año hemos creado tres *focus groups* concentrados en una determinada área de amenazas, como puede ser una región o un *malware*. Así que la OTAN ofrece una excelente plataforma para compartir información a todos los niveles. Basta con saber que cada año celebramos un simposio al que asisten unas 1.500 personas. Después, son las naciones quienes deciden cuánto quieren compartir. Aun así, puedo decir que la relación entre los departamentos de inteligencia y los técnicos ha mejorado en los últimos años. Pero, como es natural, hay cosas que deben ser compartidas y otras que no. Compartir información es esencial y la única manera de conseguirlo es que los expertos técnicos demuestren que son necesarios. Mis colegas tienen buena predisposición, pero hay que convencerlos de que es mejor que trabajen juntos para solucionar los problemas comunes.

GEORGINA HIGUERAS
Moderadora

Pasamos al tercer ponente. David Ramírez Morán es Analista Principal del Instituto de Estudios Estratégicos de España, don-

de investiga temas de seguridad, ciberdefensa y economía e industria de defensa.

DAVID RAMÍREZ MORÁN
Analista Principal del Instituto de Estudios Estratégicos de España

Empezare por decir que, en mi opinión, desde que se han definido cinco dominios que proteger, intentamos generalizar la forma de abordar estos cinco dominios. Hasta la fecha eso ha funcionado, aunque con ciertas salvedades, ya que el ciberespacio no puede ser abordado de la misma manera que se abordan los dominios tradicionales. Con el ciberespacio nos hemos encontrado que la dificultad para adaptar lo que sabíamos hacer ha sido todavía mayor. Tenemos una principal dificultad, que es la atribución: ¿quién me está atacando? En una guerra convencional, el enemigo tenía una bandera, por lo que sabías quien te atacaba. Ahora, primero debemos averiguar quién es, y en este apartado no basta con saber el origen, con tener trazas que indiquen de dónde procede el ataque; si no sé exactamente la identidad del atacante no puedo contrarrestarle, no puedo responderle. Además, tenemos un segundo problema. Cuando establecemos la diferencia entre defensa y ciberseguridad, entendemos defensa como protección de mis intereses de la frontera hacia fuera, mientras que la seguridad incluiría mis intereses de puertas adentro, por lo que surge un problema a la hora de diferenciar cada tipo de ciberataque. El oponente puede utilizar las mismas herramientas en ambos casos, quizás con pequeñas diferencias. Y los mecanismos de ataque también van a ser similares si están atacando una empresa o un organismo público; en definitiva, se trata de acceder a información utilizando técnicas similares. Asimismo, un mismo objetivo puede ser objeto de defensa u objeto de ataque por intereses económicos, y las características de este ataque tampoco me dejaran claro si me están ata-

cando con objetivos de llegar a mayores o si ése no es el caso. Por todo ello, creo que tenemos que adoptar una postura diferente en el sector de la ciberdefensa, como de hecho lo estamos haciendo, adaptando nuestros procedimientos y creando unos nuevos para abordar estas nuevas diferencias.

Una vez caracterizado el contexto, aprovecho para decir que me parece acertado que la sesión se titule con una pregunta: «¿Aliados ante los ciberataques?». El problema es que cuando preparaba mi ponencia todo lo que me salía eran nuevas preguntas. Porque, en efecto, hay una diferencia de inversión entre los diferentes países, pero ¿cómo se pueden medir esas inversiones? Si en el mundo de la ciberdefensa estamos cooperando empresas, ciudadanos, administraciones y organizaciones públicas, ¿dónde empieza y dónde acaba lo que qué es la ciberdefensa, qué es ciberseguridad y qué es seguridad privada? La frontera es bastante difusa, ya que cualquier vulnerabilidad puede suponer un serio riesgo, tanto a nivel local como nacional o, incluso, internacional. Y si mis sistemas pasan a formar parte de una *world net* yo mismo estoy suponiendo un riesgo para otros países, dado que pueden ser atacados a través de los medios que yo pongo en juego. Y también surge la duda de cómo se dota un Estado. ¿Se ha dotado correctamente invirtiendo dinero de puertas afuera? Hay que saber cómo y en qué se ha invertido ese dinero, qué herramientas le han proporcionado, cómo y dónde puede dotarse con ese dinero. En caso de que un Estado tenga capacidades propias nacionales, como puede ser el caso de los países más desarrollados, ese dinero se traduce en que sus empresas puedan mantener unos productos con unas características que supongan una solución. Sin embargo, un país más pequeño o que tenga una industria local que no le permite acceder a esos productos, ¿a quién accede, a quién le compra? Deberíamos cuestionarnos pues en ese caso qué tipo de productos puede comprar, cómo mide la calidad de un producto, cómo puede saber el nivel de seguridad que le está aportando ese producto.

Como ven, las preguntas se multiplican rápidamente, porque no tenemos referencias fiables. Podemos decir que un país está bien dotado cuando es capaz de responder ante ciertas amenazas o ataques, pero sabemos que esos ataques están cambiando día a día. Cada día que pasa puede aparecer un *zero day*, una nueva vulnerabilidad en un sistema operativo o una nueva vulnerabilidad de un protocolo. En determinado momento puedo tener un alto nivel de cobertura pero, mañana mismo, puede ser que la inversión sea cero, máxime si justo en ese momento se materializa un ataque. Por lo tanto, ¿podemos decir que el hecho de ser capaces de soportar ciertas amenazas o ataques define lo bien preparado que está un país en términos de ciberdefensa? Ésa podría ser una manera de medirlo, aunque también podríamos usar otras medidas. Otra sería mediante la definición de unas herramientas que definan el «deber tener», pues en caso de no disponer de esas herramientas eres totalmente vulnerable. Eso nos permitiría saber que aquellos países que tengan esas herramientas han cumplido el mínimo de inversión, con lo cual estarían en igualdad de condiciones con otros países. Pero este sistema también plantea problemas. ¿Quién desarrolla las herramientas? ¿En qué mercado están y que fiabilidad me dan? Yo, como empresa nacional, puedo vender todas mis capacidades o vender sólo herramientas adaptadas al tipo de país que las va a adquirir. Y queda por dilucidar si lo desarrollamos de manera individual o en colaboración. Todas éstas son dudas que me surgen y a las que, sinceramente, me cuesta mucho responder. Además hay que tener en cuenta que hay herramientas que quizá no se pueden desarrollar de manera puntual. Si me están atacando con una *botnet*, ¿cómo hago para defenderme? Me puedo poner de acuerdo con todos mis aliados o puedo desarrollar mi propia *botnet*. Tenemos pues una desigualdad que es complicada de abordar, máxime si tenemos en cuenta que si vamos a actuar como aliados tendremos que establecer mecanismos de interoperabilidad. O bien ponemos todos nuestros recursos en una cesta, para que

cuando tengamos que usarlos baste con apretar el interruptor, o bien establezco los mecanismos de tal forma que las herramientas de cada uno de los países funcionen de forma coordinada y me den protección como organización aliada frente a un atacante cuya dimensión no conozco; como ya he dicho, puede ser una persona controlando una *botnet* o un Estado con el respaldo de cien mil personas.

Dentro del mercado de seguridad, me gustaría establecer una diferencia entre la naturaleza de los países por sus capacidades tecnológicas; no tanto por su capacidad de desarrollarlas como por la cantidad de dispositivos, tanto *hardware* como *software* –me van a permitir que llame dispositivo al *software*–, que desarrollan, pues tener la capacidad de desarrollo del *hardware* al *software* se convierte en un elemento vital. Es bastante complicado esperar que mientras ciertas naciones desarrollen cierto tipo de *software* o tienen acceso a esa cadena de desarrollo, haya otras naciones que no consigan ese nivel de capacidad.

Por último, dentro de este mercado surge a menudo una pregunta: si hay una vulnerabilidad en el mercado negro, ¿la compro o no? ¿Cómo regulamos el mercado cuando un organismo internacional como la OTAN podría ser atacado por esas vulnerabilidades? Una vez solucionado el problema que supone ponernos al mismo nivel es cuando entramos en el tema de la cooperación. A mí me genera tranquilidad ver que existe una aproximación generalizada, que la forma de colaborar en la ciberdefensa es compartir información, ya que todos sabemos que disponer de las herramientas de una potencia es un elemento vital. Primero porque me proporciona seguridad y capacidad de disuasión, con lo cual ya no hay que distribuirlas de forma abierta y convertirlas en posibles fuentes de riesgo para otras naciones al vendérselas, lo que podría suponer un serio problema. Aparte de compartir la información, considero importante la realización de ejercicios. En ellos se mantiene la seguridad de cada uno de los equipos participantes, yendo cada uno con sus herramientas, pe-

ro al mismo tiempo se comparten el conocimiento y la formación de otras naciones que se han enfrentado a otros problemas similares, o se lanza un problema de una nación a otra para que las dos partes extraigan conocimientos de ello. En la cooperación se habla de la simetría entre los diferentes países, pero aquí son relevantes los diferentes conceptos de defensa que tiene cada país. En el mundo hay más de doscientos países. Si nos ceñimos a OTAN somos 28 países, pero sabemos que dentro de este grupo la forma de abordar la ciberdefensa de los distintos países es bastante distinta: desde la postura de Estados Unidos, que considera todo ciberataque una acto de guerra, hasta la postura europea, donde los ciberataques se consideran incidentes de seguridad que se intentan paliar con los mejores medios disponibles. En este entorno cabe un conflicto, debido a las diferencias de potencial económico y armamentístico entre las distintas naciones, que pueden dejar al descubierto a algunas de ellas. Lo cierto es que todo esto también me despierta muchas dudas.

Para acabar quisiera hablar sobre el equipo de respuesta rápida que se menciona en el programa del seminario. Y, de nuevo, me surgen dudas. ¿Cuándo se podría poner en funcionamiento? Dado que ya tenemos el equipo de respuesta rápida, si un país tuviera un incidente de ciberseguridad, ¿cómo se pondría en marcha el protocolo? Hay que tener en cuenta que, en ciberseguridad, el tiempo de respuesta no se mide en años, meses, semanas o días, sino que hablamos de minutos, de segundos, y es necesario tener un mecanismo de respuesta rápida que intervenga antes de que el ataque consiga su objetivo. Tal y como lo estamos haciendo en la OTAN, bajo la fórmula del *Smart Defense*, a la que los países se van apuntando o no en función de que quieran o no participar, me cuesta hacerme una imagen clara de cómo podríamos estructurar ese tipo de defensa.

Son muchas dudas pues, que yo achaco a que estamos viviendo un mundo muy joven. Dado que yo también me considero todavía bastante joven, no sé si es el mundo o si soy yo o si

es una combinación de ambos factores, pero lo cierto es que no llego a tener respuestas para todo. Pero he de reconocer también que me queda mucho por leer y por aprender.

GEORGINA HIGUERAS
Moderadora

Si los no expertos ya teníamos muchas preguntas, David no ha puesto sobre la mesa otro montón más. No sé cómo dormiremos esta noche. Es el turno del último ponente, Greg Austin, al que casi no hace falta presentar, ya que ya participó esta mañana en la primera sesión del seminario.

GREG AUSTIN
Miembro Investigador del East-West Institute

Quisiera exponer tres puntos. El primero es que nada ocurre en el ciberespacio sin un impacto real en potencia en el mundo físico. Debemos tener esto en cuenta. Todo de lo que hablamos tiene un impacto político potencial. Esto significa que los ciberaliados necesitan saber lo que sus socios hacen en el ciberespacio. Por ejemplo, pensemos en 1999, cuando Estados Unidos recurrió a sus aliados de la OTAN para emplear armas de información contra la antigua Yugoslavia. Se discutió esa posibilidad en la OTAN, pero finalmente no se aprobó la utilización de armas de información. De todas formas, los estadounidenses las usaron por su cuenta y es muy importante recordar que ésa fue la primera vez que hubo ciberoperaciones importantes en una guerra. No hablamos de algo tan lejano, sino de hace quince años. Por otro lado, casi inmediatamente después de ser elegido, Putin aprobó la doctrina de seguridad de información de Rusia. Lo digo porque es interesante mirar esto desde el punto de vista de la causa y el efecto. Pero lo contrario también es cierto. Lo que pasa en el mundo real también tiene un impacto en las ciberpolíticas. Por ejem-

plo, la crisis de Ucrania ha hecho que la OTAN redefina su postura respecto al ciberespacio y la planificación militar.

Esto nos lleva al segundo punto. En 2010, y su secretario de Defensa de Estados Unidos planteó la posible creación de un ciberescudo para la OTAN, en la línea del escudo antimisiles. Pero ese concepto ha cambiado radicalmente en los últimos cuatro años, pues la OTAN ha mejorado sus defensas y ahora, en determinados círculos, se discute la posibilidad de pasar de la ciberdefensa a la capacidad de ciberataque. Hay un largo camino hasta que se implemente esa transición, pero yo diría que se ha acelerado debido a la crisis en Ucrania.

El tercer y último punto es que lo que vemos en la OTAN es una globalización de la Alianza en el ciberespacio. En los últimos dos o tres años ha habido una serie de discusiones entre la OTAN y otros gobiernos que no pertenecen a la Alianza sobre posibles acuerdos. Existen acuerdos formales entre la OTAN y muchos países; no daré la lista completa pero están Australia, Arabia Saudí, Japón, etcétera. De hecho, los ejercicios de defensa que realizó la coalición en 2014 incluyeron también ejercicios de ciberdefensa de los que formaron parte representantes de países no miembros como Suiza o Nueva Zelanda. Así que, en su actuación cibernética, la OTAN trabaja con países que están muy lejos de la Alianza y de Europa. Por poner otro ejemplo, Japón y Estados Unidos recientemente aprobaron un acuerdo relativo a la ciberdefensa y a temas militares, ya que Japón y China tienen un viejo enfrentamiento. Sin duda, estas alianzas de Estados Unidos fuera del ámbito europeo tienen una importancia potencial para el futuro de las ciberoperaciones de la OTAN.

GEORGINA HIGUERAS
Moderadora

Se abre el turno de preguntas.

FERNANDO ORGAMBIDES
Periodista y escritor

Estamos hablando de la OTAN y de la Unión Europea como entes monocordes, sostenidos por Estados miembros con mayor o menor eficacia y con mayores o menores presupuestos individuales. Pero alguno de estos Estados miembros o países aliados sufren en amenazas secesionistas en su seno, cada vez más intensas a causa del auge de los nacionalismos. ¿Podría alguno de estos posibles ataques, de veinte, treinta o cincuenta millones de dólares –como aquí se ha dicho–, provocado no por lobos solitarios sino por estrategias de intereses desestabilizadores, llevar a los Estados miembros, o a algún Estados miembro, al extremo de no poder controlar su propio territorio, o incluso de verse abocado a un rompimiento de su propia seguridad nacional? En suma, ¿podría un ataque de esas características llevar a un Estado miembro al caos?

Por otro lado quisiera hacer una segunda pregunta al hilo de lo último que se ha planteado sobre el concepto monocorde de la OTAN y la Unión Europea. Parece que detrás de los ciberataques hay una intencionalidad prioritaria, que es el espionaje industrial, el robo industrial. ¿Cómo se contempla desde la OTAN y la Unión Europea –como entes aglutinadores– esa desconfianza que puede surgir entre países miembros? Me refiero al caso de que desde un país miembro se intente atacar a otro país miembro con el objetivo de conocer sus tecnologías nacionales o para robárselas, ya no desde fuera, sino desde dentro.

SULEYMAN ANIL
Miembro del Centro de Ciberdefensa de la OTAN en Mons

No sé si estoy en una posición de hablar sobre movimientos secesionistas. Creo que lo mejor que puedo decir es que los aliados representan a las naciones tal y como están definidas.

GREG AUSTIN
Miembro Investigador del East-West Institute

Son preguntas difíciles, pero buenas, pues apuntan hacia el espectro amplio de lo que está en juego en la ciberdefensa, ya que ésta abarca la seguridad interior, la seguridad industrial y la seguridad militar. Está claro que la evolución de las políticas de la Unión Europea y de la OTAN ha sido muy lenta en todas estas áreas. La Unión Europea, por ejemplo, aún no acepta la ciberseguridad como una competencia común perteneciente a la política de seguridad común. Queda pues mucho camino por andar. Sobre el espionaje industrial sólo decir que su pregunta subraya que dicho espionaje es un coste habitual en determinados tipos de negocios y que no hay nada realmente inusual en que lo haga China, puesto que Francia e Israel también lo hacen. Como decía, son buenas preguntas, pero no hay respuestas.

ÁNGELES BAZÁN
Informativos de Fin de Semana de RNE

¿Hasta qué punto la desconfianza que genera la constatación del espionaje de uno de los aliados al resto frena o impide el intercambio leal de información? Me refiero a eso que decía el embajador de «confía pero verifica». ¿La constatación del espionaje de Estados Unidos al resto de aliados da más peso a la parte de verifica que a la de confía?

CARLOS MIRANDA
Embajador. Exrepresentante Permanente de España en el Consejo de la OTAN

Es difícil responder, pues habría que hacerlo caso por caso. Greg Austin acaba de decir que todo el mundo practica el espionaje industrial. De hecho, hay una cierta conciencia de que tus mejo-

res amigos lo hacen y de que ellos saben que tú también lo haces. El problema surge cuando eso sale a la luz pública. Pero hay límites y esos límites probablemente estarán dictados por la confianza que se tiene respecto a un país amigo o aliado. Es decir, no es lo mismo que uno se sienta «traicionado» por un aliado –pongamos por ejemplo por Francia o por Estados Unidos– a que algo así ocurra con otro país que es amigo, con el que tenemos buenas relaciones –pongamos Argentina o un país asiático–, pero que nos coge más lejos. Así pues, creo que estamos ante una situación en la que hay conciencia de que estas cosas pasan pero en la que se piensa que es mejor hacerlo menos con los más amigos. Tengamos en cuenta que los círculos de relaciones internacionales –ya sean bilaterales o entre ciertos grupos de países que se sienten más afines– permiten tener mucha información sobre lo que cada uno hace, hasta qué punto ha llegado, etcétera. Por tanto no suele ser necesario llegar hasta el punto de espiar el teléfono de un Primer Ministro de otro país. Cuando se llega a esos extremos, desde luego, surgen problemas. Pero, en fin, estamos en un mundo muy ambiguo.

5. CIBERDEFENSA, UN ELEMENTO ESENCIAL EN EL PROCESO DE TRANSFORMACIÓN DE LAS FUERZAS ARMADAS

ALMIRANTE
FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

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

El Almirante Fernando García Sánchez

MIGUEL ÁNGEL AGUILAR
Moderador

Antes de dar paso a la intervención del Almirante Jefe del Estado Mayor de la Defensa quiero decirles que estamos muy felices de tenerle aquí un año más y del afecto y la cercanía que nos ha demostrado siempre, tanto a la Asociación de Periodistas Europeos como a este seminario, del cual celebramos la XXVI edición; algo que se puede calificar como un caso de tozudez. Cada año nos reunimos aquí periodistas, militares, analistas y estudiosos para analizar distintos asuntos relacionados con la seguridad y la defensa, siempre buscando una tangente con asuntos europeos. En esta ocasión estamos explorando mundos nuevos: las ciberamenazas y las respuestas a éstas. El Almirante nos va a hablar de «Ciberdefensa, un elemento esencial del proceso de transformación de las Fuerzas Armadas»; o, si se prefiere, de cómo ha incidido este asunto de la ciberdefensa sobre las Fuerzas Armadas y su modernización.

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

Quiero agradecer esta invitación a participar en el seminario y la oportunidad que se me brinda de poder transmitirles una serie de

ideas relacionadas con dos temas de vital importancia hoy en día en las Fuerzas Armadas españolas y, en general, de todo Occidente. Hablaré pues del proceso de transformación y del impacto que el ciberespacio y la ciberdefensa ejercen sobre este proceso de transformación.

Quiero iniciar mi intervención apuntando qué entendemos por proceso de transformación. Para entenderlo creo que ayuda enfrentarlo a lo que es una simple evolución. Si estamos hablando de adaptarnos a una situación, de ajustarnos a una situación que nos llega de fuera, estamos evolucionando, adaptándonos. El proceso de transformación, sin embargo, tiene un fondo algo más ambicioso: ahí intentamos adelantarnos a los acontecimientos, crear, desarrollar, poner en marcha conceptos, organizaciones y capacidades que nos permitan diseñar el futuro, controlar y hacer el futuro. La transformación es en realidad el núcleo detrás de la frase que el actual presidente de Estados Unidos utilizó en su campaña electoral, ese «nosotros podemos». Podemos si nos transformamos.

Las Fuerzas Armadas en general, no sólo las españolas, tienen en sus genes esa necesidad de transformarse, de adaptarse, de evolucionar y de avanzar –más allá de poder prever qué va a pasar– para poder desarrollar, crear y controlar ese futuro que queremos tener para todos nuestros conciudadanos.

Podemos señalar una serie de hitos que en el último siglo han obligado a transformarse a las Fuerzas Armadas. A principios del siglo XX aparece la utilización del espacio aéreo y se tienen que crear las Fuerzas Aéreas. Surgen entonces unas nuevas Fuerza Armadas, una nueva organización, unos nuevos sistemas, que de forma horizontal afectan a su estructura organizativa, a los niveles tácticos en su nivel operacional y estratégico. Es decir, las Fuerzas Armadas se transforman a partir de la utilización de nuevos conceptos, medios y capacidades para gestionar un futuro en el que el transporte aéreo, la utilización del espacio como elemento para el desarrollo de la sociedad civil y de utili-

zación de armas, afecta a toda la teoría de la guerra. Se crea pues un nuevo teatro de operaciones, que es el aire.

Si avanzamos cronológicamente, después de la Segunda Guerra Mundial aparecen dos conceptos, uno operativo y otro orgánico o sociológico. Son elementos de transformación que pretenden crear unas Fuerzas Armadas que sean capaces de manejar el futuro. Uno de esos conceptos es la prioridad del conjunto. Las Fuerzas Armadas no pueden trabajar en tierra, mar o aire independientemente, sino que tienen que trabajar en una acción conjunta. Este concepto desarrolla estructuras y organizaciones y, como ocurre con todos estos hitos importantes que afectan a la transformación de las Fuerzas Armadas, afecta a los tres niveles que los militares definimos: el nivel táctico de acción cercana; el nivel operacional, donde se coordinan diferentes acciones; y el nivel estratégico, que es el estudio global de una situación. También se da un cambio desde el punto vista sociológico –o se intuye que va a haberlo– y las Fuerzas Armadas se preparan para el cambio con un modelo que se ha dado en llamar el modelo institucional que pasa a un modelo ocupacional. Las Fuerzas Armadas ya no se rigen por el mero y único principio de la antigüedad y de la salud. En la Armada decíamos: «¿Qué es un Almirante? Es un Teniente de Navío con buena salud». El modelo ocupacional va desarrollando nuevas estructuras y va organizando nuevos sistemas y formas de prepararse para el futuro; los criterios que afectan son ahora de mérito, de capacidad.

Cuando caen las Torres Gemelas en 2001, surge algo tan conocido en España desde el siglo XIX como es la guerra de guerrillas, que se convierte en un elemento fundamental. La guerra asimétrica, la guerra ambigua, la guerra irregular, se convierte en un elemento y las Fuerzas Armadas tienen que transformarse para hacer frente a estos elementos, para poder manejar un futuro seguro con estas nuevas entradas. Se ve también que en esta guerra no todo se puede solucionar –o casi nada se puede solucionar– con opciones militares: hacen falta opciones de diferen-

te índole y hace falta una aproximación global a los problemas. Estos conceptos también provocan transformación, provocan desarrollos conceptuales, desarrollos orgánicos, desarrollos de sistemas que hagan posible manejar el futuro.

Éste es el mundo en que la sociedad, y concretamente las Fuerzas Armadas, están inmersas. Hace dos décadas se usaban las siglas en inglés RMA (revolución de los asuntos militares), que Estados Unidos puso de moda. Después esto desembocó en los mandos o procesos de transformación: hace ya una década se creó el Mando de Transformación en la OTAN y hay un Comandante Supremo –con el título de Comandante de Transformación– que tiene la obligación de transformar la Alianza Atlántica para organizar y diseñar el futuro. Actualmente la transformación está integrada en los procesos de entrenamiento. Y en esa integración de la transformación en los procesos de entrenamiento se incluye también la ciberdefensa de una manera horizontal. Se define un nuevo teatro de operaciones que afecta a la organización, a los sistemas, y que tiene impacto sobre los niveles táctico, operacional y estratégico.

La importancia del ciberespacio está íntimamente unida a la importancia que la sociedad de la información, y la sociedad del conocimiento están adquiriendo hoy en día. La capacidad de transmitir y utilizar información, o de manejar bases de datos, que actualmente tenemos –y a la que tiene acceso cada vez más gente en el mundo– hace que la globalidad de esa capacidad de manejo y de intercambio de información nos haga cada vez más vulnerables en este espacio o teatro de operaciones que es el ciberespacio.

El mismo concepto de globalización hace que todas las cuestiones relacionadas con la ciberseguridad y con la ciberdefensa adquieran una mayor prioridad. Esto no es pura teoría, sino que en la práctica lo estamos viviendo cuando observamos la situación estratégica que tenemos a nuestro alrededor: problemas tan actuales como las crisis en Siria, Ucrania o Irak, o la situación de

incertidumbre que rodea diferentes áreas del mundo, como el Lejano Oriente, con los problemas del mar de China y Japón, o el Sahel. Y también está la utilización de los lugares comunes por el crimen organizado: tanto del narcotráfico como del tráfico de armas o el tráfico de seres humanos. Todo esto hace que el ciberespacio sea utilizado y explotado por todos los elementos en sentido positivo y en sentido negativo. El control y capacidad de actuar, si queremos controlar ese futuro, nos obliga a conocer y a tener medios que sean capaces de actuar en este ámbito.

Generalmente se identifican tres espacios comunes que tienen una gran importancia: el marítimo, el aéreo y el ciberespacio. En estos espacios comunes tienen lugar todo tipo de actividades todo el tiempo. Nuestra sociedad tiene que intentar controlar lo que ocurre ahí para poder construir un futuro de seguridad que permita el desarrollo económico y de las libertades, en definitiva. La ciberdefensa es un modelo actual que se caracteriza por tres elementos que he citado anteriormente: por un lado, la globalización; por otro, la aproximación a un problema desde diferentes aspectos; y, por último, la capacidad de difusión de una forma rápida de la información o de la actuación en un espacio donde el concepto frontera y el concepto territorio no existen. Con esto aparece un nuevo elemento de transformación que arrastra la ciberseguridad, que es el concepto de influencia.

Hoy en día la capacidad de vencer o de ser derrotado no se mide tanto en relación con la capacidad de conquistar un terreno, de tomar una cota o de dominar un determinado mar; se mide en la capacidad de influir en los ciudadanos para conseguir los objetivos que se pretenden. Esa capacidad de influencia es algo que se ha visto muy claramente en el caso de Rusia y en cómo ha abordado el caso de Crimea. La capacidad de influencia ha jugado un papel fundamental en la anexión de Crimea.

Se podría profundizar más en el tema, pero básicamente éste es el mundo que se nos viene encima y éstas son las cuestiones en las que tenemos que pensar. Tenemos que transformarnos

para poder controlar estos frentes y para poder organizar nuestra sociedad. Las Fuerzas Armadas, como elemento integrante, como parte de estos mecanismos de defensa y seguridad de nuestro país, deben tratar de controlar estas actividades. Éste no es un problema exclusivo de España, sino que es algo que se discute en los foros internacionales. Nosotros estamos en la OTAN y en la Unión Europea, donde de esto es de lo que se habla y en lo que se está trabajando. Así, en la cumbre de la OTAN del próximo septiembre se hablará del concepto de ciberseguridad en la Alianza Atlántica. En la Unión Europea hay ya un concepto de ciberseguridad sobre el que se está avanzando, y se está empezando a estudiar la doctrina sobre la ambigüedad y cómo se pueden manejar situaciones; sin llegar nunca al límite que provoca una reacción militar clara y agresiva, sino consiguiendo que la parte de la población que nos interesa consiga los efectos que nosotros deseamos.

En Lituania, de entre los seis millones de ciudadanos totales dos millones son pro-rusos. Es decir, la capacidad que se puede tener para manejar esa base social con unos criterios de influencia es tremenda. En este proceso de utilizar la influencia para conseguir objetivos políticos, la guerra es la continuación de la política por otros medios; esto no es la División Acorazada, pero es guerra a través de mensajes con influencia. Si se consiguen tener herramientas de ciberseguridad de defensa, herramientas utilizables en el ciberespacio que puedan manejar toda esta situación, la capacidad que se puede tener para manejar una situación es tremenda.

Si nos centramos en lo que afecta directamente a España, lo que estamos haciendo está muy en consonancia con lo que se hace en la Unión Europea y en la OTAN. ¿Cómo estamos aplicando estas ideas en este nuevo teatro de operaciones? ¿Guerreamos ya en el ciberespacio? ¿Cómo estamos enfocando este problema? Bien, pues la Estrategia de Seguridad Nacional de 2013 ya recoge esta amenaza y establece líneas de actuación. Después, a partir

de la creación del Consejo Nacional de Ciberdefensa, se aprueba la Estrategia Nacional de Ciberdefensa, que intenta enmarcar y definir cómo se va a manejar la ciberseguridad en España.

Las Fuerzas Armadas son solamente una parte de todo este engranaje de ciberseguridad, que es mucho más complejo. Las Fuerzas Armadas no son ni los primeros protagonistas ni los actores principales, sino que están centradas, dentro de este esquema de la ciberseguridad nacional, en los sistemas militares. Un elemento básico de la ciberseguridad es la seguridad de la información y de los sistemas de información militares. Luego vienen los elementos añadidos posteriormente.

La ciberseguridad es un elemento horizontal donde participan y son afectados los individuos de forma individual. Por eso la autoprotección tiene un valor importantísimo en este ambiente: la seguridad en este teatro del ciberespacio empieza por la seguridad de cada uno y de sus sistemas de información. Está también la seguridad de las empresas y de las infraestructuras críticas, elementos que en España quedan bajo el amparo del Ministerio del Interior. La seguridad de las Fuerzas Armadas es donde nosotros nos centramos. Dentro del proceso de transformación, estamos desarrollando la parte que nos corresponde en la Estrategia de Seguridad en dos aspectos. En primer lugar, con la creación del Mando de Ciberdefensa, cuyo comandante habló aquí esta mañana. Básicamente, este mando está en fase de desarrollo y tiene el cometido de defender permanentemente las redes de información militares; luego detallaré un poco más cómo se desglosa esto. El segundo elemento, tan importante como el primero, es la integración de la ciberdefensa en las operaciones militares. En realidad, la utilización de las Fuerzas Armadas está dividida en dos partes: 24 horas al día en diferentes aspectos de vigilancia de espacios marítimo, aéreos, ciberespacio; y luego en los planes de contingencia que hay que utilizar en caso de que tengan lugar acontecimientos en los que el Gobierno decida utilizar a las Fuerzas Armadas en las opciones militares que se le

presenten. En estos planes de contingencia hemos integrado en todos y cada uno de los casos la ciberdefensa como un elemento básico. Esto se hace mediante la creación de los llamados mandos componentes. Es decir, el mando que tiene carácter conjunto en una determinada operación tiene una serie de mandos componentes y no tiene siempre los mismos, ni todos, sino sólo los necesarios para cada tipo de operación. Puede que sea un mando de componente marítimo, un mando de componente aéreo o terrestre, de operaciones especiales o un mando de componente en ciberdefensa. Éste último ya lo tenemos incrustado en todas las operaciones militares con una primera misión, que es defender la estructura de comunicaciones, los sistemas de información que estén apoyando. Su misión es identificar los ataques a ese sistema y reaccionar contra ellos en caso necesario.

O sea que, desde el punto de vista orgánico, en el proceso de transformación de las Fuerzas Armadas ha habido un impacto en el teatro de operaciones del ciberespacio con la creación de un mando permanente. Además, en cada una de las operaciones concretas existe un mando componente integrado en la operación. Y simultáneamente hay que avanzar en el terreno conceptual y desarrollar doctrina, a la vez que se forma y planea el futuro de este mando.

No es éste el único elemento que afecta al proceso de transformación –y conviene decirlo– pero es un elemento importante y transversal, porque afecta a algo muy importante en la forma de utilización de esas Fuerzas Armadas que queremos crear. Como decía antes, no se trata de un proceso de adaptación a la situación, sino de un proceso de transformación, de un proceso que pretende crear unas Fuerzas Armadas capaces de reaccionar ante los problemas que prevemos que vamos a tener en el futuro. Por eso nos basamos en un concepto simple, en tres niveles de actuación: prevención, decisión y acción. Hay que avanzar en la prevención y la ciberdefensa puede ayudar en este campo de una forma intensa. Hay que avanzar en la decisión, y aquí quizá

sea menos directa la relación entre la ciberdefensa y los procesos de decisión, pero para asegurar una alta velocidad de mando y una alta capacidad de decisión hace falta contar con sistemas de información claros y permanentemente actualizados que sean capaces de integrar no sólo lo que está ocurriendo sino lo que pensamos que va a ocurrir. Estos sistemas están en el ciberespacio y, por lo tanto, la ciberdefensa es básica. Si no conseguimos asegurar la supervivencia de estos sistemas seríamos incapaces de decidir. Porque cuando no tenemos clara la situación nos resulta imposible tomar una decisión. Si en el momento de la prevención la ciberdefensa es un factor vital, en el de la decisión también lo es, como también en el de la acción. La acción puede tomar distintas formas, ser más agresiva o tender hacia el concepto de influencia que he mencionado antes. Para actuar, lo importante en muchas ocasiones no es ganar zonas geográficas, sino ganar el apoyo o no apoyo de determinados colectivos. Ahí también, la ciberdefensa, con su enlace en las capacidades de información, tiene mucho que decir. Así que la ciberdefensa, de una forma horizontal, está totalmente implicada en conseguir ese diseño y esas posibilidades estratégicas de las Fuerzas Armadas en el presente y en un futuro muy cercano.

Los otros elementos para presentar las claves de la transformación global sobre las que estamos empujando son la enseñanza, como elemento primordial; la fuerza conjunta, como elemento básico; la inteligencia –porque, como ocurre con la ciberdefensa y la prevención, la inteligencia es básica en esto–; y las operaciones especiales, como elemento de actuación ágil y decisivo en muchos de los casos en que tengamos que utilizarlos junto con las armas inteligentes. Éstos son los elementos básicos en el proceso de transformación, en este conseguir crear un futuro seguro.

Con todo esto, el Mando de Ciberdefensa desarrolla un plan concreto que está centrado en primer lugar en tres etapas y, luego, en diferentes sectores que deben desarrollarse para ponerse en marcha. Las etapas son la defensa de la que he hablado ante-

riormente; la explotación, que está muy relacionada con la inteligencia y la capacidad de prevención; y la acción, muy relacionada con la utilización de capacidades para repeler ataques o para atacar, si fuera necesario. Así que hay que desarrollar unas capacidades de defensa, que es el elemento básico. En esto no es todo nuevo; se recogen capacidades que las Fuerzas Armadas ya habían desarrollado en seguridad de la información. Esto abarca desde habilitaciones personales de seguridad hasta sistemas encriptados o líneas especializadas para determinados enlaces. Es decir, se trata de sistemas clásicos de seguridad de la información que las Fuerzas Armadas ya utilizaban con normalidad, pero que se integran en la capacidad de ciberdefensa. Tiene que ser un sistema abierto apoyado en sistemas que identifiquen ataques sobre las redes y que de forma automática consigan estar chequeando y analizando la situación y las posibles agresiones o intentos de entrar en una determinada red. Estamos trabajando en el desarrollo de estos sistemas y en mejorar la defensa de nuestras redes de información militares, que, como apuntaba, son vitales para conseguir la capacidad de decisión. Porque esta capacidad se basa en conseguir sistemas de información fiables, de confianza y actualizados con rapidez. Todas éstas son características clásicas de los sistemas de información militares.

Lo siguiente es la explotación. Es decir, conseguir el análisis forense de lo que ocurre: quién, cómo y qué se está intentado hacer. El objetivo es saber de dónde viene ese intento de penetración en nuestras redes. Queremos obtener información. Por ejemplo, si pensamos en Siria y nos detenemos en el problema de la captación de combatientes extranjeros, ¿cómo se articula esto? Pues está todo en la red y hay que tener la capacidad de encontrar esa información. Cualquier cuestión relacionada con el crimen organizado también está prácticamente siempre en la red, igual que muchas cosas militares. Estuve hace poco con el Comandante de Transportes de Estados Unidos y ellos lo tienen todo en la red. Por eso, aunque quizá no nos demos cuenta, en

esta capacidad de explotación se encuentran las vulnerabilidades que tenemos. En la red está todo.

La respuesta tampoco es algo que concierne al futuro, sino que hablamos de hoy. En Ucrania, por ejemplo, están llegando ataques masivos a determinados servidores que apoyan la industria pesada de desarrollo de ese país: reciben 200.000 peticiones de entrada que bloquean determinados servidores y los vuelven inútiles. Esto es algo que ocurre en el presente. Y, por supuesto, la capacidad de avance y desarrollo es tremenda, así que si no contamos con medios de defensa seremos vulnerables a todas estas actividades.

Esto de lo que he hablado sería el aspecto más operacional del Mando de Ciberdefensa, pero hay otros dos elementos fundamentales, cuyo desarrollo también está entre sus cometidos. Uno de ellos es la concienciación; algo que no es sólo necesario en las Fuerzas Armadas, sino que debe hacerse extensible a toda la sociedad, porque estamos en una cibersociedad. Se calcula que dentro de unos años habrá 4.000 millones de personas que usarán las redes sociales y los sistemas de información; es decir, más de la mitad de la población mundial. Es pues básico que esta concienciación en torno a la seguridad en ciberdefensa se implante a nivel individual, que seamos conscientes de que debemos autoprotegernos y que sepamos que el móvil es un elemento de alta vulnerabilidad. Nosotros lo aplicamos a la esfera de las Fuerzas Armadas; por eso sabemos que ciertas informaciones deben transmitirse sólo a través de determinadas redes. Hay que tener disciplina en la utilización de las comunicaciones a nivel individual si queremos mejorar la seguridad de la red general, nacional, de la OTAN o de la Unión Europea. Este proceso de concienciación de todos y cada uno de nosotros en este campo es de gran importancia.

La formación y el adiestramiento en temas relacionados con la ciberdefensa son también elementos claves en la transformación. Hay países que están muy adelantados en estos aspectos,

como, por ejemplo, Israel, que ha introducido asignaturas y elementos relacionados con la ciberdefensa en la formación básica de todos sus ciudadanos; no sólo en la formación militar. Nuestros soldados y marineros tienen que estar formados en este nuevo teatro de operaciones que –como las Fuerzas Aéreas al principio del siglo XX– hoy supone la incorporación de un sistema de influencia y de actuación de carácter horizontal, con una tremenda capacidad de actuación en las cuestiones operativas.

El último elemento es la integración en operaciones, que es algo básico. Por poner un ejemplo, hace poco un cuartel general español ha sido certificado como Cuartel General Conjunto de la OTAN para Operaciones Sencillas; me refiero al Cuartel General de Alta Disponibilidad que tiene el Ejército de Tierra. Uno de los aspectos básicos en esta certificación fue identificar su capacidad para defender las redes desde el punto de vista de ciberdefensa, mediante sistemas Soft y programas; el estar controlando lo que está ocurriendo en cada una de las redes de información y ver exactamente si están recibiendo ataques y quién los acomete y, por supuesto, su control mediante el uso de redes alternativas o la supresión.

Para terminar quiero decir que relacionar el proceso de transformación a la ciberdefensa no crea una relación forzada. El proceso de transformación, como elemento de organización desde el punto vista conceptual de sistemas y materiales de las Fuerzas Armadas, debe hacer frente a los retos del porvenir. La ciberdefensa es un elemento de transformación que ya hoy, y en el futuro, va a tener un peso cada vez más importante. Por eso debemos responsabilizarnos y tomar medidas para actuar desde el punto de vista defensivo, de explotación y de acción.

MIGUEL ÁNGEL AGUILAR
Moderador

Muchas gracias, Almirante. Damos paso al coloquio.

JUAN ANTONIO GÓMEZ BULE
Presidente de S21sec

Siempre es muy grato comprobar que las altas instancias militares tienen un concepto de sistema global a la hora de abordar este entorno de ciberdefensa. Durante los últimos años hemos intentado trasladar que esto no era un mero elemento tecnológico, sino un elemento estructural para el entendimiento de la realidad. La primera parte de su exposición ha dejado claro el posicionamiento de los ejercicios sobre la influencia y contrainfluencia que son necesarias en el tema de la formación. Como bien sabe el Almirante, desde el grupo de trabajo de conciencia de defensa que presido, es un auténtico placer poder compartir el esfuerzo del Ministerio de Defensa. Me gustaría que nos hablara del desarrollo del concepto del sistema. Esta mañana el representante del Mando de Ciberdefensa de la OTAN dejaba entrever que en Ucrania ha quedado reflejado ese ejercicio de contrainfluencia; algo que creo que tendríamos que desarrollar. Por otro lado, también querría que nos hablara del entorno de los planes de captación. Ya hablamos con el Teniente General Alfredo Ramírez sobre la posibilidad de desarrollar una línea de formación en este entorno. ¿El Almirante ha pensado impulsarla también en todos los entornos de formación en el Ministerio?

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

Éste es un tema fundamental en el que no nos podemos dormir en los laureles. Tenemos la sensación de que vamos retrasados. Ya se ha creado –lleva un mes en marcha– un grupo de trabajo dentro del Ministerio de Defensa, con participación de los tres ejércitos, liderado por el Mando de Ciberdefensa. Es un grupo de trabajo que está enfocado a la formación, organización y preparación de los ciberguerreros. Estamos empezando a organizar

todo esto. La OTAN tiene un Centro de Excelencia en Tallin donde están trabajando estos asuntos y nosotros estamos trabajando con ellos. Se trata de equipos capaces de actuar y de contra-actuar. Su objetivo está centrado en las técnicas de manejo de sistemas muy directos de ciberdefensa.

Antes, una avioneta lanzaba octavillas para mandar un mensaje. Ahora, se utilizan sistemas de información; hay técnicas de operaciones de información de guerra psicológica. Todo esto está montado en Internet y en las redes sociales. Así que este sistema de formación tiene que ampliarse hacia los conceptos de influencia y contrainfluencia. Entre las secciones de los Estados Mayores conjuntos había una, la J9, que era la cívico-militar. Ahora ésta es la sección de influencia, donde se intentan sumar todos estos conceptos y donde es necesaria una coordinación tremenda entre inteligencia y ciberdefensa. En todo esto se está avanzando.

La Alianza Atlántica ha desarrollado un concepto llamado «guerra ambigua», algo parecido a la guerra asimétrica, pero más complejo. En la crisis de Ucrania, la OTAN se ha encontrado con un problema cuando un socio cercano como Rusia –con quien se había establecido un consejo OTAN-Rusia– se enfrenta con otro socio cercano, aunque no tanto como Rusia, como lo es Ucrania –también había un consejo OTAN-Ucrania y este país participó en Afganistán–. Así que dos aliados de la OTAN se enfrentan entre sí, pero de una forma ambigua, pues la provocación no llega a rebasar nunca la línea roja que obligaría a la OTAN a participar. Todo esto es nuevo y está muy relacionado con lo que hemos hablado.

Para empezar, estamos identificando el primer paso de defensa y explotación. Se trata de ver cómo estas posibilidades que se presentan en el mundo del ciberespacio pueden ser utilizadas de forma positiva o para asegurar el control negativo de un determinado espacio en el ciberespacio, evitando así ataques, agresiones o manipulaciones. Es un tema complejo que me recuerda

a la estrategia marítima, porque ahí siempre hubo esto del control negativo o positivo del mar, esto del dominio. De forma más sofisticada, estos conceptos parece que se repiten en el ciberespacio. Tenemos que avanzar rápido en estos procesos.

JENS WERNER MÜLLER
Agregado adjunto de Defensa de la Embajada de Alemania

En el ámbito de la ciberdefensa, ¿considera usted que lo que los estadounidenses llaman ataque preventivo es una medida legal? Y una segunda pregunta que tiene que ver con el impulso desde las Fuerzas Armadas españolas para fichar a las mejores cabezas: quisiera saber cómo tratan de conseguir esto.

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

Sobre el asunto del ataque preventivo, el Centro de Excelencia de Tallin de la OTAN ha elaborado un documento de gran interés sobre los aspectos legales de la ciberdefensa, un tema muy importante que yo no he tocado en mi conferencia pero que imagino que se tratará en este seminario. Hay algunos aspectos legales que están realmente matizados, pero hay otras zonas donde no existe todavía regulación sobre lo que podría ser aceptable hacer o no. La legislación internacional existente sobre el derecho a la guerra, o el derecho a una intervención humanitaria, no acaba de contemplar estas nuevas armas, que quedan de alguna manera en una situación de indeterminación. La polémica no es en caso de guerra, sino en caso de paz. Por ejemplo, hace unos meses, cuando se hicieron públicas las escuchas surgió este espacio complicado de actuación. Lo que sí es cierto es que, desde el punto de vista operativo, la utilización de estos sistemas «cíber» en una guerra o acción militar que esté apoyada por una resolución de la ONU estará perfectamente justificada, al mismo

nivel que lo estará la utilización de unas reglas que habrá que especificar en cada momento.

Sobre la segunda pregunta, no tenemos un programa específico para hacernos con grandes cerebros, aunque sería magnífico tenerlo. Ahora mismo, dentro del proceso de formación del Mando de Ciberdefensa, estamos avanzando y gestionando recursos humanos y materiales que sabemos para qué van a ser utilizados. AL contrario que en otros países, no gestionamos recursos humanos y materiales sin saber cuál será el objetivo de su trabajo. Avanzamos pues de forma limitada, seleccionando los recursos humanos dentro de las Fuerzas Armadas y ampliando una formación que, individualmente, soldados, suboficiales u oficiales no han recibido en el ejército, sino que han adquirido por su propia experiencia, por interés o afición. Así que, en principio, seleccionamos a gente dentro de las Fuerzas Armadas.

GEORGINA HIGUERAS
Periodista *freelance*. Excorresponsal de *El País* en Asia

Almirante, ha dicho que todo está en la red y que nos encontramos con un quinto dominio dentro el ejército: el ciberespacio. Como JEMAD, ¿no considera que haría falta entonces una reorganización total, de manera que un ejército sobrevalorado, como es el de Tierra, con un montón de hombres, cediera efectivos a ese quinto dominio? ¿Necesitamos una reforma total de los ejércitos para acoplarnos al mundo futuro?

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

Esta pregunta está relacionada con el proceso de transformación del que he hablado anteriormente. Hay un dato que es importante y que tenemos muy en cuenta: se debe evolucionar, pero no podemos perder las capacidades que tenemos sin haber asegura-

do las capacidades que permitirán ofrecer defensa y seguridad mediante otros sistemas. Este quinto dominio va a requerir esfuerzos y aún estamos empezando a ver qué refuerzos. Posiblemente haya que rediseñar nuevas capacidades. Las prioridades de inteligencia y de armas especiales son importantes. Nos obligan a cambiar no sólo el Ejército de Tierra, sino también la Armada y el Ejército del Aire. Estamos dando prioridad ahora a operaciones especiales, a armas inteligentes, a la capacidad de transporte... Otro elemento fundamental es el concepto de conjunto de inteligencia, reconocimiento y vigilancia, es decir, aquello que es necesario para conseguir que los actores que la necesitan tengan en tiempo real toda la información necesaria en una pantalla. Esto está muy relacionado con la capacidad de tomar decisiones y con la velocidad de mando. Todo esto es la guerra de hoy y exige tratar de identificar los vectores de influencia en una determinada sociedad. Y, como he dicho, todo esto obliga a rediseñar las Fuerzas Armadas. No se trata de reducir –o sí– ni de aumentar –o sí–. Lo que está claro es que es necesario cambiar los conceptos.

El gran reto de las Fuerzas Armadas en general, y de las españolas en particular, no es una cuestión presupuestaria –que es un problema importante– sino una cuestión conceptual: hay que asumir esos nuevos conceptos. Eso es lo que nos va a obligar al rediseño. Lo que tenemos sirve –no es lo ideal pero sirve–, pero tenemos que ajustar la eficiencia de lo que tenemos a los nuevos conceptos.

Actualmente, una unidad de la Guardia Civil está trabajando en Bangui (República Centroafricana). El escenario es un campo de refugiados en el aeropuerto, con unas 50.000 personas en una situación de crisis humanitaria dramática y la posibilidad de que se produzca en cualquier momento una masacre. Las unidades de operaciones especiales tratan de ejercer influencia y se presentan en los barrios sin casco, con el arma y la espalda totalmente protegidas, pero sin hacer alarde de superioridad. En

esas visitas tratan de explicar, de influir, de convencer a la población de que no deben tener miedo, de que no deben actuar contra el vecino. Éste es un ejemplo de la gestión de crisis que estamos viviendo hoy en día. Pero eso no quiere decir que la defensa clásica desaparezca. Eso existe también, aunque las operaciones que adquieren mayor prioridad son las otras dos: la gestión de crisis –como la que he comentado– y la creación de capacidades, o la cooperación, para asegurar la estabilidad en zonas que tienen problemas de gobernabilidad. Esto es un trabajo de prevención en el que las Fuerzas Armadas son sólo un elemento más. Hay que hacer una aproximación global, con participación diplomática y económica. Éste va a ser el enfoque cada vez más recurrente, porque es acorde con la aspiración del mundo occidental de extender el paraguas de seguridad y favorecer el desarrollo individual y colectivo. Y lo cierto es que sin seguridad no hay desarrollo. Para gestionar estos problemas en el futuro, tenemos que formar unas Fuerzas Armadas capaces de trabajar así, de extender el paraguas. La gestión de crisis y la estrategia de seguridad cooperativa son elementos básicos y lo serán también en el futuro.

JUAN CUESTA
Director de *Europa en Suma*

Almirante, esta mañana ha sobrevolado por aquí un interrogante y me gustaría saber cuál es su opinión ¿Hay alguna circunstancia en la que sería de aplicación el artículo 5 del tratado de la OTAN ante un supuesto de ciberataque? Este artículo habla de ataque armado, pero me temo que puede haber ciberataques que pueden ser más nocivos que un ataque armado. ¿Hay alguna circunstancia en la que eso fuera de aplicación legítima? ¿Sería éste el momento de volver a redactar o repensar el tratado, para incluir algo de esto?

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

La situación en la que estamos es la de volver a redactarlo. El concepto de ambigüedad sobre el que he hablado tiene entre sus puntos esta cuestión de si es necesario redefinir el artículo 5. Hay una polémica en la OTAN –que usted ha expresado perfectamente–, y es, efectivamente, hasta qué punto un ataque de ciberdefensa forma o no parte de este artículo 5. La opinión general del Alto Estado Mayor del Ejército es que depende de los efectos. Sé que es una respuesta poco concreta, pero lo cierto es que depende de los efectos. En cualquier caso, lo que se asume es que la OTAN –que tiene su propia organización de ciberdefensa– promueve que todos los países aliados ayuden al país atacado y se están empezando a desarrollar equipos de cibercombatientes que podrían desplegarse virtualmente para apoyar un determinado ciberataque. Estamos haciendo ejercicios en ese sentido, pero todavía no está definido explícitamente en el artículo 5.

El concepto de la ambigüedad también está relacionado con esto. Ucrania no es de la OTAN, así que este artículo no era aplicable, pero, si hubiera ocurrido en Lituania, ¿sería o no aplicable cuando la realidad es que, con medios y canales cibernéticos, se está actuando sobre una parte de la nación para provocar la secesión, para provocar un enfrentamiento? ¿Es o no es esto artículo 5? El tema es complicado, pero yo, personalmente, creo que esto se integrará en el artículo.

PEDRO GONZÁLEZ
Columnista de *ZoomNews*

Supongo que la ciberdefensa hace frente a posibilidades de ataques que vengan del exterior. ¿Se contempla también que pueda haber un ataque que proceda del interior de un país o de una organización de carácter secesionista?

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

En ciberdefensa es donde menos se tiene el concepto de interior o exterior. La idea de frontera desaparece totalmente, pues el ataque puede venir de donde sea y la ciberdefensa debe proteger en cualquier caso. La ubicuidad es una de las características del ciberespacio, como lo es también la inmediatez. En nuestros planeamientos clásicos había un trabajo fundamental, que era la relación espacio-tiempo, pues para desarrollar cualquier operación había que medir el tiempo que tardabas en llegar al objetivo. Pero esa noción desaparece en el ciberespacio, que es un ámbito instantáneo. El ataque puede venir desde un edificio emplazado al lado de nuestra sede en Madrid o desde Pekín. Es lo mismo.

FELIPE SAHAGÚN
Miembro del Consejo Editorial de *El Mundo*

Al escuchar estas intervenciones me da la sensación de que se están mezclando dos conceptos sobre la ciberdefensa que en principio no tendrían por qué estar unidos. Almirante, usted ha hablado de operaciones de influencia y ha mencionado la experiencia en Bangui. Yo recordaba algunas explicaciones de los generales que estuvieron en Bosnia, que hablaban de su trato con la población local. También recordé el trabajo de nuestras tropas en Afganistán, de eso que los americanos bautizaron como «*hearts and minds*» (corazones y mentes) cuando se dieron cuenta de que de poco servía la victoria militar y trataron de invertir en medios de comunicación para ganarse a la opinión pública en esos países. Creo que esto es un elemento clave. Lo que me preocupa es la educación, es decir, cómo se está formando a esas personas que tienen que ocuparse de las nuevas operaciones; aunque no son tan nuevas. Según he entendido, se está formando desde dentro a militares. Pero veo que se necesita una formación técnica en

aspectos puramente informáticos, algo muy difícil que un profesional normal no tiene por qué dominar.

En esta otra operación de influencia y conocimiento de la población local hay algo que va más allá de lo que se considera tradicionalmente militar. Psicólogos, sociólogos e informadores estarían más capacitados para entender cómo se trabaja en esta línea con el manejo de información. ¿No se ha debatido sobre cómo aprovechar mejor las necesidades, sobre cómo hay que trasladarlas a la forma en que hay que organizar la formación de quienes se van a ocupar de todo esto?

Además, estaba pensando que no estamos diciendo nada de los «otros». Me explico. No hablamos sobre cómo está controlando y trabajando el supuesto enemigo. Estos últimos meses lo que ha hecho ISIS con la información en la red es un paso más; nos está sorprendiendo incluso a quienes hemos tenido que seguir lo que ha hecho antes Al Qaeda. Nadie lo ha citado, pero yo estaba pensando hasta qué punto no han aprendido a emplear estos instrumentos las dictaduras mucho más rápido que las democracias. Y en esto incluyo tanto a países grandes como pequeños.

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

Estamos seleccionando a gente dentro de las Fuerzas Armadas, pero el proceso de formación que estamos desarrollando también tiene vínculos con la universidad y con otros especialistas. Creo que tenemos que llegar a establecer equipos multidisciplinares. Ya dije que en las operaciones hay un mando de ciberdefensa y una sección de influencia, y existe también una sección de oficiales de relación de información pública. Esto es lo que se está integrando en una nueva sección de influencia en la que tiene que haber psicólogos, técnicos de ciberdefensa y especialistas en conocimiento cultural de la sociedad donde se está trabajando para intentar apoyar un sistema estable que pueda ayudar

a mejorar las condiciones. Estoy de acuerdo con el enfoque multidisciplinar, que va unido a la necesaria aproximación global a un problema. Es algo complejo y se necesitan especialistas en todas estas ramas.

Estoy totalmente de acuerdo sobre lo que ha apuntado respecto a la capacidad que diferentes actores están demostrando tener en las redes sociales para crear inestabilidad en distintas zonas del mundo. Tienen la capacidad de transmitir información, de captar, de formar, de influir. Lo abordan de una forma total.

ENRIQUE PERIS
Excorresponsal de TVE en Londres

¿Esas unidades que se van a ocupar de nuestra ciberdefensa tendrían alguna relación o vinculación operativa funcional con las unidades policiales o de la Guardia Civil? Pregunto esto porque quizá sería interesante, y útil, recoger la experiencia que tienen estas unidades en el marco cibernético, por su conocimiento técnico. Desde el punto de vista informático, se han venido ocupando con las aplicaciones, las búsquedas o barridos en la red para luchar contra el ciberterrorismo, contra los llamamientos de la yihad o contra la pornografía infantil y otros delitos. ¿Se va a recoger esta experiencia ya adquirida? ¿Se contempla algún tipo de vinculación operativa y funcional?

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

Esto es precisamente el núcleo básico y lo que va a definir el éxito o el fracaso de la estrategia española en ciberseguridad. El mundo de la ciberdefensa es complejo y está repleto de actores, como el Instituto de Tecnología, empresas privadas, las Fuerzas Armadas o el CNI. Hay dos cosas claras en la estrategia española de seguridad. La primera es la definición y valoración de

la amenaza como algo a lo que hay que hacer frente. Y la segunda es la idea de que la estrategia siempre provoca una acción y de que ésta es la que debe provocar esta estrategia. El éxito estará en conseguir o no esta acción.

Hay múltiples actores en España que tienen experiencia y que trabajan en ciberdefensa. El objetivo es coordinar todas estas actividades, de forma que sumen, que la experiencia que tienen las fuerzas de seguridad reviertan en las Fuerzas Armadas, y a la inversa. Es necesario que haya transparencia y comunicación, que se compartan los resultados entre los diferentes elementos. Ésa es clave para que nuestra estrategia tenga éxito. Éste es un tema en el que se está avanzando, en el que se están organizando planes de acción. Es fundamental la colaboración. Es fundamental no duplicar esfuerzos y aprovechar todas las capacidades. Lo de las sinergias es verdad: dos y dos suma cinco en muchos casos.

SULEYMAN ANIL
Miembro del Centro de Ciberdefensa de la OTAN en Mons

Mi oficina prepara los planes de acción y estrategia a los que se ha referido y ahora estamos muy ocupados con la próxima cumbre de septiembre. Quisiera preguntarle al Almirante si lo que ha visto en la OTAN y en el progreso que se está haciendo en ciberdefensa ha sido útil para la evolución de la ciberdefensa en España. ¿Le gustaría que la OTAN manejara la ciberdefensa de una manera distinta a como lo ha venido haciendo, que hiciera algo más o menos en el ámbito de la ciberdefensa?

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ
Jefe del Estado Mayor de la Defensa

En las relaciones con la Alianza Atlántica tratamos de conseguir que ésta se implique cada vez más en las cuestiones de ciberdefensa. Nos gustaría que la OTAN apoyara lo máximo posible a

los 28 países que participamos en la Alianza. Pero existe un problema de fondo que está muy relacionado con la pregunta anterior. Cada uno de los países de la OTAN tiene una estructura y unos problemas parecidos a los que antes identificábamos: no es la parte militar la responsable de la ciberdefensa, sino que es tan sólo una pieza dentro de la ciberdefensa. Así que conseguir esa mayor implicación de la OTAN en el ámbito de la ciberdefensa, desde un punto de vista general, conlleva problemas de coordinación. Desde un punto de vista militar, en España estamos promoviendo una integración de capacidades. Querríamos que la OTAN no sólo asegurase la defensa de sus sistemas y su capacidad de actuar en el ciberespacio, sino que, en caso de que un país recibiera una agresión en el ciberespacio, apoyase a ese país en la defensa de su integridad. El punto débil de esta evolución es que la ciberdefensa, como sistema global de seguridad de cada Estado, está fraccionada: las Fuerzas Armadas y los ministerios de Defensa no son el principal actor o responsable de mantener este ámbito de seguridad. Por eso la acción de la OTAN es limitada. Y, desde un punto de vista contingente, eso es precisamente lo que queremos integrar, o pretendemos integrar, vía el ajuste del artículo 5.

MIGUEL ÁNGEL AGUILAR
Moderador

Muchas gracias, Almirante, por su intervención. Ha sido muy esclarecedora.

6. RIESGOS Y AMENAZAS EN LA RED

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Moderadora
ARANTZA MARTÍN
Responsable de Interior y Defensa
de Onda Cero Radio

Francisco Martínez Vázquez y Arantza Martín

ARANTZA MARTÍN
Moderadora

En esta sesión contamos con la suerte de tener con nosotros a Francisco Martínez, secretario de Estado de Seguridad, o, lo que es lo mismo, el número dos del Ministerio del Interior. Si me permiten, lo de ser número dos debe ser un poco exótico para él, ya que está bastante acostumbrado a ser el número uno: número uno de las oposiciones por las que accedió al Cuerpo de Letrados de las Cortes Generales y Premio Extraordinario Fin de Carrera en Derecho. También es licenciado en Ciencias Económicas y Empresariales y ha sido director de Relaciones Internacionales de la Secretaría General del Congreso. El título de esta sesión es «Riesgos y amenazas en la red». Me llama la atención que esté planteado en negativo conociendo el uso que de la red y las redes hacen las Fuerzas y Cuerpos de Seguridad del Estado; pero imagino que la intervención del secretario de Estado pondrá, además de una voz de alerta, una voz de oportunidad. No dudo de que nos hablará de cibercrimen, de ciberdelincuencia, a lo mejor lateralmente de ciberespionaje y, sobre todo, de ciberterrorismo o, como hemos escuchando aquí, el uso que los terroristas tan bien saben hacer de la red, pues no hay duda de que el ciberyihadismo ha sabido exprimir las posibilidades de Internet para radicalizar

los sentimientos y para captar terroristas. Afortunadamente, las operaciones policiales nos hablan cada día de nuevos éxitos, al igual que nos hablan de coordinación internacional, de desarticulaciones de redes de inteligencia y de la detención de estos individuos. De hecho, esta misma madrugada hemos sabido de otra detención por parte de la Guardia Civil en Ceuta. Se trata de individuos muy peligrosos a quienes se rastrea, se vigila y se identifica a través de la red. Es decir, que algo vamos aprendiendo sobre ellos. También vamos a oír aquí hablar de las redes sociales y de sus riesgos, del peligro que suponen, entiendo que sobre todo, para los grupos más vulnerables, los menores. Puedo suponer que, en su condición de padre de tres hijos, el secretario de Estado también estará preocupado por lo que esto puede suponer. De la misma manera entiendo que favorecerá el buen el buen uso de la red, el uso responsable de la red y de las redes, porque, y esto es lo que yo entiendo que será la parte positiva de esta intervención, un buen uso hace de la red y de las redes sociales un instrumento muy útil, que seguro que el secretario de Estado va a defender. Lo defenderá porque, como responsable de las Fuerzas y Cuerpos de Seguridad del Estado, ha comprobado su eficacia y su eficiencia. Algún grupo de narcotráfico ha caído gracias a alguna campaña en la red y la policía y la Guardia Civil están consiguiendo abrir con sus campañas en la red un canal de comunicación muy importante entre el ciudadano y las fuerzas de seguridad, que además es bidireccional. Han tenido y están teniendo mucho éxito porque la difusión es mucho más amplía, porque la información que se quiere hacer llegar llega a muchos más ciudadanos, pero además a grupos de ciudadanos a los que de otra manera quizá no llegaría; estoy pensando en los jóvenes, por supuesto. Y a todo esto hay que sumarle una colaboración ciudadano que a lo mejor de otro modo no se conseguiría. El perfil de la policía en Twitter, «@policia», es un buen ejemplo de ello. Ese éxito seguro que será comentado por el secretario de Estado hoy, ya que le gusta mucho lucir aquello de que han ganado al FBI en

número de seguidores. En resumen, vamos a oír hablar de riesgos y amenazas en la red, por supuesto, pero también de los puntos negros que deben ser analizados y en los que deben trabajar los responsables de seguridad. Hablaremos de todo ello con el equilibrio que se da entre los peligros y las oportunidades de Internet. Entre otras cosas porque Internet es una realidad y más vale, por lo tanto, que sepamos sacarle partido. Dicho lo cual, lo mejor será cederle la palabra sin más al secretario de Estado, que además, aunque no lo dije al principio, es profesor universitario; así que les anticipo –ya que lo he comprobado siempre en sus comparecencias de prensa– que ésta va a ser una conferencia interesante, amena y con una enorme carga pedagógica.

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Gracias por tus amables y seguro que inmerecidas palabras, Arantza. Es un desafío intervenir en este escenario, y todavía más hacerlo después del Jefe del Estado Mayor de la Defensa; cuando preparaba oposiciones siempre teníamos la duda inquietante de cuándo nos tocaría intervenir, ya que si el que lo hacía antes lo hacía francamente bien, luego, por mucho que fuera un elemento subjetivo, el tribunal estaría condicionado en un sentido un poco negativo. Bien, pues este tribunal de hoy, sin duda exigente y cualificado, espero que sea indulgente y tenga en cuenta que intervengo después del Jefe del Estado Mayor de la Defensa, que además de ser un gran militar es un gran profesor, con unas grandes dotes pedagógicas de las que, desde luego, muchos de los que le hemos escuchado nos hemos aprovechado.

A mí me corresponde hablar como secretario de Estado de Seguridad y, como anticipaba Arantza, sobre los riesgos y las amenazas de la red. Intentaré hacerlo desde una perspectiva amplia, pasando de puntillas por los temas que no son de mi competencia, porque si hay algo que caracteriza este mundo de las

ciberamenazas es que es imposible abordarlo desde la perspectiva individual, única, de uno de los muchos actores implicados en la defensa de la seguridad. Sin ayuda, el Ministerio del Interior no podría hacer frente a todos los desafíos que aparecen en el mundo de las redes sociales y de Internet, de la misma manera que no podría hacerlo solo el Ministerio de Defensa o el Centro Nacional de Inteligencia. Por este motivo ha sido importante que, en el marco de la Estrategia Nacional aprobada por el Gobierno, y como fruto de ella, este seminario haya sido capaz de reunir aquí a los distintos actores implicados en esto de la ciberseguridad. Yo me centraré pues en las cuestiones que tienen estrictamente que ver con el ámbito de la seguridad. Con mucho acierto, el Ministro de Interior defendía el concepto de seguridad como algo poliédrico, ya que existen muchas cosas que no son sólo las relacionadas con la delincuencia o el terrorismo, sino que es algo mucho más complejo y más amplio. Eso es justamente lo que está en juego en el mundo de la ciberseguridad. En un mundo sumido en cambios profundos, lo que voy a contar en esta intervención es cómo han variado las amenazas de esa ciberrealidad que es diversa, cambiante y plural. También creo que hay algo que Arantza ha apuntado con mucho acierto, que es que ante esto no hay que tener una visión pesimista, negativa ni mucho menos derrotista. Al revés, anticipando una de mis tesis fundamentales, creo que Internet, las redes sociales y el mundo cibernético han generado extraordinarias oportunidades de relación entre los humanos. Lo han hecho en el ámbito personal, en las relaciones sociales, familiares y profesionales, en el mundo de la empresa. Y eso es una grandísima ventaja que, por cierto, también tiene su traducción en el ámbito del servicio público, pues las redes sociales, Internet, tienen aplicaciones de servicio público y, desde luego, en el terreno de la seguridad y de los servicios que los ciudadanos valoran y necesitan. Eso no quita para que haya un aspecto negativo en este mundo, un aspecto que no ensombrece las ventajas pero que debemos de tener en cuen-

ta y ante el que debemos prevenir, más que reaccionar; aunque, cuando sea necesario, también reaccionar. Por eso les quiero anticipar que mi visión –y espero que así se traduzca, aunque me tenga que centrar en lo negativo– no es ni mucho menos una visión crítica u oscura, sino todo lo contrario: creo que las oportunidades que se las aplicaciones tecnológicas ha prestado a la seguridad han sido mayores que los aspectos oscuros.

Los riesgos a los que nos enfrentamos afectan a la seguridad nacional, aunque muchos de ellos son extrapolables, por la carencia de dimensión territorial que tiene el mundo cibernético, a cualquier parte del mundo, sobre todo porque el escenario en el que se producen no conoce fronteras. Esto también será un primer desafío desde el punto de vista de la concepción de la seguridad, que siempre ha estado territorializada. Ahora estamos haciendo frente a un fenómeno que exige la cooperación y el diálogo internacional, porque un solo país no podría nunca dar respuesta a las distintas amenazas que conviven en Internet y en las redes sociales, que son, por su propia definición, globales y carecen de las dimensiones físicas de las amenazas tradicionales.

Se estima que el impacto económico de las ciberamenazas por un incidente grave, medido por las pérdidas anuales, pueden suponer una media de 497.000 euros para las grandes empresas y una media de 38.000 euros para las PYMES. No obstante, se estima que un ataque dirigido puede llegar a costar más de 1,7 millones de euros en pérdidas financieras directas y en costes adicionales.

En términos más generales o globales, si se me permite, las ciberamenazas podrían tener un impacto anual superior a los 300.000 millones de euros en la economía mundial, estimándose en 1.080 las víctimas de estas amenazas que se producen cada minuto en algún lugar del mundo. Según estudios recientes, el volumen que mueve la ciberdelincuencia es ya superior al que genera otra de las modalidades tradicionales de las grandes lacras de nuestro tiempo: el narcotráfico. En el mundo de la ciber-

delincuencia ya estamos, por tanto, superando ese triste y lamentable récord que es el de las cifras del coste del volumen económico que mueve el narcotráfico.

Según un trabajo realizado por los investigadores de ciberseguridad Bob Radvanovsky y Jake Brodsky, se calcula que entre un cuarto y un tercio de los dispositivos móviles existentes contienen vulnerabilidades y que la mayoría están configurados incorrectamente. Este aspecto es clave a la hora de entender el nivel de riesgo al que nos enfrentamos. Por poner un ejemplo, si la mayoría de los dispositivos móviles están mal configurados y si entre un cuarto y un tercio son vulnerables, nos podemos hacer una idea del riesgo al que están expuestas las infraestructuras críticas, que, además de tener dependencias e interdependencias, a día de hoy tienen muchísimas interdependencias de dispositivos móviles, que son ampliamente utilizados en todos los entornos por los sectores estratégicos. Ya en 2009, un alto responsable de Intel anticipaba que para el año 2020 –que está como quien dice a la vuelta de la esquina– la conectividad entre los distintos elementos que forman parte del sistema de infraestructuras sería diez veces superior y que las denominadas redes inteligentes, o «*smart grids*», tendrían un tráfico de Internet que multiplicaría por cien el actual.

Como es lógico, esta interdependencia tecnológica se traduce en enormes posibilidades en capacidades de crecimiento y capacidades de aprovechamiento en todos los sectores, pero no sólo son nuevas las oportunidades sino también los riesgos; nuevas amenazas como los ciberataques de los que se valen los delincuentes, los terroristas y los espías. Con el objetivo de centralizar todas las actividades relacionadas con estas nuevas amenazas, que denominamos cibercriminalidad, en el Ministerio del Interior hemos puesto en marcha la Oficina de Coordinación Cibernética, que está enmarcada en el seno del Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC), que a su vez tiene por objeto configurarse como el órgano de la Secreta-

ría de Estado de Seguridad encargado del enlace entre las Fuerzas y Cuerpos de Seguridad del Estado y el Centro de Respuesta a Incidentes de Seguridad Cibernética, el CERT de Seguridad e Industria, emplazado en León, en la sede del INTECO, y que engloba y consigue importantes sinergias entre las capacidades y competencia de los ministerios de Industria, Energía y Turismo, por un lado, y el Ministerio del Interior por otro. Quisiera apuntar aquí que, además, el CERT de Seguridad e Industria ofrece un servicio gratuito a los operadores de infraestructuras críticas de los sectores estratégicos en materia de ciberprotección. Y digo gratuito porque, como es lógico, también hay quienes hacen de la ciberseguridad un servicio retribuido. Pero desde el punto de vista del servicio público lógicamente el Ministerio del Interior, aprovechando las capacidades comunes con el Ministerio de Industria, está prestando ese servicio de respuesta a incidentes de seguridad cibernética a los operadores de infraestructuras críticas. Perdón por la cuña publicitaria. Con ello quiero destacar el magnífico papel que está realizando el CERT de Seguridad e Industria, que, además, ha tenido ocasión de poner en práctica en fechas recientes, con motivo de la proclamación del Rey Felipe VI, donde, por primera vez, dentro del dispositivo de seguridad, además de los tradicionales elementos de seguridad de estas características y de esta envergadura, ha habido también un dispositivo de ciberseguridad encargado de hacer frente a las nuevas amenazas en el ámbito cibernético. Con esto no quiero decir que nos hayamos puesto a vigilar las redes sociales para ver si alguien decía alguna cosa inconveniente. Como es lógico, estamos hablando de algo muchísimo más serio. Estamos hablando de las amenazas que pudieran llegar para un acontecimiento de esta naturaleza histórica a través del ciberespacio bajo la forma de intentos de sabotaje o de ataque a las infraestructuras críticas que necesariamente debían prestar servicio el día de la proclamación. Como les digo, por primera vez un dispositivo de seguridad ha tenido una derivada específica en el ámbito de la ciber-

seguridad en España, y ello ha supuesto la coordinación, desde este CERT de Seguridad e Industria, de las Fuerzas y Cuerpos de Seguridad del Estado y, como es lógico, los proveedores de telefonía e Internet. Todos ellos coordinados por la Oficina de Coordinación Cibernética. Durante la duración del operativo se analizaron infinidad de contenidos de la red que han contribuido a incrementar la seguridad de todos.

Entre las muchas cuestiones relevantes en las que el Gobierno de España está trabajando y en las que está específicamente implicado el ámbito de la ciberseguridad, me voy a referir a algunas de manera puntual; como les decía antes, voy a pasar por alto las que tienen que ver con otros responsables y, por tanto, no son de mi estricto ámbito de competencia, como son el ciberespionaje y la ciberdefensa. Además, estoy seguro de que, del ámbito de la ciberdefensa, les ha dado cumplida cuenta el Jefe del Estado Mayor de la Defensa y, sobre el ciberespionaje, lo hará mañana el Director del Centro Nacional de Inteligencia, el General Sanz Roldán.

En lo que se refiere a la ciberdelincuencia, decir que está evolucionando rápidamente en los terminales de punto de venta y en los cajeros automáticos y que es una de las amenazas a las que nos hemos visto obligados a responder de manera muy rápida en los últimos meses. Esta nueva ciberdelincuencia se caracterizar por el empleo de herramientas de generación de ataques, conocidas por los ciberdelincuentes como «*exploits-kits*». A finales del año pasado se logró detener al autor de una de las herramientas más utilizadas, el Blackhole, cuyo *kit* se aprovechaba de las vulnerabilidades de los navegadores web y de otros programas populares, como Java, Adobe Reader y Flash Player, para descargar sigilosamente *malware*, como troyanos bancarios y *ransomware*, en los ordenadores de los usuarios. Saben ustedes que un *ransomware* es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de qui-

tar esta restricción. Algunos tipos de *ransomware* encriptan los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. En la primera rueda de prensa que di como secretario de Estado de Seguridad, yo tuve ocasión de estar junto al director de Europol, Rob Wainwright, precisamente porque la Policía Nacional desmanteló –en una operación coordinada en el contexto de Europol– nada menos que la red que llevaba el llamado «Virus de la Policía», ejemplo de *ransomware* en el que quienes accedían a determinadas páginas veían como su ordenador quedaba secuestrado y se pedía a cambio un rescate. Rescate que no era una cantidad muy elevada pero que sí lo era en la capacidad de multiplicación del efecto económico. Éste es un ejemplo más de una operación enormemente compleja, porque, desde luego, si pretendemos abordar o poner freno a la ciberdelincuencia sencillamente desde las capacidades de actuación de un Estado, estaríamos enormemente limitados. Por eso fue precisa la cooperación por parte de Europol y, en este caso, después de varios meses de una investigación dura en la que había que tener en cuenta la complejidad tecnológica y de los distintos ordenamientos jurídicos, se pudo desmantelar esa red, que es un ejemplo entre tantos otros de aplicación de virus con finalidad delictiva. Se trata de unos virus que se hicieron populares en Rusia y cuyo uso creció internacionalmente desde mediados del 2013; de hecho, la empresa MacAfee señaló que sólo en el primer trimestre del 2013 había detectado más de 250.000 tipos de *ransomwares*.

Ejemplos de ciberdelitos podíamos poner muchos más. Otra modalidad son los grupos de hacktivistas. Movidos por una determinada ideología –lo cual es absolutamente legítimo–, en un determinado momento estos hacktivistas traspasan el ámbito de la libertad de expresión –ampliamente reconocida en nuestro ordenamiento jurídico, y también en el mundo cibernético– para socavar el prestigio y la credibilidad de organizaciones privadas, de personas y de instituciones públicas. En la actualidad, estos

grupos se están regionalizando. Un ejemplo reciente de ello son acciones como las protagonizadas en 2013 por Anonymous Ukrania, en contra de la incorporación de Ucrania a la OTAN y a la Unión Europea. Otro ejemplo sería el del Ejército Electrónico Sirio.

Me referiré ahora a otra amenaza particularmente preocupante, que es una derivada malvada de un fenómeno conocido, como es el terrorismo. Estoy hablando del ciberterrorismo. En el año 2013, 21 personas fueron arrestadas dentro de la denominada operación Araña de la Guardia Civil por usar las redes sociales para enaltecer el terrorismo de ETA, así como para humillar a sus víctimas. Esto no es nada nuevo. Al revés, es perfectamente conocido e incluso está recogido en nuestro Código Penal. Pero ahora se detecta, persigue y castiga cuando el medio de difusión no son los medios tradicionales, sino las redes sociales. Por poner un ejemplo, hace menos de un mes la Audiencia Nacional ha condenado a ocho años de cárcel a Mudhar Hussein Al Malaki, conocido popularmente como el bibliotecario de Al Qaeda, por practicar la yihad –aunque yo prefiero decir la yihad malentendida– difundiendo material de exaltación del terrorismo yihadista y manuales para la formación y el adiestramiento terrorista. Le fueron intervenidos de su ordenador 214.000 archivos de temática yihadista sobre métodos para ocultar cargas explosivas en mercados, autobuses o restaurantes y manuales de fabricación de minas, bombas, granadas explosivas y venenos. Además, se encontraron treinta imágenes de cuerpos destrozados de víctimas de los atentados del 11M en las que aparece insertado el logo de Al Qaeda.

Hace ya mucho tiempo que las organizaciones terroristas internacionales yihadistas comenzaron a utilizar de forma masiva Internet, especialmente los foros yihadistas y páginas web que se utilizan con fines de comunicación, proselitismo, propaganda y medio de reclutamiento. De hecho, las últimas desactivaciones de células yihadistas en España nos permite concluir que el mal

uso de las redes sociales ha sido fundamental en su forma de operar. Así ha ocurrido recientemente con detenidos en la operación Azteca, en la que el principal implicado utilizaba Internet para captar y reclutar a yihadistas que ahora forman parte de Jabhat al Nusra y el Estado Islámico de Irak y el Levante, ambas integradas en la órbita de Al Qaeda. Uno de los detenidos era el administrador de un total de veinticinco blogs, así como de trece perfiles en Facebook, dieciocho cuentas de correo electrónico y ocho perfiles de Skype. A través de uno de sus blogs publicaba las medidas de seguridad que debían tomarse para no ser detectados por los servicios de seguridad de los diferentes países; entre ellas señalaba que debían conectarse a Internet en redes WIFI de plazas y parkings públicos sin código secreto y no hacerlo más de dos veces en el mismo lugar.

Sin duda, el mayor riesgo que corremos en el ámbito de las amenazas del ciberespacio es un posible ataque a nuestros servicios esenciales y, precisamente por eso, la amenaza del ciberterrorismo exige prestar especial atención. Hoy mismo se ha producido la detención por la Guardia Civil de otro ciberyihadista, que tenía como actividad habitual el proselitismo, la propagación de ideas radicales, la exaltación y el reclutamiento, en lo que yo considero una mala concepción de la yihad y el Islam. Son muchísimos los ejemplos. Hay otras muchas operaciones que podría citar, pero lo que todas ponen de manifiesto es que hay un uso perverso y delictivo, asociado a finalidades terroristas, de las tecnologías de la información. Preocupa especialmente que estos ataques se puedan producir sobre aquellas infraestructuras que son sustento de nuestros servicios esenciales, es decir, sobre las Infraestructuras críticas. Aunque el tanto por cierto de los ataques cibernéticos es menor del 1%, las consecuencias potenciales de una caída de servicios superan con creces la más negativa de nuestras expectativas. Les doy algunas cifras. En lo que va del año 2014, el CERT de Seguridad e Industria ha localizado y desactivado 24 ataques contra nuestras infra-

estructuras críticas. Entre el conjunto de incidentes que cada día son revisados, 24 es un número muy reducido, aunque hay que resaltar que estamos hablando de aquellas infraestructuras que son el soporte para los servicios esenciales de los que necesariamente disponemos, y debemos disponer, cada día, desde el abastecimiento de agua al sistema eléctrico, etcétera. Quiero con ello decir que debemos estar siempre alerta frente a estos desafíos y que debemos fomentar una cultura de colaboración entre el sector público y el sector privado, pues la mayor parte de estas infraestructuras son operadas por empresas privadas. De ahí que sea tan importante esa sinergia público-privada, pues sin ella sería imposible garantizar la seguridad de ciudadanos y empresas y, en definitiva, de los receptores de esos servicios esenciales.

Quiero referirme también a la sofisticación cada vez mayor de los ataques que llegan a través de Internet y de las redes sociales. Constatamos cada día cómo se van sofisticando las formas y modalidades de amenazas. Por ejemplo está la infección de páginas web de empresas de un determinado sector a través de una técnica denominada Watering-Hole, que consiste en identificar los hábitos de navegación de un empleado de la empresa e infectar con un código dañino las páginas que suele consultar; de esta manera, el empleado quedará infectado al entrar en esa página y se producirá un contagio en cadena dentro del sistema de protección de la empresa.

También está la técnica de la descentralización, que consiste en la infección de empresas subsidiarias, o subcontratistas, como paso previo para acceder al objetivo principal. También resulta bastante común en la actualidad la técnica de denegación de servicio como paso previo o técnica de disuasión mientras se realizan otros ataques.

Pero lo que resulta aún más interesante es cómo las herramientas virtuales con las que convivimos a diario son objeto de los mayores ataques. Por ejemplo, durante el pasado año 2013 las muestras de código dañino detectadas para las distintas pla-

taformas móviles han crecido exponencialmente. Este código se difunde normalmente mediante aplicaciones descargadas de las tiendas oficiales de los principales proveedores de telefonía móvil, como Google o Apple, que aprovechan la ignorancia de muchos usuarios a la hora de autorizar cualquier permiso solicitado por las mismas.

No olvidemos que la permanente conexión a Internet de estos dispositivos hace más sencillo el acceso al terminal, lugar donde albergamos fotos personales y videos familiares, así como datos e información del trabajo que intercambiamos en sistemas de mensajería instantánea como Whatsapp o a través de las redes sociales, como Facebook o Twitter.

Permítanme que dedique un apartado especial a uno de los grupos más vulnerables a los delitos en el ciberespacio, como son los menores. En los últimos meses se ha detectado un notable aumento del binomio *sexting*-whatsapp entre menores de edad. Algunos adolescentes parecen dar menos importancia que los adultos a exhibir su cuerpo desnudo, grabándose o haciéndose fotos con la cámara de su móvil que luego pueden subir inmediatamente a las redes sociales. Es decir, se puede hablar de que se detecta una cierta falta de conciencia sobre los riesgos de una excesiva exposición de la intimidad en las redes sociales. Esas fotos y videos suelen ser compartidos por su autor, en un primer momento, con personas cercanas, como novios, parejas o amigos de confianza. Pero, posteriormente, el efecto de difusión se produce en progresión geométrica, de manera que alcanzan un número muy alto de visionados. Precisamente, ese efecto viral les lleva a pensar que no existe una conducta delictiva en compartir imágenes de dicho tipo de contenido de menores de edad, como son sus compañeros de clase o de colegio. Pero los daños psicológicos para quien aparece en las imágenes suelen ser gravísimos y aumentan exponencialmente cuanta más gente tiene acceso a las mismas. Además, da lugar a otros tipos delictivos como pueden ser el *grooming*, *bullying* o *sexting*. A nivel

operativo, sólo en lo que llevamos de año, hay más de veinte detenidos en España por este tipo de delitos. Por ello creemos que es necesario impulsar –siempre con la colaboración del sector y, por supuesto, teniendo en cuenta las opiniones de los propios menores, por lo que nunca sería de manera unilateral o bajo imposición– una educación sobre los hábitos saludables en Internet, como la protección de la intimidad y de la identidad digital. Esto tiene una doble vertiente. Primero para evitar que los menores se graben en tales actitudes y difundan esas grabaciones, explicándoles las consecuencias que esto les puede ocasionar en el futuro. Y, en segundo lugar, enseñándoles que la difusión de esos contenidos constituye un delito grave del que, si tienen más de catorce años, van a ser responsables. Sobre este asunto les daré algún dato que es revelador. Según un estudio realizado por una universidad norteamericana, el 20% de las primeras entrevistas de trabajo son un fracaso por la información que el propio entrevistado ha hecho pública de sí mismo en redes sociales. En otras palabras, los primeros demandantes de puestos de trabajo no acceden a él como consecuencia de la información de sí mismos que ellos mismos han publicado a través de las redes sociales.

Sólo en el año 2013 se registraron más de 50.400 delitos cometidos a través de las nuevas tecnologías: más de 11.000 delitos de odio; 8.344 amenazas; 1.935 vejaciones leves; 719 coacciones; y 184 tratos degradantes. Así pues, las herramientas web, y en particular las redes sociales, se están utilizando también para difundir comentarios, mensajes o información que pueden llegar a ser calificados como delictivos, o al menos como infracciones administrativas. El ámbito de estos delitos de odio recoge desde los comentarios de mal gusto y las groserías –que no entrarían en el terreno de lo delictivo– hasta las calumnias, las injurias y las amenazas. No son delitos nuevos, sino que son sobradamente conocidos y están en el Código Penal desde hace muchísimos años. Lo que ha variado es el medio a través del cual se cometen, como también ha variado el potencial de dañar,

dado que se generan a través de medios que tienen una extraordinaria capacidad de publicidad.

El perfil del que comete delitos de odio es el de un líder con afán de protagonismo que arrastra a sus seguidores. Es lo que en el argot policial se llama «*troll*». Suele operar en torno a un blog y se sirve de un perfil de Facebook o de Twitter para difundir comentarios ofensivos –en algunos casos extraordinariamente crueles– hacia personas concretas; lo vimos con el accidente que sufrió la delegada del Gobierno en Madrid el verano pasado y lo vimos también con motivo del asesinato de la presidenta de la Diputación de León. En otros casos se trata de la descalificación de grupos religiosos, despertando el odio e incitando a la discriminación; hemos tenido ocasión de ver un ejemplo de esto con motivo del partido de baloncesto Madrid-Maccabi de Tel Aviv, en el que se generaron mensajes de contenido antisemita.

En algunos casos también se usan estos canales para convocar seguidores hacia la protesta violenta, como fue el caso de los altercados de Gamonal o de Can Vies hace unos días.

En definitiva, si una persona comete un delito, las consecuencias son las mismas independientemente de que lo haga en el mundo real o en el mundo virtual. Pero es cierto que en el mundo virtual, a través de una herramienta como las redes sociales, aparece un especial componente de «publicidad» que agrava el daño que se produce a través de estas conductas que ya están recogidas y tipificadas en el Código Penal. Lo que está claro, como decía al inicio de mi intervención, es que Internet no puede ser un escenario ajeno a las leyes. Tiene muchas cosas buenas, pero también otras en las que lamentablemente lo que se desvelan son conductas delictivas. Aquellos delitos que se produzcan en un entorno virtual deben recibir la sanción que establece el ordenamiento jurídico y, tal vez, haya que plantearse si, por la especial capacidad de difusión del medio virtual, esa sanción deba verse, en determinados casos, agravada.

Afortunadamente, la red también ha permitido una gran corriente de manifestaciones reivindicativas, políticas o de acción social que merecen todo el respeto y que, desde luego, son canales de expresión y participación. Gracias a las redes sociales se ha despertado un fuerte sentimiento de participación y solidaridad ciudadana. Y, ante ello, las administraciones y los gobiernos de varios países hemos empezado a abrir canales de interacción con los ciudadanos, pues somos conscientes de las enormes posibilidades que ofrecen. La demanda de un Gobierno abierto y de mayor transparencia en la gestión pública ha dado lugar a una nueva forma de hacer política, más cercana a las personas.

También lo ha hecho en el ámbito de la seguridad y de las competencias del Ministerio del Interior, que ya está sumergido de lleno en una política activa y dinámica de interacción con el ciudadano. Un ejemplo es el perfil del Twitter «Mi casa a salvo», que ha lanzando diversas campañas de seguridad para proteger nuestros domicilios frente a una modalidad delictiva que es especialmente preocupante por la alarma social que genera, como son los robos con fuerza en vivienda. Hoy cuenta con más de 2.500 seguidores y ha llegado a ser *trending topic*. Por supuesto, también está el caso del twitter del Cuerpo Nacional de Policía, que es la institución española líder en número de usuarios de sus plataformas en las redes sociales (Twitter, Facebook, Tuenti, YouTube, Flickr y Google+), lo que nos ha permitido ser masivamente útiles para la seguridad de los ciudadanos. Como digo, se ha creado un canal de concienciación y prevención, de lanzamiento de campañas y de potenciación de las actividades de participación ciudadana gracias al que se han conseguido hitos históricos, tanto en la lucha contra el narcotráfico como en la búsqueda de fugitivos peligrosos. De hecho, como consecuencia de ello se han producido arrestos este año. En Tuenti, Policía Nacional y Guardia Civil han puesto en marcha conjuntamente el Plan Contigo –actualmente con más de 75.000 usuarios–, concebido como una extensión en Internet del Plan Director que am-

bos cuerpos realizan en los centros escolares españoles, para tratar de concienciar, informar y ayudar a los más jóvenes. Asimismo, el twitter de la policía sirvió para canalizar la información de servicio público y la petición de donación de sangre en el accidente ferroviario de Santiago de Compostela, o para la localización de varias nuevas víctimas de un abusador sexual, por poner sólo unos ejemplos.

Y gracias a la llamada «tuit-redada» contra el narcotráfico en España, lanzada en enero de 2012, se han recibido más de 14.000 correos electrónicos y se han detenido a más de 420 delincuentes relacionados con el narcotráfico, desmantelando decenas de puntos de venta e incautándose cientos de kilos de estupefacientes.

Voy a ir terminando. He tratado de hacer un recorrido por las amenazas, pero también por las aplicaciones de servicio público, por el aspecto más positivo del mundo de las redes sociales y de Internet, que sin duda también lo tienen. Para hacer frente al desafío de la ciberseguridad, lo primero que se precisa es una adecuada coordinación entre los agentes que tienen competencias y conocimientos en este ámbito. Por supuesto, tampoco hay que descuidar en ningún momento la colaboración internacional. Hay que promover los esfuerzos tendentes a conseguir un ciberespacio internacional donde estén alineadas las iniciativas de todos los países que persiguen el necesario e imprescindible marco de libertad que debe caracterizar el empleo de las redes sociales y de Internet, haciéndolo también un entorno seguro y fiable. Hay que trabajar duro para proteger a las personas que acceden a las redes digitales, y sobre todo a los menores, que conviven y evolucionan a la vez que las propias redes digitales. No hay ninguna sociedad que esté libre de elementos negativos, pero hemos de afrontar estos riesgos y amenazas con proactividad y diligencia. Para ello, necesitamos la colaboración activa de todos los agentes involucrados –instituciones, empresas, educadores, padres y medios de comunicación– para construir, como preconizan las estrategias nacionales de seguridad y de ciberseguridad, una cul-

tura de la ciberseguridad, una cultura de consumo sano y responsable de la red en un necesario marco de libertad en el que se proteja la intimidad de todos los usuarios, y muy en particular de los más vulnerables, frente a los riesgos y amenazas de la red.

ARANTZA MARTÍN
Moderadora

Efectivamente, ha sido un magnífico recorrido por las amenazas de Internet y un ligero recorrido por las posibilidades que nos brinda la red. A continuación vamos a abrir un turno de preguntas.

ANTONIO REGALADO
Colaborador de *ABC*

Sin cuestionar lógicamente la labor de la policía, me gustaría que me comentara por qué salen inmediatamente a la calle aquéllos a los que ustedes detienen; me refiero a mafiosos y, sobre todo, a gente acusada de delitos pornografía infantil. Por ejemplo, usted ha hablado de ese detenido de los cajeros. ¿Sabe usted cuál es su situación? El problema que tenemos es que nunca vemos a los detenidos en la cárcel. Sé que no es un problema de Interior, si no que depende de Justicia, pero quisiera saber qué es lo que está pasando.

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

En realidad esta pregunta se podría aplicar a muchos ámbitos de la delincuencia y lo cierto es que yo me enfrento a este tipo de preguntas muy a menudo. No sólo cuando hablo de ciberdelincuencia, sino también cuando lo hago sobre robos en el campo, por ejemplo. Fíjese que no tienen nada que ver, pues he tratado de poner un ejemplo que contraste. Me reúno con representantes

del sector agrario que me dicen que, aunque están encantados con la labor de la Guardia Civil, el problema es que cuando los delincuentes son detenidos entran por una puerta y salen por otra. En efecto, es un problema de Justicia. Pero con esto no pretendo echar balones fuera. Uno de los compromisos del Ministerio de Justicia, y en este caso con una implicación decidida del Ministerio del Interior, fue precisamente endurecer el Código Penal frente a determinadas conductas especialmente rechazables –entre ellas los delitos de carácter sexual y la pornografía infantil– y poner freno al fenómeno de la multirreincidencia, es decir, que no pudiese tener el mismo reproche penal cometer un delito que cometer cien. Eso se ha traducido en una iniciativa legislativa, el nuevo proyecto de Código Penal, que se está tramitando en el Congreso de los Diputados y que –aunque probablemente sufrirá cambios en el proceso parlamentario, como consecuencia de la incorporación de enmiendas– recoge esa filosofía de una reacción más contundente frente a la multirreincidencia delictiva, además de en determinados tipos de delitos, como los patrimoniales, que preocupan especialmente a la gente. Es algo que preocupa y sorprende a la gente, que no puede entender cómo está pasando eso. Creo que en política cualquier cosa que no se pueda explicar a los ciudadanos es un semillero de problemas. Y es muy difícil explicar que un delincuente multirreincidente no tenga ningún reproche penal por el hecho de serlo. Creo que, ante eso, se ha dado una respuesta endureciendo las penas contra los delitos contra la libertad sexual y la pornografía infantil. Probablemente nuestro problema sea más de ordenamiento jurídico que de aplicación de la ley; desde luego, no quiero culpar en absoluto a los jueces. Es decir, es un defecto de la ley más que de los aplicadores de la ley. Los fiscales y los jueces tienen que ceñirse al marco jurídico penal que tienen. Por eso creo que era necesario dar ese paso y que nuestro ordenamiento jurídico se verá enriquecido en respuestas de un mayor reproche penal a ese tipo de conductas.

CARLOS MIRANDA
Embajador. Exrepresentante Permanente de España
en el Consejo de la OTAN

Me gustaría que comentara un tema que sé que es delicado, a veces vidrioso, y del que también nos podría hablar Félix Sanz Roldán en su intervención de mañana. Me refiero al respeto a la intimidad. Me da la impresión de que el Estado, con sus distintos elementos, sea un ministerio u otro, forzosamente tiene que vigilar. Y en su vigilancia debe entrar en zonas grises muy complicadas. Quería saber cómo se maneja eso y las garantías que existen para los ciudadanos. Ya sabemos que el ciudadano que cumple la ley no tiene nada que temer, pero el hecho real es que luego, cuando leemos los periódicos, nos encontramos con violaciones de la intimidad; no digo que sean concretamente del Ministerio del Interior, pero sí son situaciones que se dan, aquí y en otros países. ¿Cómo gestionan esa difícil situación?

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Creo, embajador, que efectivamente ha tocado uno de los aspectos que más compleja hacen la actuación policial en este medio. Además, no es ninguna novedad. Volvemos a encontrarnos con una de las grandes dualidades, o dicotomías, de la investigación policial, en definitiva, de la intervención pública en defensa de la seguridad, de todos los tiempos. Me refiero a conjugar esa defensa de la seguridad con un adecuado respeto a la libertad. En este caso, y de una manera muy específica, con la libertad de expresión. Como he dicho, el mundo virtual, las redes sociales o Internet, no tendrían sentido si no se desarrollasen en un clima de amplísima libertad. Creo que todos somos conscientes de ello. De la misma forma, en el mundo de la comunicación no virtual, afortunadamente y con grandes esfuerzos de muchas ge-

neraciones, se han conquistado amplias cuotas de libertad de expresión que deben ser preservadas. Pienso que nuestro ordenamiento ha sido capaz de encontrar los equilibrios para garantizarlas, pues existe una intervención restrictiva de todas las potestades públicas, que, por ejemplo, necesitan en determinados momentos de intervenciones judiciales que dejen claros cuáles son los ámbitos de actuación policial. Todo eso ya se ha ido forjando en el ámbito de las comunicaciones convencionales. Existe mucha jurisprudencia y existen límites. Desde el punto de vista tecnológico, existen límites, por ejemplo, a las intervenciones de comunicaciones que puede realizar SITEL, que tienen que estar presididas por un mandato judicial y están limitadas incluso desde el punto de vista técnico. Todo eso ahora hay que aplicarlo al ámbito del ciberespacio, donde no hay tanta experiencia, jurisprudencia ni casuística. Creo que, afortunadamente, lo que sí existe es una plena conciencia por parte de quienes tienen responsabilidades públicas en el ámbito de la seguridad. Por supuesto, ése es el caso de quienes ejercen funciones de seguridad, como los miembros de las fuerzas de seguridad del Estado, y estoy seguro de que ocurre lo mismo en otras administraciones. Debemos ser absolutamente escrupulosos en el respeto a las libertades y eso es algo que está asentado en nuestra conciencia, en nuestra cultura política. Yo lo veo todos los días cuando hablamos en términos más prácticos sobre protección frente a ciberamenazas. Desde luego, lo que no podemos hacer es convertirnos en un Estado policial de patrullaje de la red para luchar contra la ciberdelincuencia. Eso sería malísimo y nadie lo pretende. Quisiera mencionar aquí que se generó un cierto efecto de alarma social con motivo de los comentarios en redes sociales tras el asesinato de la presidenta de la Diputación de León, cuando se empezó a difundir la idea de que el Ministerio del Interior estaba patrullando las redes. No, eso no es lo que hace el Ministerio del Interior. Las redes, por su propia definición, tienen que desarrollarse en un clima de amplia libertad, aunque es ver-

dad que la investigación tiene que tener medios para poder llegar a la información, ya que de otra manera no podríamos llegar a detectar aquellas conductas que ya no están amparadas por la libertad de expresión, sino que entran en el terreno delictivo. Creo que, en eso, un buen ejemplo lo tenemos en la operación Araña de la Guardia Civil, donde por primera vez los detenidos por enaltecimiento del terrorismo y humillación de la víctimas no lo eran por conductas llevadas a cabo en el medio ordinario, sino por haberlo hecho en las redes sociales. En su actuación, la Guardia Civil, con la dirección de un juez, fue extraordinariamente exquisita a la hora de distinguir lo que entraba dentro del tipo penal de lo que quedaba amparado por la libertad de expresión, de manera que nadie pudiese quedar afectado por un exceso de rigor. Aunque determinados comportamientos o conductas en las redes sociales nos puedan parecer vergonzosos, repugnantes y crueles, no todos son delito. En esa operación se deslindó perfectamente lo que era un delito de humillación a las víctimas del terrorismo de otro tipo de expresiones, desde mi punto de vista, muy rechazables moralmente, pero no delictivas. Creo que eso mismo hemos tenido ocasión de verlo también con todo este debate que se ha generado a propósito de los delitos de odio, cuando se preguntaba si había alguna conducta delictiva en los comentarios de Twitter contra la comunidad judía con ocasión del partido entre el Real Madrid y el Maccabi. Y, desde luego, ése es un delito que está recogido en el Código Penal. Otra cosa es que seamos capaces de definir bien donde termina la libertad de expresión y dónde empieza lo delictivo; a lo mejor, de acuerdo con nuestra jurisprudencia, llegaremos a la conclusión de que la libertad de expresión ampara muchas conductas groseras, de mal gusto o incluso crueles, pero que no dejan de estar amparadas por la libertad de expresión. Otra cosa será el juicio moral que hagamos. Lo delictivo tiene que interpretarse en sentido restrictivo. Ése es un debate muy abierto. Cuando se generaron mecanismos de intervención policial frente a las co-

municaciones convencionales se fue generando un cuerpo de doctrina, y lo mismo es necesario para que la intervención sea siempre lo más respetuosa posible con los derechos fundamentales y las libertades de información en el mundo cibernético. Es un desafío al que tendremos que enfrentarnos día a día, y es tranquilizador que hay plena conciencia de que eso tiene que ser así. Desde luego, no se trata ahora de convertirnos en grandes censores de las redes o en policías virtuales para detectar cualquier tipo de comportamiento. Se trata de dar una respuesta eficaz, pues lo que no puede ser tampoco es que, detrás del anonimato o del encubrimiento que pueden dar las redes sociales, se escondan ámbitos de impunidad. Eso no puede ser. Tiene que haber la misma capacidad de reaccionar ante el delito en el mundo real que en el mundo virtual. Pero también los mismos límites y las mismas garantías públicas.

PEDRO GONZÁLEZ
Columnista de *ZoomNews*

La suya ha sido una respuesta muy larga que ha tocado muchísimos temas y algunas de sus respuestas abren otros debates. Hay uno que me parece que también entra dentro de ese diálogo y ese debate a propósito de las libertades, de la privacidad y del patrullaje de las redes sociales. Me refiero al de la gente que se manifiesta y que, aunque las manifestaciones tienen una finalidad que entra dentro de la normalidad, de crítica al Gobierno o al sector que sea, al final aparece mezclada con una serie de gente que acuden a las manifestaciones con ánimo de bronca. Se ha visto en Gamonal, en el paseo del Prado de Madrid, en Can Vies... En este sentido, y teniendo en cuenta movimientos como Rodea el Congreso, ¿hasta dónde llega el patrullaje o la legalidad o legitimidad para evitar este tipo de comportamientos? Me refiero a comportamientos de los que luego terminan siendo víctima la propia manifestación pacífica de mucha gente, que se ve

arrollada por operaciones de comando perfectamente organizadas a través de las redes sociales.

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Éste es otro tema recurrente: el derecho de manifestación y sus límites. Creo que en nuestro ordenamiento, no sólo en términos teóricos de previsión legislativa sino también de aplicación práctica por parte de los jueces y de las propias Fuerzas y Cuerpos de Seguridad del Estado, el derecho de manifestación está recogido y protegido con una extraordinaria amplitud. Y creo que eso es un síntoma razonable y necesario de una sociedad abierta y democrática. Así debe ser. El propio número de manifestaciones que se han producido en Madrid y en el resto de grandes ciudades españolas en los últimos años habla por sí mismo. Lo que también es verdad es que el derecho de manifestación no es patrimonio de determinadas corrientes ideológicas o de determinadas posicionamientos críticos. Ha habido tantas manifestaciones que el derecho ha sido ejercido por personas de muy diversa ideología, creencias y propósitos. Y la inmensa mayoría de las manifestaciones, incluso en momentos muy difíciles desde el punto de vista económico y social, como ha tenido este país, se han desarrollado de forma exquisita por parte de los manifestantes, en actitud pacífica y reivindicativa. En consecuencia, toda la presencia policial que haya podido haber en esas manifestaciones no ha tenido otra finalidad que proteger el propio ejercicio del derecho de manifestación. Ahí los datos son abrumadores.

Ahora, hemos encontrado infiltrados en manifestaciones que han causado enormes daños personales y económicos con destrozos del mobiliario humano. Eso también es una realidad. Creo que, desde el punto de vista jurídico, nadie podría defender que eso sea un ejercicio de un derecho fundamental. Eso es el ejercicio pura y simplemente de la violencia. Los disturbios en ma-

nifestaciones son totalmente minoritarios, pero existen. Tal vez sean anecdóticos desde el punto de vista cuantitativo, pero son alarmantes desde el punto de vista cuantitativo. Lo vimos en Madrid el 22 de marzo. Creo que todos recordamos las imágenes de las agresiones a los policías. En ocasiones, esas minorías –que en muchos casos han sido además las mismas personas– han aprovechado el ejercicio del derecho de manifestación para producir destrozos y violencia. Afortunadamente, tenemos unas Fuerzas y Cuerpos de Seguridad del Estado –hablaré de las que dependen de mí, pero seguro que se puede extender a las demás– extraordinariamente profesionales que han sido perfectamente conscientes de que había que minimizar los supuestos de intervención policial a los casos estrictamente necesarios, en los que se estaba desbordando el desarrollo normal de una manifestación y se estaba produciendo otra cosa. Por eso el número de intervenciones policiales es anecdótico. Lo que no podemos hacer es mirar a otro sitio. Por mucho que no sea un problema de enorme dimensión, está ahí y es un problema de violencia. Son pocos pues los casos en los que la policía ha tenido que hacer uso del material de defensa y creo que nuestra principal garantía y nuestro principal elemento de confianza es su profesionalidad. Permítanme que les recuerde una cosa: cuando en España se producía ese número enorme de manifestaciones, fundamentalmente en el año 2012, porque muchos españoles lo estaban pasando mal, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado también se les había recortado el sueldo, sólo que con la diferencia que a ellos se les pedía que trabajaran más, ya que el nivel de reivindicaciones y manifestaciones en las calles era muy superior. Creo pues que han demostrado una gran profesionalidad, que han permitido que todos esos movimientos se hayan desarrollado en un clima pacífico y que sólo han intervenido cuando ha habido incidentes violentos. Tenemos que tener claro que hay un límite también para el derecho de manifestación. Un límite que tiene que estar siempre en las interpreta-

ciones más extensivas del ejercicio del derecho, pero un límite al fin y al cabo. Eso no es una cosa que esté diciendo yo gratuitamente; es algo que podemos encontrar en la jurisprudencia del Tribunal Constitucional, en la jurisprudencia del Tribunal Supremo y, si me lo permiten, en el sentido común. Cuando unos individuos están quemando contenedores y papeleras, yo creo que ya no se están manifestando, sino que están haciendo otra cosa. Ahí creo que nuestro ordenamiento jurídico y nuestros cuerpos de seguridad deben tener capacidad de respuesta, pero es verdad que ésa tiene que ser siempre –en una expresión un poco cursi de jurista– la última *ratio*. Es decir, la última capacidad de reacción, reservada sólo para aquellos casos en los que sea absolutamente necesaria. Creo que eso es lo que ha caracterizado la actuación de las Fuerzas y Cuerpos de Seguridad en lo que va de legislatura y que ésa es nuestra mejor garantía.

GEORGINA HIGUERAS
Periodista *freelance*. Excorresponsal de *El País* en Asia

En primer lugar, gracias por su intervención, que ha sido muy formativa. Yo quería saber cómo se organiza o si está institucionalizada la relación entre la Policía Nacional y la Guardia Civil y las policías autonómicas. Además, quería saber si el clima más o menos de crispación que hay en la actualidad con algunas autonomías ha deteriorado esa conexión de traspaso de información de un sitio a otro. En el caso de un ataque o un temor cualquiera, ¿la información que fluye desde la policía autonómica a la Policía Nacional es puntual o está institucionalizada?

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Casi le puedo contestar con la misma afirmación que en la pregunta anterior: los cuerpos policiales son muy profesionales y,

por tanto, creo que saben que, por encima de disputas y dificultades políticas, tiene la misión nada menos que de garantizar los derechos y libertades de los ciudadanos y de proteger la seguridad. Como le digo, creo que son suficientemente capaces como para poner eso por encima de cualquier otra cuestión. Sé que lo que digo suena muy abstracto. Concretando, efectivamente existen diversos mecanismos de colaboración, de compartir información. Ha habido operaciones conjuntas con policías autonómicas y hay organismos, como el Centro Nacional de Coordinación Antiterrorista o el Centro de Inteligencia contra el Crimen Organizado –ambos dependientes de la Secretaría de Estado de Seguridad–, en los que hay presencia de las policías autonómicas con el objetivo de que todos estemos, por decirlo de alguna forma, en las mismas redes de información, compartiendo la información que sea necesario compartir. Luego, lógicamente, cada cuerpo tiene sus objetivos y sus ámbitos de actuación y competencias. Pero hay muchos mecanismos a través de los cuales se comparte información. Sería deseable que todavía existiesen más, que hubiera más bases de datos compartidas, más instrumentos de puesta en común de inteligencia y más operaciones. Eso desde luego sería lo deseable. Pero le puedo decir que, en términos generales, la colaboración que puedan tener la Policía Nacional y la Guardia Civil con los Mossos d'Esquadra, con la Policía Foral de Navarra o con la Ertzaintza, así como con las policías locales, es una colaboración razonable, satisfactoria y, ante todo, profesional, siempre guiada por criterios profesionales. Es a los responsables políticos a quienes nos corresponde impulsar mecanismos que hagan esa coordinación y cooperación más intensa y mejor. Yo he tenido ocasión de reunirme en varias ocasiones con el secretario general de la Consejería de Interior de Cataluña y con el viceconsejero de Interior del Gobierno Vasco, precisamente con la idea de mejorar los mecanismos de coordinación policial, siempre bajo la premisa de que nuestro objetivo es prestar un servicio a los ciu-

dadanos que tiene que estar por encima de reivindicaciones políticas. Creo que no hay en ese sentido ningún problema, aunque, por supuesto, lo deseable es que sea todavía mejor; claro que no nos vamos a conformar. Pero no hay ningún problema de relación.

De hecho, hay incluso mecanismos en los que necesariamente tienen que estar implicadas, no ya las policías autonómicas, sino también las policías locales. Estoy pensando por ejemplo en el sistema integral de violencia de género, coordinado desde la Secretaría de Estado de Seguridad, que tiene la finalidad de que las víctimas de violencia de género puedan estar protegidas por el cuerpo policial más cercano al lugar donde estén. Si una mujer es víctima de violencia de género y tiene su residencia en Madrid y decide irse de vacaciones, por ejemplo, a Torrevieja, el cuerpo policial competente más cercano, que en muchas ocasiones es la policía local del municipio competente, tiene que tener toda la información para darle protección. Para ello existe un sistema informático completo en el que se integran no sólo el Cuerpo Nacional de Policía, la Guardia Civil y las policías autonómicas, sino también las policías locales. Esto es un ejemplo de algo que estamos intentando promover para que esa integración sea lo más amplia posible. Pretendemos que todas las policías locales de España estén incorporadas a ese sistema, para que no se pueda dar la fatalidad de que una mujer víctima de violencia de género se desplace a un municipio en el que la policía local no tenga acceso a su expediente por el hecho de que no esté integrada en el sistema integral de protección de víctimas de violencia de género. Eso, de nuevo, es un esfuerzo de coordinación que debemos impulsar los responsables políticos correspondientes y ya hemos firmado muchísimos convenios con ayuntamientos para incorporar a sus policías locales. Se hace desde una perspectiva profesional y al margen de colores políticos, de reivindicaciones, de disputas o de cualquier otra cosa.

JESÚS ALFARO
Director de Comunicación de Navantia en Cádiz

Buenas tardes. Ha tocado usted todos los temas relacionados con las ciberamenazas y las respuestas que da el Ministerio del Interior a los complejos asuntos a los que se enfrenta nuestra sociedad. Quería que nos ampliara, en la medida de sus posibilidades y manteniendo la discreción pertinente, qué pasa con nuestro vecino del sur, con esos elementos de captación o, mejor dicho, esas mafias de trata de personas. En la otra vertiente, respecto al yihadismo salafista y al terrorismo internacional, quería saber qué cooperación hay con Marruecos. Es un país fronterizo y nosotros somos la puerta a Europa de un mundo que provoca enormes amenazas, como desgraciadamente sabemos por la trágica experiencia del 11-M. Querría saber qué se está haciendo, cómo se colabora entre los servicios de inteligencia españoles y los de esa zona.

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Le puedo asegurar que no le estoy dando una respuesta teórica ni retórica cuando le digo que la cooperación con el Reino de Marruecos en materia de seguridad es ejemplar. Tanto en lo que tiene que ver con la lucha contra la inmigración irregular, donde la presión migratoria y la actividad de las redes de trata de seres humanos la padece España, Europa y, por supuesto, el propio Marruecos. Solamente hay una fórmula en este caso: la cooperación internacional. Tiene que haber cooperación con los países de origen y con los países de tránsito, y en ese sentido, para España, la colaboración de Marruecos es absolutamente crucial. En estos momentos –le aseguro que no es retórica, por lo menos desde la perspectiva del Ministerio del Interior– sólo podemos tener agradecimiento y reconocimiento por la labor que han rea-

lizado las fuerzas de seguridad marroquíes en la lucha contra las redes de inmigración irregular.

Respecto a la lucha contra el terrorismo yihadista, le puedo asegurar también que Marruecos tiene una especial preocupación por este fenómeno, hasta el punto de que hemos realizado operaciones conjuntas con sus servicios de seguridad, haciendo detenciones simultáneas en España y en Marruecos, desmantelando redes de reclutamiento que operaban al mismo tiempo en territorio español y marroquí. Creo que la preocupación y nivel de movilización de Marruecos para hacer frente a este fenómeno es, para nosotros, una garantía de seguridad. No veo fácil estar mejor. Realmente la relación es estrecha, decisiva y activa y ha dado frutos en muchas de las operaciones que se han producido en las últimas semanas. Le doy un dato que ayuda a entender cómo se articulan esos mecanismos de actuación, al margen de las relaciones que tengan los operativos, que las tienen. Como secretario de Seguridad, por aquello de pertenecer al Ministerio del Interior, me desplazo muy poco al exterior. He hecho muy pocos viajes en este año y medio que llevo en el cargo. Pero, eso sí, he ido hasta cuatro veces a Marruecos. Cuatro veces. Aparte de eso, sólo he ido al Reino Unido y a Bruselas. Nada más. Ésa es toda mi agenda internacional. Y le puedo asegurar que en Marruecos he tenido reuniones enormemente interesantes y fructíferas. El ministro llama directamente al móvil al ministro marroquí y yo tengo el mismo nivel de interlocución con el ministro-delegado, que es mi homólogo. Hemos tenido muchos motivos de agradecimiento y muchas ocasiones de felicitación recíproca. Al fin y al cabo, que se desmantele una red de reclutamiento yihadista es motivo de alegría tanto para ellos como para nosotros. Si no colaboramos, ni la lucha contra las redes de trata ni la lucha contra el terrorismo yihadista van a tener fruto.

Marruecos también ha expresado otra serie de preocupaciones, por ejemplo, por la lucha efectiva contra las redes que operan en su territorio, donde se carga la mercancía en aeronaves

para llevarla a territorio español. Así, aeronaves lógicamente ilícitas aterrizaban en el sur de España, cargaban la droga en vehículos, generalmente de gran cilindrada, y la ponían en circulación en el conjunto de Europa. Como consecuencia de todo ello se constituyó el G-4, donde Marruecos, Francia, Portugal y España luchan con el objetivo de poner una barrera al tráfico de drogas desde el norte de África al conjunto de Europa. Y creo que con resultados muy satisfactorios. Ha habido muchas reuniones, muchas operaciones conjuntas y mucho intercambio de información, que es lo más importante. Y con un nivel de efectividad que, sin caer en la complacencia, calificaría de muy razonable. Por tanto éste es un ámbito en el que la cooperación es excelente. Por mi parte, sólo agradecimiento y reconocimiento al Reino de Marruecos.

JUAN CUESTA
Director de *Europa en Suma*

He oído claramente al secretario de Estado decir que «el delito es el delito, independientemente del medio a través del cual se lleve a cabo». Deduzco por tanto que aquellas especulaciones que hubo en su momento sobre una reforma legislativa que contemplara determinados tipos de delitos en las redes ha pasado a mejor vida. Entiendo pues que se ha olvidado. Si no es así, me gustaría que lo comentara. En segundo lugar, permítanme una reflexión. Cuando se persigue a personas que han hecho determinados tuits delictivos, está claro que se trata de una persona, que individualmente manda ese tuit, aunque tenga alguna identificación o perfil anónimo. En cualquier caso, siempre hay una responsabilidad individual cuando coloca ese tuit. Hay un fenómeno diferente que se da, por ejemplo, en los medios de comunicación, que abren sus noticias a la opinión y a los comentarios de los lectores o de los oyentes. Y lo cierto es que hay auténticas perversiones en determinados chats de los medios; ocurre en

los medios deportivos, por ejemplo. Algunos de esos comentarios son claramente delictivos, racistas. No sé si los medios saben que tienen responsabilidad sobre lo que publican, aunque lo haya hecho uno de sus lectores. Me pregunto si se habla con los medios, si los medios son conscientes de que tienen responsabilidad en esto, de que deben tener moderadores para controlar el tráfico, ya que ahí se están cometiendo delitos, por ejemplo, de racismo. No hay más que mirar algo tan habitual como son los comentarios después de un partido entre aficiones rivales.

FRANCISCO MARTÍNEZ VÁZQUEZ
Secretario de Estado de Seguridad

Sobre la primera pregunta, efectivamente, eso es lo que he querido decir, aunque seré un poco más preciso. Es verdad que se generó un debate a raíz de la alarma social que provocaron determinados comentarios o expresiones que resultaban en algunos casos, desde luego, delictivos, sin la menor duda. En otros casos eran extremadamente crueles, pero no delictivos. El fenómeno estaba estudiado desde un punto de vista jurídico y penal, pero lo volvimos a estudiar desde la perspectiva policial y desde la perspectiva del Ministerio de Justicia y del Ministerio Fiscal, donde existe una fiscalía especial de coordinación de los delitos que se cometen a través de la red. Llegamos a la conclusión de que tenemos algunos retos en el terreno de la investigación criminal de los delitos de ese tipo que se comenten a través de Internet. Debemos dar a los investigadores medios adecuados para que nadie, amparándose en el anonimato, pueda quedar impune si lo que comete es un delito. Sin embargo, desde el punto de vista de la legislación penal, llegamos a la conclusión de que el Código Penal ya recoge muchas conductas que son delito, con independencia de dónde se cometan. Pero teníamos algunas dudas. Primera: el hecho de que aquellas conductas puedan generar un mayor daño, porque al difundirse a través de redes socia-

les tiene una mayor capacidad de difusión que en un medio convencional, ¿debería suponer un agravante de la conducta delictiva? No un tipo penal diferente, sino una agravante de la sanción penal. Pues bien, eso ya está contemplado así en el proyecto de Código Penal que está en el Congreso de los Diputados: agravar la sanción penal por el hecho de que al cometerse a través de redes sociales tiene una mayor capacidad de daño. La segunda era respecto al encaje penal, pero no por la necesidad de crear nuevos delitos, sino más bien de encontrar el encaje penal adecuado a determinadas conductas –vamos a llamarlas de especial hostigamiento– que se producen contra personas a través de las redes sociales. Le puedo asegurar que lo que le preocupa a los ministerios del Interior y de Justicia no es tanto proteger a quienes tienen, o tenemos, responsabilidades políticas, que de alguna manera, como ya ha dicho la jurisprudencia, estamos más expuestos a la crítica, e incluso a la cruel, sin que eso quiero decir que valga todo. Jurisprudencia y doctrina hay sobradamente al respecto; no era esa la preocupación. La preocupación era el especial hostigamiento que a través de redes sociales pueden sufrir determinadas mujeres víctimas de violencia de género, o que pueden sufrir menores, el acoso, etcétera. La duda no era tanto que hubiera que crear un nuevo tipo penal para eso como que hubiera que crear un cuerpo de doctrina capaz de incorporar eso en delitos que ya existen. En algunos casos cuando el motivo es claramente discriminatorio, como los delitos de odio que están recogidos en el artículo 510 del Código Penal, la legislación está pensada para penar esas conductas con independencia del medio por el cual se cometan. Ése es el caso de los delitos o conductas antisemitas u homofóbicas. En otros casos, los delitos recogidos en el Código Penal bajo la modalidad de delitos contra la integridad moral podrían ser un encaje. Lo que hay que crear es crear cierto cuerpo de doctrina, pero solamente para aquellas conductas que no son injurias, que nos son calumnias, amenazas, enaltecimiento del terrorismo o delitos de odio, porque en esos casos

ya está claro lo que son los delitos y cuál es su castigo. Pero hay otros comportamientos que es verdad que se pueden producir de manera, por decirlo así, novedosa, a través de redes sociales y que son especialmente graves. Por ejemplo, hemos visto casos de menores que en su ambiente escolar estaban siendo absolutamente asediados –o asediadas, porque en muchos casos eran mujeres– por personas con una extraordinaria crueldad que estaban realizando un acto casi de hostigamiento a través de redes sociales. ¿Eso está cubierto entre los casos que el Código Penal contempla como delito contra la integridad moral? Bueno, entendemos que sí, que podría tener cabida ahí. Así lo entendieron la Fiscalía, el Ministerio de Justicia y las Fuerzas y Cuerpos de Seguridad del Estado: éstos son delitos contra la integridad moral. Es verdad que ese tipo delictivo no estaba inicialmente previsto para ese tipo de conductas, pero podría encajar vista la definición penal. Por tanto, la conclusión es que, en el Código Penal, no hay que crear nuevos delitos, sino que lo que hay que hacer es ver si hay que adaptar de alguna manera la definición de los que ya existen a los hechos que se cometan a través de nuevas tecnologías. Pero los delitos ya están inventados, por decirlo de alguna forma. Lo que sin duda hay que hacer es un esfuerzo por mejorar las herramientas de investigación criminal, que es ahí donde creo que debemos juntar los esfuerzos legislativos.

A propósito de los medios de comunicación y de quienes participan e intervienen en ellos, yo quiero pensar –aunque no sea la persona para responder a la pregunta– que los medios de comunicación son muy conscientes de la responsabilidad en que incurren por la difusión de opiniones de terceros que puedan proyectarse a través de las plataformas que ofrecen; o en la que podrían incurrir si no toman las debidas garantías por la difusión. No sé si, a lo mejor, Arantza podría responder mejor que yo a esta pregunta, como profesional de la comunicación que es, pero yo creo que son conscientes. Desde luego, nosotros, desde el Ministerio del Interior, tenemos una buena y estrecha relación

con los medios de comunicación, por muchos motivos. Ahora mismo no le sabría decir si sobre esto han trabajado específicamente las Fuerzas y Cuerpos de Seguridad del Estado; probablemente sí, aunque ahora no me consta. Pero entiendo que la principal responsabilidad es de los propios medios. De nuevo nos enfrentamos al mismo fenómeno, pues eso mismo se podría dar también antes a través de la comunicación convencional, a través de una Carta al Director o de un artículo. Lo que es verdad es que el mundo virtual hace que todo sea mucho más rápido, mucho más ágil y más fácil, pero la responsabilidad se podría dar del mismo modo.

ARANTZA MARTÍN
Moderadora

Lo más probable es que en los medios nos falte un poquito de diligencia y que podamos achacar fácilmente esos casos a que no tenemos medios suficientes para controlar la rapidez con la que nos llegan esos mensajes.

Creo que debemos agradecer especialmente al secretario de Estado que no solamente se haya quedado en los riesgos y amenazas, en el asunto que le traía aquí hoy, sino que haya tratado otro tipo de cuestiones que se le han planteado; entiendo que era difícil resistirse teniéndole delante. Agradecerle pues especialmente que haya dado respuesta a todas ellas.

7. NUEVOS OBJETIVOS DE LA INTELIGENCIA

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

Moderadora
ÁNGELES BAZÁN
Informativos de Fin de Semana de RNE

Ángeles Bazán y el General Félix Sanz Roldán

El factor «inteligencia» es clave en el planteamiento preventivo y en la resolución de cualquier conflicto y, desde luego, coopera a la estabilidad de los Estados democráticos. Su espectro de actuación se ha ampliado al ritmo de la tecnificación de los agresores y no se restringe ya a lo meramente militar, pues la globalización de las agresiones exige otras formas de actuación.

Una nueva incógnita se ha introducido en la ecuación de la defensa: la inteligencia económica, entendida como un instrumento más al servicio de los intereses generales y, en particular, de las empresas españolas que pueden verse perjudicadas por actores que no operan en el campo de la defensa convencional y cuya intervención se proyecta en distintos escenarios.

¿Cuál es el nuevo cometido de los servicios de inteligencia a nivel nacional e internacional? ¿Cómo han cambiado las nuevas amenazas las prioridades del Centro Nacional de Inteligencia? Ante un escenario global, ¿funciona la relación entre los servicios de los distintos países? ¿Es utópico pensar en un Centro de Inteligencia Europeo?

ÁNGELES BAZÁN
Moderadora

Bienvenidos a esta sexta sesión del seminario «Ciberamenazas y respuestas». Ante todo dar las gracias a la Asociación de Periodistas Europeos por permitirme presentar al General Félix Sanz Roldán, a quien tengo en una gran estima; quienes le conocen también saben de su empatía y del afecto que derrocha. El General es un viejo amigo de la APE y ha participado en estos seminarios en muchísimas ocasiones; hace un rato me comentaba que probablemente en más de diez ocasiones y en sus muy distintas responsabilidades: en el ejército, en el Ministerio de Defensa, como representante español en distintos organismos internacionales... Es decir, a lo largo de una muy larga carrera profesional de cincuenta años que no impide que esté en una forma excelente. Quienes conocen al General saben de su enorme vocación de servicio al país. De hecho, cuando habla de los servicios secretos, él dice que son más servicios que secretos. Cuando habla del trabajo del Centro Nacional de Inteligencia (CNI), se empeña en dar una sensación de normalidad a todo este trabajo que, para quienes somos aficionados a las películas y libros de espionaje, resulta un poco decepcionante, ya que todo se hace de acuerdo con el más escrupuloso servicio a la ley. El trabajo del CNI está marcado por la estrategia de seguridad nacional y también tenemos ahora una Estrategia de Ciberseguridad. A eso hay que sumarle que un juez del Tribunal Supremo autoriza todas las operaciones especiales y las escuchas. No hay misterio pues en el trabajo del CNI, ni tampoco superagentes con licencia para todo. El General nunca se queja, pero dirige el Centro Nacional de Inteligencia con un presupuesto que podríamos calificar, comparándolo con nuestro entorno, de exiguo, pues consiste en algo más de doscientos millones de euros. Con las amenazas que tenemos, no sé si, por muy buena gestión que se haga, se puede tener un servicio secreto innovador, a la última,

con todas las nuevas tecnologías que se necesitan, con ese presupuesto. También cuenta, afortunadamente, con un capital humano excepcional, cuya labor el General no se cansa de elogiar. Son 3.500 personas de las que él suele decir que son capaces de interpretar un susurro en más de treinta idiomas. Son además especialmente buenos en algunas cuestiones concretas. Eso es lo que salvaguarda la falta de presupuesto. Están muy preparados y gozan del reconocimiento internacional. La labor del CNI, como saben, es proporcionar al Gobierno elementos de juicio para tomar decisiones estratégicas, algo para lo que cuenta también con el Servicio Nacional de Criptología y con la Unidad de Inteligencia Económica. Podríamos decir que el General nos visita en un momento feliz, pues me consta que una de sus grandes preocupaciones son los secuestros y, afortunadamente, en los últimos meses se han resuelto los de los ocho españoles que había secuestrados en Somalia, el Sahara Occidental, Siria, etcétera. Todos ellos perpetrados por Al Qaeda, o por grupúsculos de Al Qaeda. El terrorismo fundamentalista se ha convertido en una de las prioridades de todos los servicios de inteligencia y de seguridad. Vemos la proliferación de grupos, tanto en países africanos como en Oriente Medio, en Siria, en Irak... En estos momentos, lejos de mejorar la situación, están proliferando grupúsculos de muy difícil control que manejan tanto armas como *hashtags*. Ayer comentábamos que en la red hay todo tipo de delincuencia, pues tiene bajo coste y un mínimo riesgo para el atacante. En la red, como ya saben, no hay fronteras, de manera que constituye todo un desafío para los servicios de inteligencia. Hoy, el General nos va a hablar de los nuevos objetivos de la inteligencia, entre los que, por supuesto, también está la ciberseguridad, con el Centro Nacional de Ciberseguridad de reciente creación y que él preside. Ayer, en la especie de máster acelerado que nos impartió el General, quedó claro que somos muy vulnerables, que no hay fronteras y que no hay una seguridad inviolable. Pero también quedó claro que somos muy conscientes de nuestra vulnerabili-

dad y que estamos poniendo los medios necesarios para evitarla; quizá uno de esos medios sería que los mejores *hackers* estuvieran de nuestra parte, trabajando para nosotros. Estoy segura pues de que la conferencia del General será muy enriquecedora.

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

Muchas gracias, Ángeles, mi buena amiga. Antes de empezar a desarrollar el tema que se me propone, les quiero dar una noticia para que no suban mucho el tono de sus expectativas. El año pasado, o hace dos años, invitaba a los que vinieron a escuchar la sesión de este seminario en la que participé a que hicieran un ejercicio. Les invitaba a que miraran por ejemplo el texto que editó la APE en el año 2002, hace doce años, cuando se celebro el seminario «Nuevos retos para la seguridad». Mírenlo y verán la cantidad de aciertos, o desde luego de buenas prescripciones, que en el año 2002 se hacían sobre lo que podría pasar en el año 2014. Y lo mismo en el año 2004, con el seminario titulado «Conceptos nuevos para la seguridad en el siglo XI». Les pido que vayan a su biblioteca, o a la biblioteca de la APE, y vean hasta qué extremo este ejercicio que estamos haciendo ha sido útil. Ha sido útil para aquellos interesados que querían saber más sobre la seguridad y ha sido útil, especialmente, para aquéllos que tienen que tomar decisiones y a veces no tienen suficiente tiempo para analizar todos los elementos de juicio que se han de tener en cuenta para tomar una buena decisión. Para los que estamos en esa posición, es magnífico que haya alguien que ponga su tiempo, su trabajo, su esfuerzo y sus neuronas a trabajar en nuestro beneficio y que lo concrete después, como hace la APE, en forma de libro. Es por tanto un gran honor para mí estar aquí. Es un gran honor haber sido invitado durante todos estos años; espero que no sea contumacia sino que, verdaderamente, alguna cosa interesante haya dicho y que por eso me inviten.

Hablo con frecuencia en público y, como bien decía Ángeles, casi siempre les digo a quienes me escuchan que somos un servicio secreto y que somos más servicio que secreto. El secreto lo mantenemos en sus límites justos, aunque es nuestra base para obtener información y para ser útiles al Gobierno. Pero también las gentes que trabajan en el CNI tienen algún derecho a que se reconozca su trabajo y eso, desde luego, se reconoce mejor sabiendo un poco lo que hacen, cómo lo hacen y por qué lo hacen. Yo tengo un defecto, que es que hablo de lo que se me pregunta. Hoy, si cogen ustedes el programa, dice que se ha ampliado el ritmo de la tecnificación de los agresores, que ya no es simplemente militar, que se han producido nuevas incógnitas... Y dice: «¿Cuál es el nuevo cometido de los servicios de inteligencia a nivel nacional e internacional? ¿Cómo han cambiado las nuevas amenazas?». Esto es lo que yo pretendo contarles, sin olvidar que estamos en un seminario que se titula «Ciberamenazas y ciberrespuestas». Por tanto, algo habrá que hablar también sobre ese asunto.

Llevo cinco años en el CNI, donde he adquirido alguna experiencia, y espero que esta experiencia pueda también transmitirles algún dato a ustedes. Creo que está magníficamente planteado que hablemos de los retos que tienen los servicios de inteligencia. Desde que yo llegué al centro hasta hoy hemos tenido que asumir misiones muy diferentes y actividades muy distintas a las que entonces teníamos. El esfuerzo de flexibilidad que ha realizado el centro ha sido pues importante. En primer lugar, hemos querido explicar a los españoles cuál es nuestra misión. En algunos momentos, esta misión ha estado difuminada por actividades muy llamativas, como ha sido la lucha contra el terrorismo, pero que no son la principal misión definida para el centro. Otra cosa es que el Estado, que el Gobierno, en uso de sus atribuciones, le encargue en un momento determinado al centro el cumplimiento de una determinada misión. Pero la misión general del centro siempre ha sido proporcionar elementos de juicio al Gobierno para que tome sus decisiones estratégicas.

¿Estratégicas en qué aspectos? Pues en prevenir y evitar cualquier riesgo o amenaza que afecte a los intereses nacionales, a la estabilidad del Estado de derecho y a sus instituciones. En el fondo ésa es la cuestión. Nuestro principal, y casi único, cliente es el Gobierno y nuestra misión es proporcionarle elementos de juicio para que tome decisiones estratégicas. No tenemos otros clientes. No pretendemos, desde luego, invadir competencias de las Fuerzas y Cuerpos de Seguridad del Estado, del Centro de Inteligencia o de las Fuerzas Armadas. Aunque, naturalmente, cuando colaboramos somos mejores todos. Y en colaboración hemos trabajado y seguimos trabajando con mucha intensidad.

La mayor parte de nuestra información, desde luego más de la mitad de ella, se obtiene de fuentes abiertas. Las fuentes abiertas son algo a lo que todo el mundo puede tener acceso, y son una fuente valiosísima de información. No hay que pensar en que todo aquello que manejamos son secretos, escuchas, intervenciones... Pero hay una parte singularmente importante de información obtenida por procedimientos propios de los servicios secretos, que son los que constituyen a veces la goma que pega toda aquella otra información obtenida mediante fuentes abiertas. Si esta obtención entra en colisión con alguno de los derechos que la Constitución reconoce a los españoles –por ejemplo la inviolabilidad del domicilio, el secreto de las comunicaciones, etcétera–, pues gracias a Dios el Centro Nacional de Inteligencia tiene una ley orgánica, la 2/2002, muy breve, que establece de forma clara que para cualquier actividad que hagamos que entre en conflicto con los derechos fundamentales de los españoles, o de los extranjeros en tránsito, necesitamos una autorización de un magistrado de la Sala Segunda del Tribunal Supremo. Fíjense que –sin menospreciar las actividades de nadie– no se trata del juez de Primera Instancia e Instrucción de mi pueblo. Es un magistrado del Tribunal Supremo, que está 365 días al año y 24 horas al día a nuestra disposición. Y realmente lo está. Ésa es una de las razones por la que estamos convencidos de que nuestra

actividad es una actividad digna, una actividad que se ejecuta siempre dentro de la ley. No salimos de caza ni hacemos aquello que no sea imprescindible para proporcionarle elementos de juicio al Gobierno. Y esto es muy importante. Un colaborador mío escribió una vez una frase que decía algo así como: «La calidad de una democracia y la eficacia del uso de los principios democráticos son precisamente los mejores parámetros para medir un servicio de inteligencia». Dicho en un lenguaje un poco más próximo a la calle, eso significa que cuanto más acepte y cumpla un servicio de inteligencia los principios en los que se sustenta una democracia mejor será la calidad de la democracia a la que sirve. Los servicios de inteligencia no pueden ser el centro del Estado, no pueden hacer que aquí valga todo, sino simplemente tienen que ser un instrumento más que cumpla la ley como todos los demás. Y, desde luego, es difícil encontrar un sistema que mida mejor el valor de una democracia que comprobar que sus servicios secretos cumplen exactamente con los principios democráticos. Y yo les garantizo que esto es absolutamente así.

Gracias a Dios contamos con una legislación muy clara. Y eso es algo que no todos los servicios tienen. También tenemos algo de lo que podemos presumir –ha habido recientemente casos muy notables al respecto, como el caso Snowden, etcétera–, que es que el deber de custodia de la información que se obtiene después de un auto judicial no ha sido conculcado nunca en los últimos años; y espero que eso siga así durante mucho tiempo. Ningún español ha visto u oído en un periódico, en un medio de comunicación, en una radio o en cualquier otro sitio, algo de sí mismo que se obtuviera vulnerando alguno de los derechos que la Constitución le reconoce. Ninguno. Yo les invito a ustedes a que me digan si conocen algún caso en el que haya salido algo del Centro Nacional de Inteligencia que esté protegido por el deber de custodia. Y eso es tan importante como no conculcar la ley, como no interferir, como no violentar los derechos fundamentales que la Constitución nos reconoce a todos. Es importantísimo que,

una vez que con un auto del magistrado tengamos acceso a determinadas cosas, nunca nadie pueda después utilizarlas en un medio de comunicación, de forma que alguien sienta que su intimidad ha sido maltratada. Las dos cosas son ciertas.

La inteligencia es una cosa radicalmente distinta a la información que se produce en los medios de comunicación. Yo he oído muchas veces decir: «Pero, hombre, ¿cómo es posible que hayamos sabido antes por la Reuters que han secuestrado un barco que por el servicio de inteligencia?». Pero una cosa es la información y otra cosa es la información que yo puedo proporcionar. Hay un caso muy llamativo, que fue un caso de secuestro de españoles en Mauritania. Efectivamente, una agencia –creo que fue la agencia oficial de Marruecos– anunció el secuestro. La tendencia normal es a preguntarse cómo es posible que lo sepa la agencia y no lo sepan los servicio de inteligencia, pero lo que yo sé treinta minutos después, y no lo sabe Reuters, es quién es el jefe del grupo que los secuestró, por dónde se mueve, en qué dirección están trasladando a los secuestrados para esconderlos, que dos de ellos están heridos, etcétera. Todo eso lo sabíamos los servicios de inteligencia media hora o una hora después. Por tanto, piensen ustedes que el valor que nosotros podemos aportar es un valor añadido, generado por haber estado trabajando en esa zona, en ese área, por haber trabajado sobre la posibilidad de ese tipo de delito, diez o doce años antes de que produzca. Y de ahí surge, sin duda, la primera virtud que tiene que tener una persona que trabaje en el CNI. Que es la paciencia. En este caso que les estoy contando era una mujer. A la media hora, cuando nos sentamos en el centro de situación, esta mujer ya tenía hasta los proyectables hechos, con las fotos y las caras de quienes, con el 99 % de seguridad, los había secuestrado y todas las actividades relacionadas. Por tanto, una cosa es la noticia, que con la capacidad de los medios de hoy es muy importante, y otra cosa es el dato de inteligencia, que tiene un valor añadido. Hay otro caso que juega en nuestra contra. En el secuestro del «Alacrana»,

que fue el primer secuestro que yo me encontré, un determinado día –era diciembre, una tarde horrible–, me llama alguien del Gobierno y me dice: «Ya han soltado al 'Alacrana'». Y lo le digo: «Pues yo no tengo noticias». «Hombre, ¿cómo es posible que no lo sepas? Si lo está dando la televisión». Es obvio que no los habían soltado y que era una noticia mal apreciada por los medios. Por eso digo que una cosa es inteligencia y otra cosa es información. La inteligencia es una cosa mucho más elaborada, que necesita de un trabajo específico, absolutamente profesional y muy delicado. Porque, naturalmente, el resultado es un elemento de juicio ni más ni menos que para que un Gobierno tome una decisión estratégica. Por tanto, no hay opinión en la inteligencia, ni debe haberla. Nosotros si no sabemos algo seguro, si no damos valor añadido a la información, sencillamente no lo decimos.

¿Dónde estamos ahora? Pues la realidad es que estamos viviendo un momento, por decirlo de forma gráfica, de sorpresa permanente. Hay muchas sorpresas en la historia de los servicios de inteligencia. Por ejemplo, creo poder afirmar que ningún servicio de inteligencia supo de la caída del muro de Berlín antes de que se produjera, o que ningún servicio de inteligencia supo de la inmolación del frutero tunecino que desencadenó la Primavera Árabe. Por tanto, no vayamos tampoco a decir que somos maravillosos y que todo lo que hacemos cuenta con una pátina de eficiencia. Hay muchos casos en los que no es así. Especialmente en este mundo en el que vivimos ahora. Estamos en un mundo nuevo y, por tanto, habrá que hacer algo nuevo, como está escrito en el convento de San Esteban en Salamanca. Fíjense qué clarividencia. En el año 1502 un franciscano dijo: «El mundo se ha hecho otro y por tanto hay que hacer otras cosas». Lo dijo en 1502. Bueno, pues aquí estamos en lo mismo. El mundo está en ebullición y estamos ya pensando en que tenemos que establecer procedimientos nuevos, medios nuevos, elementos de análisis nuevos... Porque nuestra misión, que es reducir el nivel de incertidumbre, tiene hoy unas dificultades superiores

que las que tenía hace veinte años. Podría parecer que es lo contrario porque contamos con mejores medios, pero no. Aquí ayer se hablaba de ciberseguridad y seguro que todo el mundo pensó, bueno, el CNI entrará en los ordenadores de los españoles como Juan por su casa. No es así, pero aun si lo fuera, no es tan fácil como parece. Es tal el número de lugares donde tenemos que poner el foco, es tal el número de inquietudes, de riesgos, de amenazas que pueden afectar al ciudadano español, que antes de hacer nada necesitamos saber hacia dónde mirar, Y después necesitamos de un análisis delicado y preciso, casi quirúrgico, de aquello que miramos. Por tanto, yo creo que el trabajo de los servicios de inteligencia se ha complicado enormemente. Nuestro trabajo es cada vez más difícil.

Por otra parte, también los propios ciudadanos nos exigen cada vez más. El ciudadano tiene todo el derecho a sentirse seguro. Digo sentirse porque una cosa es sentirse y otra cosa es que realmente lo esté. Y el trabajo de los servicios de inteligencia también consiste en proporcionar elementos de juicio para que nos sintamos seguros. Lo cierto es que, con la cantidad de actividades que desarrolla hoy una persona cualquiera que están afectadas por un riesgo de seguridad, sería fácil dejar de sentirnos seguros, pues la amplitud, la panoplia de cuestiones a las que tenemos que adaptarnos, es muy superior a la que había hace veinte años. Fíjense ustedes. Todo el mundo va a su cuarto de baño por la mañana, abre el grifo y espera que salga agua caliente. Imaginen lo que pasaría si no saliera, por ejemplo porque alguien en un sistema singularmente complicado de distribución de gas hubiera cometido un atentado, o porque alguien hubiera entorpecido tanto las relaciones comerciales internacionales como para que el gas que viene de fuera no llegara a España, o porque alguien hubiera sido capaz de hacer subir el precio del gas hasta unos precios tremendos y tuviéramos que pensárnoslo antes de abrir el grifo. Todas esas cosas, que ninguno de nosotros pensamos cuando nos duchamos por la mañana o cuando vamos a echar gasolina, ocurren. Es de-

cir, que, en el caso de una potencia como España, que es deficitaria en energía, podamos sentirnos seguros, sentir que todo fluye de manera normal, porque hay alguien que está ocupándose de todo ese ciclo de distribución, adquisición, distribución, etcétera, del gas. E igualmente nos sentimos seguros porque cuando entramos en nuestra cuenta bancaria nadie ha entrado excepto nosotros. O porque –y eso mis compañeros militares y Guardias Civiles lo saben especialmente bien– ya no miramos los bajos del coche con el espejito de nuestra mujer cuando salimos de casa. Nos sentimos seguros. Pero, en cada una de esas actividades, que tan naturales nos parecen, para sentirnos seguros es necesario que haya detrás un esfuerzo tremendo por parte de las Fuerzas y Cuerpos de Seguridad del Estado e incluso, si me apuran ustedes, de la actividad privada, que cada vez está entrando en los ámbitos de inteligencia con más fuerza. Ya que estamos hablando de esto, imagínense lo que es hoy la inteligencia económica; saber que no hay agresiones a nuestro sistema económico es una necesidad vital para la acción del Gobierno. En este momento un editorial del *Wall Street Journal* puede analizar infinitamente mejor que yo. De ahí que sea tan importante que esa simbiosis entre centros de inteligencia y la sociedad en general se vaya perfeccionando cada vez más. Ésta es otra cuestión, pues, como ven, estamos en un mundo cada vez más complejo y tenemos por tanto que aprovechar todo lo que se pone a nuestra disposición para disminuir esa complejidad y poder conseguir algo fundamental para los servicios de inteligencia, que es la capacidad de anticipación. El Centro Nacional de Inteligencia es perfectamente consciente, pues, de que hay riesgos que hace poco eran poco habituales y ahora lo son mucho. Todos estamos hablando siempre de, por ejemplo, el yihadismo radical. Éste es un problema que ya está en el frontispicio de la mayor parte –si no de todos– de las Fuerzas y Cuerpos de Seguridad del Estado en España, así como de los servicios secretos. Y también está, por supuesto, la ciberseguridad. Hay muchos elementos nuevos.

¿Qué ha hecho el Centro Nacional de Inteligencia al respecto? Pues, en primer lugar, el CNI ha hecho una reflexión muy profunda y ha dado forma ya a un documento en el que está muy bien elaborada nuestra estrategia: el CNI 2030; es todavía un borrador, pero no tardará en dejar de serlo. ¿Cómo creemos que debemos ser en el año 2030? En el año 2030 el mundo será otro. Será incluso diferente al de hoy. Pero, claro, dirán ustedes, aún faltan dieciséis años. ¿Qué no va a pasar hasta entonces? Hay un documento complementario a éste, que es el uso, ya con mucha naturalidad, del Centro de Lecciones Aprendidas, también establecido en el CNI. Seguro que a mis compañeros militares esto del Centro de Lecciones Aprendidas les suena. Yo fui militar 47 años y todo lo que aprendí vistiendo el uniforme que pueda ser de utilidad para el CNI –que es mucho– naturalmente lo aplico. Sabemos pues el horizonte al que vamos, que es el 2030. Y sí sabemos cuáles serán nuestras posibilidades y nuestros riesgos. También sabemos la forma en la que hemos afrontado situaciones parecidas con anterioridad, el *modus operandi* empleado entonces, que es para lo que sirve el Centro de Lecciones Aprendidas. Y, desde luego, hemos establecido también un sistema de planeamiento por capacidades, también similar al que se empezó a hacer en las Fuerzas Armadas cuando yo era Jefe del Estado Mayor de la Defensa. Haciendo un planeamiento por capacidades de lo que necesita el CNI, les puedo decir a ustedes que, por muy corto que sea el presupuesto, siempre se obtiene un beneficio. Naturalmente, en el beneficio se puede llegar más o menos lejos, pero haciendo un planeamiento en el que definas claramente las capacidades que tienes, las priorices y, a continuación, apliques los recursos económicos, siempre, sin excepción, obtienes unos beneficios. En resumen, ésos son los tres elementos fundamentales de lo que ha hecho el Centro Nacional de Inteligencia para enfrentarse a las nuevas amenazas.

Yo creo que España está mejorando mucho, pero durante muchos años hemos tenido poca tradición de inteligencia. Fíjense

ustedes en el Reino Unido, por ejemplo. En el Reino Unido la inteligencia tiene una gran tradición, y no sólo porque se hayan hecho catorce películas de James Bond y del MI5 y del MI6. Es algo que se ve. Cuando alguien habla con un británico un rato, por muy poca curiosidad que tenga por estos temas de seguridad y defensa, termina enterándose de que conoce a alguien en el sector, o que alguien le ha dicho algo, o que él estaría dispuesto a colaborar de una forma activa en la seguridad del Reino Unido. En España eso nunca ha sido así, desgraciadamente. Cuando llegué al Centro Nacional de Inteligencia, hice visitas a mis homólogos en países muy punteros en esto, y recuerdo que el entonces jefe del MI5 me dijo: «Excepto a los miembros del Gobierno, yo puedo convocar a mi despacho a quien quiera. Pero lo bueno no es eso. Lo bueno es que viene». Algo que era radicalmente diferente en el Centro Nacional de Inteligencia al que yo llegué. Primero había que llamar a alguien y dorarle la píldora para intentar convencerle de que lo que iba a hacer era una cosa razonable para nuestra seguridad, que iba a ayudarnos a ser más eficaces. Desde luego, aquí ése no era el *modus operandi* natural. Pero también es verdad que vamos progresando. Ahora vemos que nuestro trabajo va consiguiendo la aceptación social necesaria; tampoco puede ser excesiva, porque muchos de ustedes no conocen el detalle de lo que hacemos y, por tanto, podrían tener alguna reserva. Pero sí vamos encontrando una mejor apreciación de los españoles.

Como también nos damos cada vez más cuenta de que la inteligencia no es monopolio del CNI. Muchos empresarios, centros de educación o escuelas de negocios han entrado, gracias a Dios, en este juego de hablarnos, porque cada uno puede aportar una visión diferente y, entre todos, podemos hacer que España funcione mejor. No sólo hablo de instituciones públicas, sino también de instituciones privadas. Para que sea buena, la relación tiene que ser simbiótica. Si yo doy y doy pero no recibo nada, me canso. Y al revés. Y les diré que, a la hora de defender los inte-

reses de nuestras empresas en el exterior, también la relación es simbiótica. Del mismo modo que yo puedo facilitar una información a un empresario que le vendrá bien para implantar su negocio en un determinado lugar, les diré –y se lo digo con mucho orgullo– que es también norma que los empresarios nos ofrezcan su ayuda para que podamos servir mejor a España en el exterior.

Los objetivos informativos, desde luego, hay que preverlos con tiempo. La previsión, en nuestro caso y como todos ustedes saben, es el proceso de generación de la Directiva de Inteligencia. Nos lleva ocho meses dar forma a la Directiva de Inteligencia, que se aprueba siempre en el mes de enero para el año en curso. Por tanto, ya hace tiempo que empezamos a hacer la Directiva de Inteligencia del año que viene. ¿Qué es lo que vemos como posibles cambios a corto plazo? Pues, en primer lugar, yo creo que no resulta probable que los grandes intereses de nuestro país se pongan en juego en escenarios geográficos muy distintos a los que tenemos ahora. Creo que el foco, en ese caso, está bien puesto. Creo, en cambio, que la lucha contra el terrorismo radical ha pasado sin duda a ser el primer elemento de nuestra estrategia de seguridad. Desde luego, también podemos decir que los sectores estratégicos españoles van a seguir contando con nuestro apoyo y, si podemos –y creo que vamos a poder–, les vamos a dedicar un mayor esfuerzo. Tienen ustedes que ver que los intereses estratégicos españoles, que hace veinte años estaban muy centrados en España y en algunos países de nuestro entorno, hoy están en todo el mundo. Hoy una empresa española puede estar licitando por la construcción de una autopista en Nueva Zelanda o construyendo el metro de Riad o haciendo el canal de Panamá. Son tantos los lugares en los que ahora se manifiestan los intereses españoles que tenemos que ampliar nuestro despliegue exterior. Creo que eso es algo que también vamos a hacer. El despliegue interior, en cambio, lo vamos a mantener en las funciones y en los lugares que tenemos ahora. Lo que sí vamos a potenciar es un nuevo sistema de inteligencia humana. Todos sa-

bemos que la inteligencia obtenida por fuentes humanas es definitiva, por lo que siempre hay que trabajar en ese sentido. Para ello ya se ha establecido la Dirección de Enseñanza del CNI y se han establecido unos nuevos sistemas que pondrán a las fuentes humanas en el lugar que ocupan hoy los riesgos que nos preocupan. Y, desde luego, la adquisición técnica también tiene que continuar. Les diré que el CNI tenía unas capacidades técnicas que yo calificaría de magníficas –logradas con el esfuerzo de todos los españoles– después del 11-M, pero la técnica va muy rápido y se queda vieja muy pronto. Por tanto, tenemos también que hacer un esfuerzo en las adquisiciones de materiales modernos. Antes el seguimiento consistía en una persona que se centraba en otra persona, pero ahora hay miles de medios técnicos que nos ayudan y que, además, permiten que las propias personas que están en la calle tengan un concepto nuevo de la seguridad y un concepto nuevo de los retos a los que nos enfrentamos.

Por tanto, tenemos que hacer un esfuerzo importante en medios; y, si no se puede adquirir todo en un año, pues iremos a los programas plurianuales. Tenemos que priorizar y, para eso precisamente, establecimos un sistema de planeamiento por capacidades. Y, desde luego, tenemos y tendremos una relación cada vez más estrecha con otros servicios de inteligencia. Les diré que, con los países amigos y aliados, éste es el funcionamiento normal. Yo no actúo en Francia, por ejemplo, o en el Reino Unido sin que Francia y el Reino Unido lo sepan. Lo hacemos juntos. Lo hacemos con su apoyo. Y compartimos lo que tenemos. Pero esta colaboración es en países determinados, amigos y aliados, donde verdaderamente alcanza su verdadero valor; cuando estamos en coalición. Me refiero a las *Coalition of the Willing* que tanto se mencionan en la OTAN y en la Unión Europea. Por supuesto, las agencias de inteligencia también protegen a nuestros soldados, en Afganistán por ejemplo; ahí está el CNI protegiendo a nuestros soldados y colaborando con las agencias de otros países. Pero no sólo es eso. En los servicios de inteligencia tam-

bién se está empezando a generar algo que ya se generó hace diez años en las Fuerzas Armadas, que es lo que se llama en inglés *role specialization*, especialización por funciones. Es decir, los servicios de inteligencia tienen que tener dos o tres cosas excelentes –no más– que puedan ofrecer a sus servicios amigos y aliados, y, a cambio, reciben de ellos otro servicio en el que el amigo aliado es excelente. Esto se está produciendo todos los días. Yo les puedo decir a ustedes que, en un determinado escenario –y permítanme que sea discreto–, España tiene esa especialización en inteligencia humana. Pues nuestros amigos y aliados nos dijeron: «No se preocupe usted, dedíquese usted a esto, de lo que sabe mucho, y yo le proporcionaré la información técnica que necesita, para que no tenga que distraer ni un solo esfuerzo de aquello que está haciendo». Y el de al lado dijo: «Sí, y yo le proporcionaré este otro asunto». Así creamos la *Coalition of the Willing*, donde cada uno hace lo que mejor sabe hacer en beneficio del conjunto. Éste es el pan nuestro de cada día. Cuando yo era JEMAD, nos reuníamos en la OTAN, o en la Unión Europea, y se hacía una foto de familia y salíamos todos sonrientes para demostrar que estábamos en buena sintonía. Pues todo eso ocurre igualmente en los servicios de inteligencia; lo que pasa es que se hace con discreción, sin fotos de familia. Creo que es singularmente importante que sepan ustedes que esto existe, que es como les digo.

Para terminar, quería reiterar que sería difícil encontrar en España un grupo de hombres y mujeres que se dediquen con más esfuerzo a las labores que se les asigna. No digo que no haya otros que dediquen el mismo esfuerzo, la misma ilusión, pero les garantizo que nadie tiene más dedicación. Los 3.500 hombres y mujeres que sirven a España en el CNI son conscientes de que trabajan en la oscuridad, con muchas incomodidades, de que trabajan incluso sin la posibilidad de comentar los detalles de su trabajo con su familia o sus amigos, pues saben que si se produce un hecho de especial relevancia, como por ejemplo ocurrió

con el 11-M, los medios de comunicación y los ciudadanos volverán su vista hacia ellos y se preguntarán por qué no fueron capaces de evitarlo. Lo que sostiene a todas estas personas que trabajan en el CNI, más allá de estas presiones que les cuento, es el desempeño de una obligación crucial para la seguridad de España y de los españoles, un desempeño que afrontan con toda la ilusión y con todo el esfuerzo posibles.

Esto es lo último que quería comentarles. Aquí termino. Muchas gracias.

ÁNGELES BAZÁN
Moderadora

Muchas gracias por la exposición, tan clarificadora y enriquecedora. A continuación, el General ha accedido a responder a las preguntas que quieran hacerle.

ENRIQUE PERIS
Excorresponsal de TVE en Londres

Gracias, General, por su brillante y completa exposición. Usted dice que una de las tareas del centro que dirige es defender y apoyar los intereses de España y secundar los intereses de las empresas españolas en su expansión en el mundo. Al mismo tiempo, nos ha hablado de la utilidad y necesidad de compartir lo que tenemos con amigos y aliados y una de las preguntas de la exposición inicial es hasta qué punto es utópico pensar en un centro de inteligencia a nivel de la Unión Europea. No sé si hay una cierta esquizofrenia en esos dos objetivos –aunque los dos sean absolutamente legítimos–, porque compartir lo que se tiene con los amigos y aliados y al mismo tiempo defender los intereses de las empresas nacionales parece contradictorio cuando, por ejemplo, los intereses de las empresas españolas y los de las empresas francesas son absolutamente contrapuestos, e incluso se dan pu-

ñaladas en la espalda unas a otras, como ocurre, por poner un ejemplo, en su implantación en Marruecos o en Arabia Saudita. ¿Cómo va a ser posible un servicio a nivel de la Unión Europea cuando las naciones siguen siendo tan terriblemente competitivas unas con otras y usan abierta y descaradamente el juego sucio?

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

Creo que esto es algo que ocurre en todas las alianzas. Me acuerdo de las discusiones que se produjeron –quizá el embajador Miranda, que está presente, lo recuerde– cuando trabajábamos en el concepto estratégico de la OTAN en el año 1999. Pero al final todos teníamos intereses comunes de seguridad. Y ése es el tono en el que se hacen generalmente las cosas. Por ejemplo, si hay una colaboración con los franceses contra el terrorismo, estamos defendiendo un interés común, sin que eso quite que, en algún lugar de la Tierra, haya empresas francesas litigando con empresas españolas por la obtención de algún contrato notable. En el caso de los intereses comunes se trabaja en común y en el caso de los intereses contrapuestos se trabaja para que, al menos, se respete el juego limpio. Además, si en alguna ocasión –que yo no he detectado hasta el momento– se viera que no se respeta este juego limpio, quizá sería más fácil hablar entre servicios de inteligencia que entre Estados. Una de las virtudes que tienen los servicios de inteligencia es que pueden utilizar los recursos del Estado, influyendo en decisiones del Estado sin que lo parezca. Así es como funcionan; no es que esté hablando de lo que podría ser, sino que es como detallo.

Sobre los servicios de inteligencia comunes en la Unión Europea, creo que de momento es difícil. Y lo es por varios motivos. Una es que, en algunos casos, las naciones son muy celosas a la hora de compartir con otras 27 naciones aquello que obtienen sus servicios de inteligencia con mucho esfuerzo y riesgo, y

que normalmente es de gran valor. A su vez, en Bruselas tampoco hay una cultura sobre la utilización de los informes y notas que pueda dar un servicio de inteligencia, salvo en el día a día. Aunque el Centro de Situación de la Unión Europea está funcionando francamente bien, con informes de los servicios de inteligencia de los países miembros. Pero el concepto de tener un sistema de inteligencia propio de la Unión Europea, en mi opinión, está todavía muy lejos. Es un poco como lo que viví antes del establecimiento –aún no logrado– del ejército europeo. Llegamos incluso a confundir el Eurocuerpo con un ejército europeo, pero todos los bien informados saben que eso no es así. La creación de un sistema de inteligencia europeo será una repetición del proceso de la creación del ejército europeo. Aun así, tampoco hay que olvidar que los servicios nacionales de inteligencia siempre aportan cosas a la Unión Europea.

ÁNGELES BAZÁN
Moderadora

A propósito de lo que dice, General, me gustaría plantearle una cuestión que ya se expuso ayer. ¿Hasta qué punto ha influido en el intercambio de información leal entre los distintos servicios de inteligencia el hecho de comprobar que un país aliado ha espiado a algunos de sus socios? El embajador Miranda apuntó una frase que me encantó. Decía: «Confía, pero verifica». ¿Hasta qué punto hay más reticencia ahora? ¿Hasta qué punto pesa más ese «verifica» que el «confía»?

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

Creo que hay que ir caso a caso. Es decir, en algunos lugares se lo han tomado peor que otros, donde el espionaje ha sido menor. No se puede dar una respuesta universal. No es que quiera elu-

dir la respuesta; es que es así. Cada país, en vista de la agresión que haya podido sufrir, o que haya percibido, ha generado después una respuesta acorde. No hay forma de saber todo lo que ha ocurrido en otros países. Yo fui al Congreso, como saben, y todos los grupos políticos terminaron diciendo que las explicaciones eran suficientes y razonables. Y ahí acabó el asunto.

PEDRO GONZÁLEZ
Columnista de *ZoomNews*

Buenos días, General. Suscribo lo que decía Ángeles Bazán respecto a la empatía que suscita usted en todas sus comparecencias en este Seminario; siempre aporta algún elemento novedoso. En esta ocasión me quedo con dos cosas. Una se la había oído antes; me refiero a lo de que la población se sienta segura. La otra es la observación que ha hecho al respecto de que, ahora, los servicios secretos viven en una sorpresa permanente. Uniendo las dos cosas, mi pregunta iría en el sentido de si, teniendo en cuanta esa sorpresa permanente, podemos los españoles sentirnos seguros, por ejemplo, de que no vaya a haber un proceso secesionista, de no vaya a haber alguna sorpresa.

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

Creo que usted entenderá perfectamente que no hable en público de ese asunto; por una razón que también entenderá, que es que cualquier afirmación del Centro Nacional de Inteligencia sobre ese asunto será sin duda malinterpretada. Mantengo informado al Gobierno al respecto, como lo hago sobre cualquier otro asunto. Perdónenme que no sea más explícito, no porque no tenga mi opinión personal y oficial –que las tengo ambas–, sino porque lo que yo diga sobre ese asunto puede interpretarse en contra del beneficio común. Pero también le diré que, efectiva-

mente, el esquema de sensación de seguridad en España es muy bueno. En este momento las encuestas manejan que sólo hay dos países en Europa más seguros que España; eso es lo que dice el Eurostat. Tampoco es cuestión de echarnos flores a nosotros mismos, pero consulte el Eurostat y verá que sólo hay dos países más seguros que España –siguiendo los parámetros que ellos imponen, y en los que llevan trabajando muchos años–. Por tanto, serán razonables. No hay duda de que el esquema de seguridad español es bastante eficaz. Pero tenemos que seguir trabajando, igual que lo hacíamos por ejemplo ante un atentado de la banda terrorista ETA, cuando los cometía. La posibilidad de anticiparnos a la comisión de un acto que vaya contra la seguridad de los españoles es nuestro oficio. Un oficio complejo, desde luego, en el que nos esforzamos por tener muchos más éxitos que fracasos. Pero debemos esperar que se produzcan ambas cosas.

FELIPE SAHAGÚN
Miembro del Consejo Editorial de *El Mundo*

Muchas gracias, General. Teniendo en cuenta la prioridad que ha dicho que tienen los servicios secretos españoles en el seguimiento e información del terrorismo yihadista, y teniendo en cuenta lo que ha ocurrido en los últimos dos años en Siria y en Irak, junto con la multiplicación en los medios europeos de declaraciones anónimas citando a fuentes de los servicios secretos de los distintos países, ¿hasta qué punto se ha intensificado la preocupación por el fenómeno de los europeos que están luchando con el grupo ISIS y con su posterior retorno? Incluso se han citado cifras por países, aunque creo que no podemos saber hasta qué punto son reales. ¿En qué medida nos puede trasladar información sobre el trabajo que los servicios de inteligencia europeos están haciendo al respecto?

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

En efecto, el yihadismo es un reto importante para nuestra seguridad. El yihadista, antes de atentar, tiene que hacer la yihad, que es una condición que ellos mismos se imponen. Y cada vez tienen más oportunidades y lugares donde hacerla. El otro día, en la nota que daba el Ministerio del Interior sobre una operación de los Cuerpos y Fuerzas de Seguridad del Estado, se hablaba del número de personas detenidas que habían ido a hacer la yihad a Siria y del número de personas que había ido a hacerla a Malí. Por tanto, ahora está claro que esa condición, que es condición *sine qua non* para ser yihadista, está más cerca de nuestras fronteras. La yihad ha pasado de Afganistán, o de escenarios muy lejanos, a escenarios más próximos. Eso no quiere decir que sea más fácil el control. Por eso nos hemos aplicado y hemos sacado más conclusiones. Creo que es cierto que los escenarios del yihadismo son los que citamos, como también lo es que para ser un terrorista en un país europeo previamente han tenido que estar en uno de esos escenarios. Incluso los lobos solitarios hacen cosas en común. Eso va dando algunas posibilidades a los Cuerpos y Fuerzas de Seguridad del Estado en el sentido de que los atentados ya no sean tan imprevisibles como lo fueron al principio. Y de ahí se derivan esos éxitos indudables que son las detenciones de yihadistas de los últimos días; éxitos absolutamente indudables, como digo. Cada uno tiene sus cuentas, pero sí podemos saber con alguna aproximación más o menos quiénes son los que pueden actuar en cada lugar.

JOSÉ MANUEL VERA
One Magazine

Habla usted de intensificar los esfuerzos en inteligencia humana y de las posibilidades que nos ofrecen la tecnología. Todos mi-

ramos a un futuro lleno de robots, pero eso es justo lo contrario de lo que usted acaba de poner en valor, que es que el hombre sigue siendo necesario. En este sentido, y dado que también hablamos de ciberamenazas, del ciberespacio, en ese futuro del 2030, ¿va a perder fuerza el elemento humano en favor de la tecnología, que facilita muchas cosas, o, por el contrario, piensa que por mucha tecnología que haya al final la persona va a ser en 2030 incluso más importante que ahora?

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

Lo que he querido decirles, a lo mejor de forma poco clara, es que se va por el segundo camino. Es decir, aunque la inteligencia humana va a seguir siendo importante, en muchos casos imprescindible, también es verdad que va a contar con la ayuda de los nuevos desarrollos técnicos. Sé que es un ejemplo un poco de andar por casa, pero imaginen lo que ha significado pasar de las antiguas cámaras de fotos, que por muy pequeñas que fueran tenían un cierto tamaño, a la cámara actual, que es un poco mayor que una lenteja. Imaginen lo que ha mejorado la inteligencia humana simplemente con ese desarrollo. Aunque, por supuesto, ese desarrollo sigue exigiendo de las relaciones humanas para completar el ciclo de inteligencia. Precisamente por eso reitero que tenemos que establecer un nuevo sistema para adiestrar a las personas que se dedican a inteligencia humana dentro del CNI. El ciclo continuará con más capacidades técnicas y con una formación actualizada para la inteligencia humana.

EMILIO ANDREU
Corresponsal para Asuntos de Defensa de RNE

Le quería preguntar, General, de qué sirve tanta anticipación, estar en Afganistán tantos años como hemos estado, en Malí, en la

República Centroafricana, si según el último informe de la RAND Corporation, de 2010 a 2014 hemos pasado de tener cincuenta mil yihadistas a tener cien mil, y de 31 organizaciones a 49. Es decir, que ha ido en claro aumento. ¿De qué nos sirve pues todo esto? Está muy bien lo de la inteligencia humana y lo de desplegar soldados –aunque hayan muerto muchísimos–, pero al final estamos consiguiendo lo contrario de lo que pretendíamos, pues los yihadistas se han duplicando el número. Y una segunda pregunta, si la puede contestar. Sabemos que en Alemania, Inglaterra y España se han desbaratado complots yihadistas que estaban a punto de cebarse con nosotros. ¿Puede decirnos cuántos casos se han dado en España en los últimos años? Muchísimas gracias por su explicación y por su conferencia.

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

La repuesta a la primera parte de su pregunta es relativamente sencilla, aunque entramos en una nueva indefinición. ¿Si se han multiplicado los esfuerzos, por cuánto se podría haber multiplicado la amenaza sin estos esfuerzos? La realidad es que esto es una lucha de voluntades y el éxito o el fracaso se está midiendo como usted bien dice. Pero yo le puedo asegurar que la situación sería infinitamente peor si los servicios de inteligencia no estuviéramos dedicando el esfuerzo que dedicamos. Sólo Dios sabe lo que hubiera ocurrido de no hacerse este esfuerzo, pero no tenga la menor duda de que la situación sería mucho peor. Hay muchos estudiosos sobre este asunto. Por otro lado, no hay que olvidar que el yihadista inicialmente cree que se está defendiendo de un ataque terrible de nuestra civilización, de nuestra cultura, y que, por tanto, estamos ante una lucha de voluntades. Pero a mí no me cabe la menor duda de que la situación hubiera sido peor en caso de no haber dedicado el tiempo y el esfuerzo que hemos dedicado. Sobre su otra pregunta, no sé el número exac-

to. Ayer mismo el Ministro de Interior daba datos estadísticos sobre las detenciones, pero no los recuerdo.

MIGUEL ÁNGEL AGUILAR
Secretario general de la Asociación de Periodistas Europeos

General, ¿esta obsesión por la exhaustividad, por controlar toda la información, por que no se escape nada, produce mejores resultados a la hora de emitir un juicio o, por el contrario, resulta en ocasiones desorientadora? Lo digo porque da la impresión de que hay mucha más información de la que algunos servicios son capaces de digerir, de contextualizar, de que ese desbordamiento no añade nada nuevo, más que confusión y desorientación. A veces, con menos datos pero mejor buscados se está en condiciones de hacer un juicio más ponderado y exacto. La otra cuestión si, en medio de todos estos avances tecnológicos tan acelerados, no habrá campo para un regreso a procedimientos antiguos que a lo mejor ahora cobran un nuevo valor.

GENERAL FÉLIX SANZ ROLDÁN
Director del Centro Nacional de Inteligencia

En primer lugar, en efecto, cuando la información tiende a infinito el problema es insoluble. Si pasamos de un umbral de información en el trabajo, pues adiós, estamos perdidos. ¿Cómo se atempera esto? Con los nuevos procedimientos de análisis y con las herramientas que hoy empezamos a tener para el análisis. Por ejemplo, no es lo mismo analizar un problema ahora, ante un ordenador en el que cada uno tiene su base de datos, tiene su propia Wikipedia para recordarle cualquier dato del que no se acuerde, como dónde estuvo una persona en un día determinado. Así pues, la técnica aumenta la capacidad de analizar noticias. Pero tienes toda la razón: cuando estamos con demasiadas cosas, con demasiados datos, el problema es insoluble. Pero ése no es nues-

tro caso. Hablando del CNI, hay algo que tenemos que dejar claro. En primer lugar, nosotros no salimos a buscar datos que no estén relacionados con los objetivos de la Directiva de Inteligencia o con las órdenes que de una forma circunstancial nos haya dado el Gobierno. Es decir, los chicos del CNI no se reúnen por la mañana, como en las películas de policías de Nueva York, y dicen: «Johnny y Matthew, vosotros a la calle 36, que ha habido un...». No. Aquí se levantan y cada uno coge su Directiva de inteligencia, dentro de su división, en la que tiene un objetivo asignado, y eso es lo que hacen, exclusivamente eso. Por tanto, eso ya disminuye mucho el foco. No tienen que salir a mirar qué pasa por el mundo y luego ver que si lo pueden aprovechar para su caso, sino que la operación es al revés: éste es el caso que tengo asignado; voy a ver dónde encuentro un dato que pueda ser de valor para este caso. Es así como se hace. Pero también es verdad que hay que tener mucho cuidado con no abrir demasiado el espectro; aunque, como he dicho, los elementos técnicos que tenemos hoy en día son de gran ayuda para analizar grandes cantidades de información. Por ejemplo, mezclando fotos con conversaciones, el analista, el buen analista, con las nuevas técnicas de las que dispone, puede sacar muchas más conclusiones que el viejo analista, que sólo tenía lo que apuntaba en un papel. Así pues, la técnica a veces ayuda y a veces no, pero en general sí ayuda. El genio, voy a decir militar, porque ése ha sido el caso en mi vida, el genio militar siempre ha sido el que ha sabido poner la técnica de su parte. Analicemos la historia. ¿Por qué el Gran Capitán no pierde ninguna batalla? Porque los arcabuces mataban más que otras armas. En la batalla de Bicoca –por eso se dice «esto es una bicoca»–, el Gran Capitán se enfrenta con quinientos españoles en Italia a 13.000 enemigos. No hay ni un solo muerto español y hay dos mil, o los que fueran, en el ejército contrario. La batalla la ganó el Gran Capitán sin un solo muerto porque supo poner de su lado la técnica. Y eso ocurrió también con Federico el Grande y con Patton, etcétera. Por tanto, no hay que olvidar que mien-

tras la técnica esté de nuestra parte tendremos más posibilidades de ser eficaces.

ÁNGELES BAZÁN
Moderadora

General, muchísimas gracias. Ha sido como siempre muy interesante escucharle. Muchas gracias también a los asistentes por sus preguntas y por su atención. Gracias a todos.

TENIENTE CORONEL DE LA GUARDIA CIVIL FERNANDO JOSÉ SÁNCHEZ
Director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)

JUAN ANTONIO GÓMEZ BULE
Presidente de S21sec

TENIENTE CORONEL DE LA GUARDIA CIVIL LUIS HERNÁNDEZ
Jefe del Área de Ciberseguridad de la Guardia Civil

Moderador
ALBERTO RUBIO
Director de *The Diplomat in Spain*

Fernando José Sánchez, Luis Hernández, Juan Antonio Gómez Bule
y Alberto Rubio

La tecnología que involucra a la ciberdefensa es empleada en numerosos delitos para eludir riesgos y garantizar el anonimato irresponsable, ya que resulta difícil identificar el origen o a los autores del ataque. Se trata de una materia transversal que afecta a numerosos departamentos, instituciones y empresas y que necesita de un elevado grado de colaboración.

Los ministerios de Defensa y de Interior están especialmente relacionados en esta materia, pero, además, para desarrollar las tecnologías necesarias y mantener seguro el ciberespacio es imprescindible que exista una estrecha relación con las empresas privadas. ¿Pueden las administraciones competir con la amenaza que suponen los hackers *que actúan desde la impunidad sin más arma que un ordenador portátil? ¿Necesitamos la colaboración de quienes invierten a diario en desarrollar antídotos contra esos ataques? ¿Cómo se apoya la administración en lo civil? ¿Cuál es el papel de la empresa privada, tan sólo el de vendedor de software, o debe asumir otras responsabilidades?*

ALBERTO RUBIO
Moderador

En esta sesión nos vamos a centrar en lo que hemos titulado en el programa como «Sumandos para la inteligencia». Es decir, la

cooperación absolutamente necesaria para proveer de seguridad tanto a administraciones públicas como a empresas que, en estos tiempos que corren, son víctimas de un tipo de espionaje o de ataques que, a los que somos legos en la materia, nos cuesta tanto comprender como que los aviones vuelen o que los barcos floten. Desde luego, la ciberseguridad es algo que, por mucho que intente comprender, se me escapa por todas partes, porque es un mundo que simplemente no vemos, que tenemos que imaginar, y por eso están estos tres caballeros conmigo, que les aseguro que, si de algo saben, es de esta materia. Me lo acaban de demostrar en las sucesivas conversaciones que hemos mantenido y les puedo confirmar que va a resultar muy ilustrativo para todos nosotros lo que nos van a contar sobre la seguridad y cómo proveer a esa seguridad, y sobre la colaboración, absolutamente necesaria, como les decía, que debe existir entre administraciones y empresas.

Los presento por el orden en el que van a intervenir. El Teniente Coronel de la Guardia Civil Fernando José Sánchez, director del Centro Nacional para la Protección de Infraestructuras Críticas; José Antonio Gómez Bule, presidente de S21sec, la empresa decana de seguridad en España –llevan quince años trabajando en este sector y, entre otras cosas, tienen muchísimas cosas que aportarnos respecto a cómo colabora una empresa de seguridad privada con todo el ámbito de las administraciones públicas–; y el Teniente Coronel Luis Hernández, Jefe del Área de Ciberseguridad de la Guardia Civil, un cuerpo que, creo, Teniente Coronel, que está en la avanzada, en la punta de lanza, de la ciberseguridad.

Volviendo al tema que nos va a ocupar a partir de ahora, «Sumandos para la inteligencia», ¿qué significa esto? Hablamos de una materia transversal en el que colaboran diferentes sectores, ya les digo, públicos y privados. Pero ¿cómo compatibilizar, cómo armonizar todo esto? Hay muchas preguntas que se nos plantean en este ámbito. Por ejemplo, ¿pueden las administraciones competir con la amenaza que suponen los *hackers*? ¿Nece-

sitan la colaboración de los que invierten a diario en desarrollar antídotos contra estos ataques? O, por ejemplo, ¿cómo la empresa privada puede asegurar a la administración pública que el trabajo que va a desarrollar es absolutamente fiable y seguro? Todas estas cuestiones vamos a tratar de irlas desarrollando a partir de ahora, y se me ocurre empezar por preguntar al Teniente Coronel Sánchez cuál es la estrategia que se viene desarrollando para que todos sus sistemas tengan una seguridad fiable. Si quiere podemos empezar por ahí.

TENIENTE CORONEL DE LA GUARDIA CIVIL
FERNANDO JOSÉ SÁNCHEZ
Director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)

Es un placer estar en este magnífico marco dirigiéndome a ustedes y, además, creo que es muy acertado, muy procedente, el título de esta charla, de esta mesa. Estamos hablando del concepto de colaboración público-privada, que al fin y al cabo es de lo que se trata de eso, del concepto de *public-private partnership*, que surge hace algo más de diez años, un poquito antes del 11-S; ya sabemos que, cuando hablamos de seguridad, por desgracia, siempre hay que empezar con ese hito histórico. Este concepto es eminentemente anglosajón pero hace referencia a una necesidad indiscutible hoy en día en el marco de la seguridad. Y es que la seguridad está cambiando. Las amenazas están cambiando y estamos viendo que las ciberamenazas van en crecimiento. Internet no fue configurado –hace ya varias décadas– como un espacio seguro, sino como un espacio para intercambiar ideas e información. No tiene parámetros de seguridad y eso, lógicamente, es algo que el delincuente, el terrorista o el espía, aprovechan. El concepto de colaboración público-privada, como digo, precede incluso al 11-S, pero a partir de ahí los gobiernos de nuestro entorno nos hemos empezado a dar cuenta de un axioma que es

cada vez más claro, que es que la seguridad, incluso la defensa de un país, no depende, como hace varias décadas, exclusivamente de tener unas potentes Fuerzas Armadas, unas Fuerzas y Cuerpos de Seguridad robustos y un adecuado servicio de inteligencia. La seguridad de un país depende, en muy buena medida, de los ciudadanos. Por eso hay que involucrar a los ciudadanos y por eso, lógicamente, las empresas también son parte de ese esquema. Como apunte, y para reforzar esto, decir que el 80% de nuestras infraestructuras críticas están en manos del sector privado. Por tanto, ahora mismo, nos estamos enfrentando a una realidad en la cual tenemos nuevas amenazas –asimétricas además– en las que, sin colaboración con nuestras empresas y con nuestros ciudadanos, no se podrá garantizar esa seguridad. Por tanto, es necesario involucrarlos.

Hace un rato el General Sanz Roldán hablaba de abrir la llave del gas o abrir la llave del grifo y ésa es, quizás, la base del concepto de protección de infraestructuras críticas. Es decir, estamos todos acostumbrados a darle a un interruptor y a que se encienda la luz, a abrir la manija del lavabo y que salga agua, a coger el cercanías o hablar por teléfono. Es decir, que todo esto está sustentado por una serie de infraestructuras. Y detrás de esto hay otra serie, una cadena de distribución. Esas infraestructuras son las que proporcionan esos servicios y esos servicios nos condicionan a todos, incluidas las administraciones públicas y las empresas. Es inimaginable que una empresa no tenga acceso a Internet, que no depenga de Internet, de las telecomunicaciones, de la energía eléctrica. Por lo tanto, somos rehenes de esos servicios esenciales. Nos dan una gran calidad de vida, pero eso está sustentado por infraestructuras y los que nos quieren atacar, lógicamente, tienen el punto de vista puesto en esas infraestructuras, porque es el eslabón más débil, que es la propia sociedad, que somos nosotros. También decía el General que un ciudadano no entiende que en un momento determinado nos quedemos sin fluido eléctrico o se nos vaya el televisor o se nos vaya la co-

bertura de Internet. A los cinco minutos ya estamos buscando culpables, y el culpable suele ser el Gobierno. Pero en muchos casos no sabemos que esos servicios son proporcionados, precisamente, por infraestructuras que en la mayor parte de los casos están dirigidas por operadores privados. Y ésa es una de las razones por las que, desde hace ya varios años, llevamos trabando para afianzar esa colaboración público-privada.

En el caso del centro que dirijo, el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), podemos presentar un modelo de éxito, porque tenemos ya esa colaboración público-privada en materia de seguridad de las instalaciones y de los activos que tienen esas instalaciones. Eso es ya un hecho, un hecho palpable. Tenemos una legislación al respecto y tenemos una concienciación alta de estas empresas, de estos operadores críticos. Y una rama de esto, de las infraestructuras críticas, es lógicamente también la ciberseguridad. Está todo perfectamente engarzado y perfectamente definido. Entonces, esta situación va madurando. Por ejemplo, la semana que viene se van a nombrar 37 operadores críticos que tienen una serie de obligaciones y también una involucración muy importante en la seguridad nacional, de forma que tienen voz y voto en una serie de foros y colaboran de forma íntima con el Ministerio de Interior, que, en este caso, es el competente en materia de protección de infraestructuras críticas. En ese ámbito, la protección de infraestructuras críticas lleva unos años de ventaja a este fenómeno –llamémoslo así–, porque los que trabajan, o trabajamos, en ello, en la ciberseguridad, ya llevamos muchos años en esto. Aunque también es verdad que el fenómeno de la ciberseguridad, o de las ciberamenazas, es algo que ha eclosionado algo más tarde desde el punto de vista de opinión pública. Pero estaba ahí hace mucho más tiempo, aunque ahora mismo resulte mucho más palpable que un ciberdelincuente, un ciberespía o un ciberterrorista nos puede golpear y nos puede hacer daño de múltiples maneras. Lógicamente, de forma económica, robando

información o, por ejemplo, mediante un ataque a nuestras infraestructuras críticas.

¿Cómo se está reaccionando en este sentido? Como digo, se están implantando una serie de medidas por parte de las instituciones públicas y creo que en los dos últimos años, desde que la Estrategia de Seguridad Nacional fue aprobada, se están viendo ya los resultados. Tenemos una Estrategia de Ciberseguridad Nacional donde se marca como objetivo claro la cooperación público-privada en ocho líneas de acción diferentes. Las empresas proveedoras de servicios de telecomunicaciones o de Internet, los operadores de infraestructuras críticas y las empresas en general tienen una participación en todo este ámbito. Una muestra puede ser, por ejemplo, la reciente proclamación del rey Felipe VI, en la que se puso por primera vez en marcha un operativo de ciberseguridad en relación a un evento concreto. Se movilizaron capacidades tecnológicas de unos elementos técnicos que se llaman CERT (Computer Emergency Response Team); perdónenme por los acrónimos y por tanto inglés, pero en ciberseguridad es el idioma que se maneja. Estos CERTs son muy limitados a nivel nacional y digamos que tienen unas misiones muy concretas a la hora de analizar, prevenir, mitigar y responder a un ciberataque. Se puso pues en marcha un dispositivo con el CERT de Seguridad e Industria de León, con la Oficina de Coordinación Cibernética del Ministerio del Interior y con las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad, pero, en buena parte, el éxito radicó en el contacto que tuvimos también con las grandes empresas de telefonía o proveedores de servicios de Internet y de telecomunicaciones, que nos pudieran ir alertando de situaciones que se pudieran ir desarrollando en la red, en fuentes abiertas. Se trata de un concepto que también abordó el General en su intervención anterior, que es el del intercambio de información. Y el intercambio de información a este nivel sólo se puede conseguir con dos preceptos: confianza mutua, es decir, que nos fiemos el uno del otro, la empresa y la administración pública, que sea

simbiótico, que se obtenga algo a cambio; y, segundo, confidencialidad, es decir, que nosotros nos tenemos que obligar a que los datos, la información que nos pueden aportar esas empresas, esos ciudadanos, lógicamente tienen que ser confidenciales, porque en muchos casos son sensibles, son estructurales para la marcha de la empresa. Con esa información sí que estamos en condiciones de hacer una inteligencia en la cual nuestras unidades de Guardia Civil y de Policía, o los propios operadores, las propias empresas u otros CERTs, pueden explotar esa información para anticiparse a un evento negativo desde el punto de vista de la ciberseguridad o, digamos, reaccionar o mitigar este efecto. Básicamente éste es el esquema que yo quiero plantear, aunque la colaboración público-privada no es fácil; llevamos siete años trabajando con una serie de empresas de primer nivel y lo más difícil es siempre obtener esa confianza. Pero una vez que se consigue la confianza, esa colaboración sí que es factible y ése es el caso de éxito que estamos presenciando y que se puede extrapolar al ámbito de la ciberseguridad, pues se trata de confiar los unos en los otros, de que la parte privada sea partícipe de la seguridad nacional. Tenemos, como ciudadanos y como empresas, mucho que aportar a la seguridad nacional. No es una cuestión sólo de policías y de Guardias Civiles y Fuerzas Armadas. Es una cuestión mucho más amplia, una labor de concienciación que se logra gota a gota, de difusión de mensajes y, sobre todo, de confianza y de intercambio de información.

ALBERTO RUBIO
Moderador

Muchas gracias. Vamos a pasar a un ámbito más operativo, si le parece al Teniente Coronel Luis Hernández, que, como les decía antes, es jefe del Área de Ciberseguridad de la Guardia Civil y que nos va a contar precisamente cómo funciona –si me permiten la expresión– un «ciberpoli».

TENIENTE CORONEL DE LA GUARDIA CIVIL
LUIS HERNÁNDEZ
Jefe del Área de Ciberseguridad de la Guardia Civil

Lo primero que pretendo es intentar reforzar algunas de las ideas que ya han expresado algunos ponentes que me han precedido, clarificar algunos puntos y, luego, someterme al duro debate. A ver cómo salimos de él. Intentaré no repetir conceptos, pero sí reforzarlos en lo posible. El primer concepto fundamental es que estamos hablando de ciberamenazas, del concepto de ciberseguridad. Simplemente una pequeña reflexión sobre los nuevos retos, sobre las ciberamenazas del siglo XXI. En toda la documentación que se está generando en los últimos años, todas las directrices, instrucciones, normas, acuerdos, etcétera, siempre está presente esta palabra: «ciberamenaza». La ciberamenaza hay que considerarla como una amenaza transversal. Está presente en la Estrategia Europea de Ciberseguridad, está presente en la Estrategia Nacional de Seguridad y también está presente en las dos estrategias de segundo nivel que el Gobierno ha aprobado: la de ciberseguridad, que da pie a estas jornadas, y la de seguridad marítima, donde también se contemplan las ciberamenazas. No soy adivino ni pretendo serlo, pero seguro que vamos a ir viendo que la ciberamenaza va a aparecer como tal en las nuevas estrategias sectoriales que se aprueben en el futuro.

También se ha hablado aquí de los agentes, o los actuantes, concretando un poco más las amenazas. Se pueden resumir o se vienen resumiendo en cinco, básicamente: ciberterrorismo, hacktivismo, ciberespionaje, ciberdelito y ciberguerra. Bueno, pues, lógicamente, desde los distintos ámbitos de la administración se trabaja contra todas esas amenazas. Pero el hecho de que sea una amenaza transversal implica que también deba ser transversal la manera de combatirla. ¿Eso qué quiere decir? Pues, por ejemplo, el ciberterrorismo cae plenamente en el ámbito competencial de los Cuerpos de Seguridad del Estado. Y el *hacktivismo* también.

¿El ciberdelito? Ni que decir tiene. ¿Y el ciberespionaje? Ahí hay una responsabilidad compartida entre el Centro Nacional de Inteligencia y el Centro Nacional de Protección de Infraestructuras Críticas, porque ¿qué es lo que se espía? Básicamente, al menos en nuestro país, se espía el ámbito empresarial. ¿Quién tiene la responsabilidad de proteger o apoyar en la protección de los activos empresariales? El Centro Nacional de Protección de Infraestructuras Críticas, en tanto en cuanto una gran parte, o la parte más sensible, del entramado empresarial a su vez forma parte de las infraestructuras críticas, tanto nacionales como europeas. Y luego está el concepto de ciberguerra, del que hablaré más adelante. Pero, en definitiva, lo que les quería trasladar es que todos colaboramos en todo; estamos presentes e intentamos interactuar con ese entorno del ciberespacio, que en unos aspectos es muy bueno, muy positivo, una oportunidad desde el punto de vista social, económico, cultural, pero que también es el punto débil de todo este entramado.

Ya se ha hablado aquí bastante de ciberterrorismo, algo que se entiende normalmente como el uso de Internet, y de las tecnologías asociadas, por parte de las organizaciones terroristas, aunque sin descartar que los terroristas ataquen las infraestructuras de Internet como objetivo de una acción ilícita. A mí sólo me cabe certificar que eso es así, pues ésa es la experiencia que arrastramos los Cuerpos de Seguridad del Estado desde hace muchos años.

En el último año y medio ha habido una eclosión de todo el concepto de ciberseguridad. El año pasado fue tremendo. Empezamos con la aprobación de la Estrategia Europea de Ciberseguridad a principios de años; a mediados de año se aprobó la Estrategia Nacional de Seguridad; y a finales de año se aprobaron la de Ciberseguridad y la de Seguridad Marítima. Dirán que por qué ahora habla todo el mundo de seguridad y ciberseguridad. Ahora se está dando más visibilidad al problema, pero, en el caso concreto de Guardia Civil, todo el equipo humano y los

medios técnicos de los que nos hemos dotado para intentar contribuir a este esfuerzo colectivo de protección vienen del año 2000. En el plan estratégico de lucha contra el terrorista de la Dirección General de la Guardia Civil del año 2000 ya se establecía la necesidad de crear unidades especializadas para la lucha contra las nuevas amenazas en Internet. Y en el año 2002, para ser exactos, en noviembre del 2002, incorporamos los primeros efectivos humanos para conformar lo que ahora es el Área Técnica de la Jefatura de Información, que, entre otras muchas cosas, atiende a la amenaza ciberterrorista. ¿Qué quiero decirles con esto? Que aquí no hay una improvisación, que esto no un: «Bueno, pues ahora es el tema de moda, así que vamos a organizarnos». No. Aquí ha habido un trabajo continuo, y no sólo de los cuerpos de seguridad. Véase si no la propia Secretaría de Estado, el Centro Nacional de Inteligencia, que conformó el Centro Criptológico Nacional. Esto es algo que se ha ido madurando a lo largo de años. Ahora estamos viendo la eclosión, pero ha habido un trabajo previo importante.

¿Cuáles son las misiones fundamentales del Servicio de Información de la Guardia Civil? Pues son la lucha contra el terrorismo, la lucha contra formas de delincuencia especialmente graves y la lucha contra movimientos de desestabilización y subversión del ordenamiento constitucional. Lo cierto es que tenemos ya una dilatada trayectoria realizando estas funciones. Pero, concretando un poco, ¿cuál es el trabajo que desarrollamos en las unidades de investigación tecnológica? Bueno, pues, como pueden imaginarse, consiste en pelear contra este enemigo difuso, disperso, extraño, que no se ve, que es intangible, pero que está ahí. ¿Cómo lo hacemos? Quizás me repito un poco, porque el General Sanz Roldán ya ha hecho alguna alusión a ello. Lo hacemos fundamentalmente a base de dedicación e ilusión. Todo el personal que integra las unidades –las unidades de la Guardia Civil, las unidades de investigación en el ámbito de la Jefatura de Información y, en el caso que a mí más me afecta, las

unidades de investigación tecnológica– es personal voluntario, con una altísima motivación; para ellos no existe el reloj, no existen los horarios. Gracias a ello, y a pesar de la crisis, a pesar de que –como también se ha dicho aquí– hemos sufrido los recortes de la crisis, no se ha bajado la guardia en lo que es el trabajo, sino más bien lo contrario. Y a esa dedicación hay que unirle una muy alta capacitación técnica, pues hacemos un proceso de selección muy riguroso y luego nos preocupamos constantemente de proporcionar una formación continua. Trabajamos a nivel nacional y también fuera de España. La colaboración es fundamental. Nuestro trabajo no se entiende sin la franca y leal colaboración con otros cuerpos de seguridad, con el Centro Nacional de Inteligencia, con la Secretaría de Estado de Seguridad, con el mundo de la defensa y, por supuesto, con otros actores a nivel internacional. Participamos muy activamente en grupos de trabajo, en equipos conjuntos y en grupos de estudio en Europol, en Interpol, en un montón de organismos internacionales.

Volviendo un momento a la estrategia de ciberseguridad, quería hacer dos apuntes. El primero es sobre la Estrategia Europea de Ciberseguridad, que marca un principio: el principio fundamental de la Estrategia Europea de Ciberseguridad es defender los valores esenciales de la Unión Europea, tanto en el mundo físico como en el digital. Hay que recordar los tres objetivos fundamentales, o los tres desafíos fundamentales, que desde la Secretaría de Estado de Seguridad se plantean ante el reto de la ciberseguridad; algo que además he tenido oportunidad de leer en el libro que la Asociación de Periodistas Europeos ha publicado con las sesiones del seminario del año pasado. El secretario de Estado de Seguridad realizó en este mismo escenario una ponencia el año pasado en la que ya habló, entre otras cosas, de ciberseguridad. Sus palabras están en el libro, pero también las he oído en otro tipo de reuniones, incluso en reuniones internas de coordinación, porque respecto a esto hay una directriz muy clara. ¿Cuál es pues la triple vertiente de la ciberseguridad?

Primero, lógicamente, proporcionar seguridad en el ciberespacio; parece lógico. Segundo, y fundamental, hacer todo con un escrupuloso respeto a los principios de privacidad y seguridad del ciudadano. Ni que decir tiene que todas las actuaciones de los cuerpos de seguridad están regidas por el ordenamiento legal vigente y por la figura del juez instructor, que a veces pasa desapercibida pero que en realidad funciona como un juez de garantías, porque es el que vela porque las actuaciones de los cuerpos policiales se ajusten a un principio de racionalidad, proporcionalidad y oportunidad. Y, por último, y no menos importante, mantener el ciberespacio libre para que pueda desarrollarse, expandirse y crecer, consolidando el dinamismo que en lo social, en lo económico y en lo político nos están facilitando Internet y las nuevas tecnologías.

Ya para terminar, quisiera complementar la respuesta que el Jefe del Estado Mayor de la Defensa dio ayer al señor Enrique Peris sobre la cooperación entre defensa, interior, sector privado, etcétera. Quiero incidir en ello porque realmente es así. El General decía que había una franca y leal colaboración y yo doy fe de ello. En concreto, nuestra unidad lleva participando de forma activa en los ejercicios nacionales de ciberdefensa desde el 2008 o el 2009 –no recuerdo la fecha exacta–. Hemos participado en todos los que ha habido. Y hemos participado también activamente apoyando al equipo nacional conformado por el Ministerio de Defensa en los ejercicios de ciberdefensa que la OTAN organiza desde el Centro de Excelencia de Ciberseguridad de Tallín. Y todo esto antes de que existieran el Mando de Ciberdefensa OTAN, el Centro Nacional de Protección de Infraestructuras Críticas o el Centro Criptológico Nacional. Como anécdota puedo decirles que, cuando el General Medina tomó posesión de su cargo como jefe del recién creado Mando de Ciberdefensa, estábamos enfrascados en el segundo ejercicio de ciberdefensa de la OTAN. Yo tuve la oportunidad de saludarle en la anterior sede, antes de que se fueran a su ubicación actual, y, lógicamente, allí estábamos pre-

sentes todos los actores. En los ejercicios que ha habido en el ámbito militar, el Ministerio del Interior y los cuerpos de policía y Guardia Civil hemos estado muy implicados, y en los ejercicios de ámbito civil que lidera el Ministerio del Interior también hay una importante colaboración del Ministerio de Defensa.

ALBERTO RUBIO
Moderador

Vamos ahora a atar el cabo de la empresa privada. Hasta ahora hemos hablado de las administraciones públicas, hemos visto cuál es la estrategia que mantienen las administraciones públicas y cómo actúa la administración pública en defensa de sus intereses, cómo hace las funciones de policía en el ciberespacio. Vamos a ver ahora como colabora la empresa privada en todo esto. Sabemos que la ciberseguridad es un tema transversal: nos comentaba antes el Teniente Coronel Fernando Sánchez que el 80% de los sistemas de la administración pública están en manos privadas. Precisamente para hablarnos de ese 80% tenemos aquí a Juan Antonio Gómez Bule, que es el presidente de S21sec, una empresa privada que lleva quince años trabajando en este sector, por lo que es la decana de las empresas españolas que trabajan en este ámbito, además de una de las cinco principales empresas de seguridad en todo el mundo. Estoy seguro de que nos podrá aportar mucho respecto a cómo debe actuar una empresa de seguridad privada, si se debe limitar simplemente a aportar sistemas, es decir, a ser un proveedor, cobrar por su trabajo y continuar con otra cosa, o si debe implicarse mucho más en todo lo que significa la seguridad.

JUAN ANTONIO GÓMEZ BULE
Presidente de S21sec

La ciberseguridad no es sólo un elemento tecnológico. Quien se quede en la parte tecnológica se queda muy lejos de lo que es su

verdadera razón de ser, la realidad del entorno. Llevo treinta años trabajando en modelos de cambio social, introducción de tecnologías, identificación de los nuevos modelos sociales y entornos de entendimiento del comportamiento humano. Y llevo veinte años trabajando en los modelos de Internet. Estoy seguro de que tanto Luis como Fernando, desde la salida de la academia, ya estaban metidos en este determinado entorno, que es como comprendemos la realidad en el sector, con una determinada vocación que hace que esta aproximación sea conjunta.

¿Cómo somos capaces de poder tener un determinado entorno de certidumbre a la hora de gestionar, informar y recopilar los datos? Internet es una alegoría de la vida, y tenemos que ser capaces de sobrevivir en ella. Se trata de un entono de difusión en el que emerge una realidad social y una realidad que está muy enraizada con los conceptos de seguridad nacional, una seguridad para todos, una obligación para todos, donde todos tenemos que ser capaces de aportar los conceptos tradicionales y los nuevos conceptos que tienen que ver con la percepción de seguridad de nuestro Estado. Y la percepción de seguridad de nuestro Estado tiene que ver también con tener una capacidad disuasoria creíble, a la vez que se defienden los intereses estratégicos, uno de los cuales es el desarrollo tecnológico, que a su vez tiene que ver con el I+D, que es necesario de impulsar en un modelo parecido al norteamericano o al israelí.

Respecto a la Estrategia Europea de Ciberseguridad, como bien comentaba Luis hay dos temas. Uno es la ciberresistencia, es decir, cómo somos capaces, una vez que tenemos un ataque, de volver a tener nuestras infraestructuras, nuestras capacidades, de nuevo en sentido de partida; aunque el sentido de partida siempre es distinto, porque nada vuelve nunca atrás. Se trata de una forma muy elástica de poder entender la realidad. Es la elasticidad del combate diario. Y la elasticidad del combate implica que, desde hace cierto tiempo, puedas tener una estrategia operativa, táctica y de operaciones estratégicas. Y no una estrategia

de salón, pues al final tienes que defender una serie de infraestructuras que tienen mucho que ver con la generación y el entendimiento de los conflictos. El entendimiento de los conflictos, de enfrentamientos que muchas veces no entendemos, que son polimórficos, asimétricos, nos tiene que llevar a desaprender muchas de las antiguas formas de entender nuestra realidad. Eso es algo importante desde el punto de vista de la tecnología de la ciberseguridad. Tenemos que entender la realidad social, ser capaces de modificar unas estructuras burocráticas organizadas que se resisten al cambio, de adaptarnos a una realidad social que está gestionada en tiempo real, en nanosegundos, cuando nuestras típicas estructuras se movían en unos espacios-tiempos que no tienen nada que ver con la realidad actual. Eso es necesario para poder entender el cambio y ser capaces de transformarnos. Una cultura sistémica permite que, desde las Fuerzas y Cuerpos de Seguridad del Estado, y en concreto el entorno de transformación del Ministerio de Defensa, seamos capaces de poder orientar una nueva formación, una nueva elasticidad a la hora de gestionar y entender dónde están los terrenos de batalla, los teóricos y los prácticos.

Si hacemos una asimilación sin restricciones de la doctrina de la guerra –ayer hablábamos de guerras irregulares, de guerra de guerrillas– nos encontramos con que la guerra sin restricciones lleva la guerra a un entorno que no es el tradicional campo de batalla. Y eso es algo que afecta a todo: guerra mediática, guerra de comunicación, guerra de Internet, guerra de subversión de intereses. Todo eso tiene que ver con una plataforma tecnológica que transmite una serie de conocimientos. Hoy comentaba el General Sanz Roldán cuáles son las nuevas aproximaciones al concepto de la formación de los analistas de inteligencia. Yo, que tengo que dar clase a los analistas, sé que formar a un analista no es fácil. Y, además, un analista no se sustituye. La tecnología es una herramienta. De lo que sí somos capaces es de eliminar en un momento concreto la intoxicación de informa-

ción, la desinformación, el desbrozamiento de la información, y hacer que el trabajo del analista sea el que realmente tiene que ser. Podemos hacer un informe que realmente sirva para tomar una decisión, pero ese informe obliga al analista a tener una capacidad de abstracción importante, además de una capacidad de entendimiento, pues hay determinadas ideas incrustadas en nuestro inconsciente que hacen que seamos capaces de entender la realidad de una determinada forma.

Eso es la segunda y la tercera derivada de lo que es el entendimiento social, el a dónde vamos, lo que realmente existe. Es decir, hay que ver más allá de las evidencias y, desde la tecnología, desde la ciberinteligencia, hay que entender que esto no es solamente un fenómeno episódico, sino que es un fenómeno de transformación. Ese fenómeno de transformación aparece bajo distintas manifestaciones, como son las ciberamenazas, que hacen referencia específica a lo que tiene que ver con la competencia del Ministerio del Interior a través de Centro Nacional de Protección de Infraestructuras Críticas; esto tiene que ver fundamentalmente con el entorno de infraestructuras y con la protección de los ciudadanos. La defensa de infraestructuras críticas y estratégicas es parte del derecho y la obligación del Estado a defender un concepto de soberanía nacional que, explicado y estructurado en la Estrategia de Seguridad Nacional, establece una serie de amenazas, una serie de defensas y una serie de capacidades para darnos cuenta de cuáles son. Tomar conciencia, darse cuenta de las cosas, es fundamental.

En cuanto a lo que comentabas antes Alberto sobre los niveles de compromiso, hay que destacar tres palabras: *trust*, o confianza; *knowledge*, o conocimiento; y *commitment*, o compromiso. Lo cierto es que muchas veces no se ha entendido ni el *trust* ni el *knowledge* ni el *commitment*, pero ahora mismo esos tres conceptos forman parte de la columna vertebral de lo que es el concepto de la seguridad nacional. Un concepto que, además, es un concepto evolutivo, un concepto de corresponsabilidad, un

concepto en el que la parte pública y la parte privada tienen que trabajar juntas, y un concepto en el que nosotros llevamos trabajando muchos, muchos años. Sirva como ejemplo que desde la Secretaría de Estado de Seguridad, con la colaboración de la Guardia Civil, del Cuerpo Nacional de Policía, de la universidad y de nuestra compañía, hemos desarrollado y mantenemos una línea de colaboración que se traslada en Europol.

Les pongo dos ejemplos más. Por un lado estamos colaborando con Everis en el desarrollo de la agenda europea de ciberdefensa. Y también está el proyecto que se denomina CAMINO, un proyecto en el que, al amparo de la Unión Europea, queremos generar un *think tank* que nos permita desarrollar nuevas capacidades. Porque una cosa es saber cómo son las cosas y otra es comunicarlas. En lo que es la parte del entorno de la comunicación, creo que es fundamental que todos los que estamos aquí, incluidos los que os dedicáis al periodismo, a la comunicación, seamos capaces de poder identificar y comunicar de una forma adecuada, de generar los espacios de colaboración adecuados para poder transformar todo esto en una ventaja competitiva para nuestro país.

Para resumir, ley de Acción Exterior del Estado; ley de Protección de Infraestructuras Críticas; sistema de Inteligencia Económica para España; Estrategia de Seguridad Nacional; Estrategia Nacional de Ciberseguridad; Estrategia de Seguridad Marítima; proyectos de colaboración... Todo eso genera una infraestructura de confianza, que es, bajo mi punto de vista, donde tenemos que colaborar, como venimos haciéndolo desde hace ya catorce o quince años.

ALBERTO RUBIO
Moderador

Gracias José Antonio. ¿Cómo has dicho que se llama el último proyecto?

JUAN ANTONIO GÓMEZ BULE
Presidente de S21sec

El proyecto se llama CAMINO, pero no recuerdo a qué corresponden las iniciales. Es un proyecto que presentamos a Europa porque somos conscientes de que hay que transformar determinados entornos, de que hay que comunicar. Hace años, cuando comunicábamos la necesidad de la protección de las infraestructuras críticas, ni la parte política ni la parte pública ni la parte empresarial eran capaces de entender hasta qué punto era crucial. Ahora ya hay mucha gente que lo entiende, por el hecho de la comunicación, del trabajo de la Secretaría de Estado y de todo lo que tiene que ver con esa labor de concienciación, divulgación y diseminación. Sin ir más lejos, yo presido la Comisión de Desarrollo de la Conciencia Nacional de Ciberseguridad y Ciberdefensa. Es una tarea en la que tenemos que participar todos.

ALBERTO RUBIO
Moderador

A continuación vamos con el turno de preguntas Previamente, yo quisiera hacerle una pregunta al Teniente Coronel Sánchez. ¿Considera usted que las administraciones públicas invierten lo suficiente en ciberseguridad, teniendo en cuenta también los tiempos de crisis que corren? ¿Estamos en ese nivel en el que podemos darnos por satisfechos respecto a lo que, digamos, gastamos como administración pública para mantener la seguridad?

TENIENTE CORONEL DE LA GUARDIA CIVIL
FERNANDO JOSÉ SÁNCHEZ
Director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)

Esa pregunta tiene un poquito de truco, ¿no? Desde el punto de vista operativo, evidentemente siempre queremos más. Y en eso

coincidiría cualquiera de mis compañeros. Siempre nos parece poco lo que recibimos. Pero también es verdad que se está haciendo un esfuerzo notable, sobre todo desde que la Estrategia de Ciberseguridad ha visto la luz. Se ha estado haciendo un esfuerzo muy importante en presupuestos, en personal y en formación por parte de la administración pública. Pero, claro, siempre hace falta más. Estamos en buen camino –no sólo nosotros, sino la mayoría de países– y, evidentemente, esto va a ir creciendo, porque la necesidad obliga a ello; vemos cada día cómo nos va invadiendo esta terminología cibernética. La respuesta, pues, sería que sí se está invirtiendo, aunque siempre hace falta más. Pero yo creo que vamos en el buen camino.

JESÚS ALFARO
Director de Comunicación de Navantia en Cádiz

Muchas gracias a todos por vuestras intervenciones. A mí la única preocupación que me producen estas ciberamenazas, el ciberterrorismo, la ciberdelincuencia, es la multiplicidad de instituciones públicas que se ocupan de ello. ¿No creéis, desde el punto de vista técnico, que eso puede distorsionar los resultados, aunque exista una coordinación evidente, que habéis resaltado todos y cada uno de vosotros? ¿No creéis que esa obsesiva pluralidad y diversificación puede ser perjudicial en ese mundo tan complejo y tan delicado del ciberespacio, en el que los delincuentes, en su sentido más genérico, van por delante del Estado? Eso por un lado. Y después quería enlazar otro tema con lo que decía Juan Antonio Gómez Bule. ¿Cómo se logra aumentar esa sensación de seguridad de la ciudadanía, del ciudadano medio, que no conoce los entresijos de este tema? ¿Qué papel pueden jugar los periodistas y los medios de comunicación en lo relativo a estos retos tan inmensos que tiene la sociedad –no sólo la española, sino la sociedad mundial–, en lo relativo a ese acoso cibernético que puede causar desastres tan importantes?

TENIENTE CORONEL DE LA GUARDIA CIVIL
FERNANDO JOSÉ SÁNCHEZ
Director del Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC)

Voy a ser breve en ambas respuestas, porque creo que mis compañeros también pueden complementarlas. Sobre la primera pregunta, ¿quién es competente para la defensa nacional? ¿Quién está preparado? ¿Quién tiene los recursos necesarios para la defensa nacional? Está la delincuencia, el terrorismo, la información, el espionaje, la protección de infraestructuras críticas... Al final, no dejamos de ser los mismos órganos con un planteamiento dirigido hacia el ciberespacio. O sea, estamos ante un mundo complejo, que es un mundo virtual, pero que se solapa al real. Por lo tanto, el escenario es el mismo que el real, pero en lo virtual, y los enemigos, los atacantes, los delincuentes, son los mismos, sólo que con una capa virtual. Por lo tanto, la respuesta es clara. Depende de Defensa, depende de Interior, depende del CNI... Es decir, seguimos siendo los mismos, sólo que tiene que organizarse a nivel técnico y tiene que complementarse y coordinarse. Es más una cuestión de rodaje inicial que un problema real. Basta con quitar el término «cíber» y todo queda mucho más claro.

Respecto a la segunda pregunta, la relativa al papel de los medios en esto, me parece crucial. Tienen un papel fundamental. No debemos pasar de un estado de feliz ignorancia, que es el que podíamos tener hace pocos años, cuando tanto el ciudadano como muchos altos ejecutivos o altos dirigentes no consideraban las ciberamenazas como algo plausible, o como algo peligroso, al polo opuesto, a pensar que estamos prácticamente en un estado de sitio y que todo son peligros. Y la labor de ustedes ahí es crucial. Tenemos que poder transmitir la necesidad de la implicación ciudadana y de nuestras empresas, o del sector privado, porque se trata de defensa y seguridad nacional, algo que nos

importa a todos. Pero hay que hacerlo sin llegar al paroxismo de parecer que nos están bombardeando continuamente. Ahí tenemos mucho que hacer todos para transmitir ese mensaje correctamente. En el ámbito periodístico, los medios de información son vitales para hacer que el ciudadano de a pie vea que esto es importante, que se tiene que involucrar, que es algo que le afecta directamente, pero sin un alarmismo innecesario.

TENIENTE CORONEL DE LA GUARDIA CIVIL
LUIS HERNÁNDEZ
Jefe del Área de Ciberseguridad de la Guardia Civil

Yo simplemente quería reforzar lo que acaba de comentar Fernando. Se ha planteado que la ciberamenaza es algo complejo. No sólo es algo complejo, sino que es muy complejo. Y, lógicamente, un problema muy complejo no tiene soluciones sencillas. De ahí que la solución a su vez sea compleja. Lo que sí hay es un esfuerzo claro, pues es necesario que todos los actores estemos perfectamente coordinados, de forma que el trabajo que desarrollemos los cuerpos policiales no interfiera con el trabajo que desarrollan las unidades del Ministerio de Defensa, por ejemplo. Estamos perfectamente conectados, nos conocemos todos, hablamos constantemente, nos reunimos con periodicidad, compartimos experiencias y nos ayudamos mutuamente, pero cada uno tenemos muy claro cuál es nuestro ámbito. Como ha dicho Fernando, quítenle el prefijo «cíber» y verán que no es más que la traslación de la realidad a un mundo virtual.

MARTÍN ORTEGA CARCELÉN
Universidad Complutense de Madrid y Real Instituto Elcano

Una pregunta para el Teniente Coronel Hernández sobre la frecuencia de los ciberataques, o de las ciberamenazas. Sobre otras cuestiones relativas a la seguridad, yo he visto tablas, gráficos y

datos sobre cómo han ido evolucionando las frecuencias. Le digo un ejemplo: la piratería en el Índico. Hay unas curvas que nos dicen claramente que, después de unos picos en los años 2008-2009, ahora está disminuyendo. Es decir, que con una panoplia de medidas, incluidas las operaciones contra la piratería, hemos conseguido que descienda la piratería en el Índico. ¿Ocurre algo así con las ciberamenazas o podemos decir, al contrario, que todavía estamos en una curva creciente? Además, usted ha distinguido muchas categorías dentro de las ciberamenazas: la ciberdelincuencia, el ciberhacker, el ciberterrorismo, la ciberguerra... ¿Cómo está evolucionando la frecuencia de las distintas amenazas? ¿Usted diría que durante el tiempo que lleva trabajando en esto han aumentado los ataques? ¿O han descendido? Y qué nos puede decir sobre la realidad de esos ataques.

TENIENTE CORONEL DE LA GUARDIA CIVIL
LUIS HERNÁNDEZ
Jefe del Área de Ciberseguridad de la Guardia Civil

Ayer tuvimos la oportunidad de escuchar a Javier Candau, que es jefe del Área de Ciberseguridad del Centro Nacional de Inteligencia, en este caso del Centro Criptológico Nacional. Él nos daba un dato estadístico muy relevante. Respecto a los años 2013-2014. En el 2013 se habían producido 7.264 incidentes de esta doble categoría y en seis meses de 2014 se habían producido 4.684; su estimación era que al final de 2014 estaríamos bordeando los 10.000 incidentes de este tipo. Yo recuerdo estadísticas de hace escasamente cinco años en los que se hablaba de doscientos incidentes de esta categoría al año. Fíjese. Pasamos de doscientos a más de 7.000 y a una previsión para este año de 10.000. Pregunta en qué momento estamos. La curva es exponencial. El número de incidentes es altísimo.

No puedo concretar la información sobre los incidentes porque no tengo esa información. Lo cierto es que los Cuerpos

de Seguridad sólo trabajamos en aquellos incidentes en los que se abre una investigación judicial y, lógicamente, éstos son los menos. En la mayoría de los incidentes se mitiga el ataque, se contrarresta y se restablecen los sistemas sin necesidad de abrir una investigación, porque no existe capacidad para investigarlo todo. Eso sí se lo puedo decir con rotundidad. Se investigan una mínima parte de los incidentes, en función de la relevancia o trascendencia del incidente en sí o porque las evidencias que quedan del mismo vislumbran que puede haber un canal o una vía de investigación. La mayoría de los incidentes que investigamos, lamentablemente, tienen que ser cerrados en fases muy incipientes de la investigación. ¿Por qué? Pues porque, como decía antes, la cooperación internacional es fundamental para esto. Pero también hay que decir que, aunque la cooperación judicial internacional no es que sea precisamente universal, por ejemplo, en el en el marco de la Unión Europea es muy ágil, muy abierta. Con otros países de nuestro entorno, como pueden ser Estados Unidos, Canadá, también es abierta, pero no es tan ágil; las cosas como son. Y cuando nos vamos a otros entornos más lejanos, por decirlo de alguna forma, la cooperación es ya muy difícil o incluso nula. Por eso es muy, muy complicado hacer una investigación sobre un ciberincidente o sobre un incidente de seguridad tecnológica. Pero, por cerrar la respuesta, decirle que en este momento estamos en plena eclosión. De ahí las medidas que se están adoptando, tanto a nivel nacional como internacional.

JOSÉ ANTONIO GÓMEZ BULE
Presidente de S21sec

Si me permites, Alberto, quería añadir que el modelo de negocio –porque esto es un modelo de negocio y hay que entenderlo como tal– de aquéllos que están al otro lado de la raya no tiene ningún tipo de escrúpulo. Tienen muchos recursos, tienen

muchos medios y esto es un pingüe beneficio para ellos. Ayer comentaba el secretario de Estado de Seguridad las cifras mundiales de todo aquello que es pérdida de una forma directa, de la pérdida censada; pues la total puede ser muchísimo más alta. Para que nos hagamos una idea, las muestras de *malware* que se pueden estar analizando en un laboratorio como el nuestro pueden alcanzar 42.000 casos distintos al día. El año pasado estábamos en una media de aproximadamente 20.000 al día y hace tres años estábamos en 7.000. Eso es algo imposible de gestionar manualmente. Entonces, ¿cómo se actúa frente a ello? Se utiliza la tecnificación, la industrialización, la ingeniería inversa. Y lo que vemos es que cada son mayores los recursos de quienes nos atacan, que quien tiene mucho interés en conseguir un objetivo no repara en gastos; ni en gastos ni en tiempo. Esa definición del modelo estratégico del vector de ataque está clarísima. Hay muchos entornos en los que, como comentaba ayer Javier Candau, hay elementos que quedan durmientes, que quedan ahí a perpetuidad, hasta que tienes que activarlos. Así es como funcionan las amenazas persistentes avanzadas. Contra eso es contra lo que tenemos que ser capaces de luchar. El nivel de madurez y de sofisticación es cada vez mayor. El esfuerzo que hay que hacer para poderlos prevenir y mitigar, y para reaccionar ante ellos, es cada vez mayor. Pero hay muchos frentes y son relevantes una serie de temas, como el anonimato, obviamente, y la ubicuidad. Estamos rompiendo los espacios temporales clásicos y tenemos que ser capaces de adaptar nuestra forma de acción a esos nuevos entornos. Pero, desde luego, lo que sí está claro es que todo esto ha eclosionado y que hay más elemento de gestión. Los ataques están ahí, aunque muchos de ellos no sean comunicados a las Fuerzas y los Cuerpos de Seguridad y éstas sólo actúen y censen los elementos que están comunicados. Pero, claro, lo que no está comunicado obviamente es mucho más.

ALBERTO RUBIO
Moderador

Entiendo entonces que estamos ante una nueva versión de la vieja delincuencia, por decirlo de alguna forma. Hemos cambiado el ámbito en el que nos movemos, pero siguen siendo los mismos delincuentes. Continuamos con las preguntas.

ENRIQUE PERIS
Excorresponsal de TVE en Londres

Escuchando al Teniente Coronel Sánchez, me acordaba de dos películas de Hitchcock, llamadas las dos *Sabotaje*, y pensaba en cuánto puede llegar a desestabilizar la interrupción brusca de un servicio público. Y también me acordaba del libro del agente secreto de Joseph Conrad en el que se basaba esa película. En relación con lo que acabamos de escuchar, me preguntaba cuánto debe gastarse una empresa en «ciberprotegerse», sobre todo en relación con su negocio y en relación con cuánto le costaría el no estar ciberprotegido. ¿Y quién debe pagar o en qué medida deben las empresas privadas contribuir a la protección que le dan los poderes públicos? Por ejemplo esa empresa de zapatos española que de repente descubre con horror que le han robado los diseños. Supongo que esas empresas deberían pagar, aparte de la protección general de los poderes públicos, su propio servicio de protección. Pero, en el caso por ejemplo de una infraestructura crítica, de una empresa de distribución de agua potable o de una empresa eléctrica, un sabotaje causaría un efecto desestabilizador mucho más grave; aparte de que le echarían la culpa al Gobierno, efectivamente. Esa infraestructura crítica goza de la protección especial de un servicio como el que encabeza en este momento el Teniente Coronel Sánchez, pero ¿cómo deben contribuir, cómo se paga todo eso –sobre todo en época de crisis–, en qué medida las empresas tienen que contribuir al gas-

to público en ciberprotección de los servicios y de la vida normal de una ciudad, o de una población, o de un país?

TENIENTE CORONEL DE LA
GUARDIA CIVIL FERNANDO JOSÉ SÁNCHEZ
Director del Centro Nacional para la Protección
de Infraestructuras Críticas (CNPIC)

Las películas de Hitchcock son quizás demasiado alarmistas, pero una película que puede dar indicio de lo que en un futuro puede pasar es *La jungla de cristal IV*, que describe un ciberataque que prácticamente neutraliza todo Estados Unidos; después viene Bruce Willis y, claro, soluciona el tema. También hay un documental que se llama *American Blackout*, emitido por National Geographic, que explica muy bien todo esto –está publicado en la web–, lo que puede pasar cuando cae un servicio, el efecto dominó. El caso es que si nos quedamos sin energía eléctrica, pues eso va arrastrando. Se van las telecomunicaciones, se va el sistema financiero, no puedo pagar con tarjeta, no puedo sacar dinero de un banco, se me paraliza el transporte, no puedo llegar a mi trabajo, si soy enfermero o médico no llego al hospital... Realmente hay que tomar todo esto con cierta cautela para no ser alarmista. La hipótesis del documental es qué pasaría si un ciberataque dejase Estados Unidos sin energía eléctrica durante diez días, algo que es difícil que ocurra hoy en día; digamos que es un escenario futurista. Pero vamos en esa dirección, estamos en el salto éste, y en el futuro un ataque cibernético podría provocar toda esa cascada. Aunque de aquí a que pueda pasar esto nos quedan años, no nos quedan demasiados, porque cada vez estamos poniendo más servicios en red, o en el ámbito de las telecomunicaciones y de Internet. Lo estamos haciendo porque es más cómodo, más rápido, pero el riesgo es que ya no sólo podrán atacarnos en un ámbito físico, sino también cibernético.

Esto me lleva a la segunda pregunta. El concepto de seguridad por el que abogamos desde el Ministerio del Interior, desde el CNPIC concretamente, que es el que impera a nivel global, es un concepto de seguridad integral. Si me pregunta cuánto debería invertir una empresa en ciberseguridad, le contestaría que quite el prefijo «cíber». ¿Qué empresa de primer nivel o qué empresa que quiera proteger sus activos no tiene unas alarmas y unas verjas, no tiene, dependiendo lógicamente de la entidad de esa empresa o de ese activo, personal vigilante de seguridad, no tiene cámaras, no tiene control de acceso? ¿Qué empresa en uso de su razón dejaría prácticamente abierta su fábrica y no pondría ningún tipo de medida física de seguridad? Saltando al ámbito cibernético, que va creciendo cada vez más, y donde efectivamente roban información o pueden neutralizar un sistema y paralizar las máquinas de producción, por ejemplo, nosotros intentamos abrir el campo de visión para que las empresas se den cuenta de que si no invierten en ciberseguridad están haciendo una inversión ruinosa en seguridad, porque es como dejar la ventana abierta y ponerle a la puerta siete candados. Es una cuestión de pura.

En el ámbito de las infraestructuras críticas, la aproximación que hacemos obviamente parte de que si atacan una empresa ya no sólo va a salir perjudicada la propia empresa, sino que el ataque va a perjudicar a los ciudadanos, con todo eso que mencionaba anteriormente de la concatenación de caída de un servicio. ¿Qué se está haciendo desde la Administración? La condición de operador crítico, que es aquel que posee esas infraestructuras críticas, da acceso a información mucho más rigurosa y mucho más confidencial de la situación de las amenazas que puedan existir, de forma permanente, así como a un asesoramiento permanente, también a través del CERT de Seguridad e Industria, y a una emisión de buenas prácticas a través de una serie de guías que estamos emitiendo. Es decir, la empresa también tiene que invertir en su ciberseguridad. Estamos en un concepto mucho más moderno de seguridad, en el cual necesitamos la implicación de la empre-

sa, en el cual necesitamos intercambiar información de forma fluida con la empresa y en el cual nos ponemos a su disposición e incluso, de ser necesario, desplegamos unidades de las Fuerzas y Cuerpos de Seguridad, e incluso de las Fuerzas Armadas, según un escalado que tenemos en los Planes de Protección de Infraestructuras Críticas o en el Plan Nacional Antiterrorista.

PEDRO GONZÁLEZ
Columnista de *ZoomNews*

Mi pregunta es para Juan Antonio Gómez Bule. Quería hablar de la dimensión del negocio de la ciberseguridad. Quizás en la ciberseguridad se haya dado un avance tan exponencial como en los ciberataques e, igual que hace muchos años la policía fichaba al delincuente que era un manitas abriendo cajas fuertes y cerraduras casi imposibles, ahora se trata de fichar a las mejores *hackers*, a las mejores cabezas informáticas. Quisiera abordar este tema del negocio, que evidentemente es un sector económico de unas enormes dimensiones y con una proyección tremenda que puede ilusionar, incluso darle una nueva dimensión y una nueva proyección profesional, a muchas personas.

JUAN ANTONIO GÓMEZ BULE
Presidente de S21sec

Desde luego es un modelo de negocio, aunque es más rentable emprenderlo en Estados Unidos que aquí. ¿Por qué? Porque, si realmente quieres desarrollar capacidades tecnológicas y capacidades humanas, hay que trabajar en un determinado entorno para generar un caladero adecuado de personal. En otras palabras, hay que invertir en las capacidades humanas. Se trata de una línea de inversión de extraordinario calado que tiene que incluir a las compañías que son adquirientes de estos servicios. Estamos intentando concienciar a la sociedad de que la seguridad no es

un gasto, sino una inversión que forma parte de una estrategia. Tomemos el caso de una gran compañía multinacional española dedicada al sector petrolífero. Dicha empresa tiene un presupuesto de alrededor de 46 millones de euros anuales en seguridad. Pero hay agregados una serie de servicios que dan posibilidades no sólo de protección, sino también de anticipación. Volviendo a tu pregunta, éste es un modelo de negocio razonable siempre que esté asociado a las compañías que desarrollamos tecnología. Como decía ayer Francisco López Luque, es necesario un marco de colaboración muy claro para prevenir y desarrollar esas capacidades de I+D. Me refiero a un I+D aplicado, porque normalmente se hace I+D sin llegar a terminar en un producto. En esa línea, ayer nos planteábamos si teníamos suficientes capacidades en España como para tener un *player* global en seguridad y defensa y se comentaba que no tenemos el suficiente tamaño. Pues éste es un problema también de visión y de tamaño. EADS es la única compañía europea que está entre las cincuenta principales compañías globales proveedoras de tecnología de seguridad y defensa. Todo lo demás es no-europeo. Respecto a la estrategia de ciberseguridad, se plantean dos temas. Por un lado, en este momento no tememos capacidades humanas suficientes para repeler un determinado ataque, por lo que hay una línea importante y de desarrollo y formación de capacidades y de desarrollo de puestos de trabajo cualificados en este sector. Por otro lado, no hay tecnología en Europa. Somos tecnológicamente dependientes en materia de seguridad y defensa. Esto es algo que sólo se puede manejar siendo conscientes de que es así, llegando a acuerdos de transferencia tecnológica y cambiando los modelos de innovación. Pero, una vez más, eso no es algo que se improvise de un día para otro. En eso estamos trabajando. Es algo que los que nos hemos dedicado al desarrollo tecnológico hemos sufrido mucho, y seguimos sufriendo. El I+D hay que pagarlo. Lo que vemos nosotros ahora es que al otro lado ganan mucho más dinero del que ganamos nosotros.

9. I+D+i PARA LA CIBERSEGURIDAD

JAVIER MONZÓN
Presidente de Indra

Moderador
MIGUEL ÁNGEL NOCEDA
Periodista de *El País*

Miguel Ángel Noceda y Javier Monzón

MIGUEL ÁNGEL NOCEDA
Moderador

Terminaba la sesión anterior hablando de la ciberseguridad como negocio. Pues bien, ahora Javier Monzón nos hablará de la ciberseguridad desde una perspectiva industrial. Cuando Indra cumplió quince años en el 2008, Javier Monzón, que es su presidente, fundador y hacedor, comentó en un acto ante el rey Juan Carlos y varios ministros que el grupo era el resultado de una gran ambición y que seguía teniendo más futuro que pasado. Seis años después, sigue mirando al futuro, pero también puede mirar al presente. Indra es hoy una realidad, una empresa de la que su presidente puede presumir, y España también, pues es una empresa que aspira a consolidar la tecnología española en el mundo. Indra es líder en tráfico aéreo y ferroviario, en sanidad, en defensa, finanzas, vigilancia de fronteras, sistemas electorales y un largo etcétera. Es un empresón español que puede presumir de aportar a España algo que ningún otro tiene. Ha cumplido el objetivo con el que nació: ser una empresa global tecnológica con un I+D muy desarrollado. Una frase que yo le he oído más de una vez a Javier es que «nuestro ecosistema está donde haya innovación». Es un buen mandamiento para una empresa como ésta. Antes de ser presidente de Indra, Javier Monzón

trabajó en Caja Madrid y fue director financiero y presidente de Telefónica Internacional, así como socio de Arthur Andersen. Sin más preámbulos, paso la palabra a Javier, que tendrá mucho que decirnos sobre la perspectiva industrial

JAVIER MONZÓN
Presidente de Indra

Muchas gracias por invitarme a estar aquí con ustedes. Estoy seguro que todos los asistentes habrán descontado adecuadamente la exageración y el exceso de las palabras de Miguel Ángel Noceda, fruto de la amabilidad debida hacia alguien que se desplaza para compartir este tiempo con ustedes. Yo lo hago encantado. Me gustaría también felicitar a los organizadores, que un año más han elegido un tema muy relevante y han conseguido tratar todos los asuntos y aspectos destacados del mismo con ponentes de gran interés.

Como decía Miguel Ángel, yo voy hacer unas reflexiones que plantearán, como normalmente ocurre en estos casos, más preguntas que respuestas. Porque este mundo de la ciberseguridad todavía tiene muchos ámbitos oscuros, o grises, donde es muy difícil tener claridad en los diagnósticos y recomendaciones. Ustedes saben mejor que yo que hablamos de ciberseguridad desde que hacemos un uso intensivo y generalizado de las tecnologías digitales, ya que a través de las tecnologías se capta, procesa, gestiona, almacena y transmite la información. Y ahora la información se ha convertido en el centro de casi todo. Algunos dicen también que la información es la que define actualmente la superioridad en el mundo de la Defensa. Una vez que la información es el centro de la mayoría de nuestras actividades económicas, sociales y de todo tipo, el concepto de ciberseguridad se sitúa en el centro de nuestras preocupaciones, tanto por la protección de las personas como por la protección de nuestras sociedades. Todos estos procesos digitales, como saben

ustedes bien, implican una mayor vulnerabilidad y un mayor riesgo, porque hay más oportunidades para los delincuentes. Delinquir en el mundo cibernético tiene, en primer lugar, menor coste, porque requiere menos recursos económicos y porque implica menos riesgo para el atacante. En segundo lugar, todo tipo de atacantes tienen espacio para hacerlo, desde particulares hasta grupos organizados de distinto tamaño y condición, y por supuesto también países con intereses específicos industriales, económicos o estratégicos.

Este proceso de digitalización va a seguir; es algo imparable y ya no es cuestionable ni siquiera si lo podemos desacelerar. Al contrario, va a seguir aumentando en intensidad y en alcance. Ya está llegando a todos los ámbitos de la actividad económica y social. Y está llegando mediante un proceso de continuado crecimiento, acelerado y transversal, a través de plataformas y espacios tan transversales como las tecnologías *cloud* o la interconectividad de toda clase de dispositivos y sistemas. Estas formas van a aumentar todavía más los riesgos y la vulnerabilidad de los sistemas. Digo que es un proceso imparable porque nuestras sociedades ya han interiorizado esta nueva forma de gestionar y manejar la información, no sólo desde el punto de vista económico-productivo, sino desde el punto de vista de las relaciones personales y sociales. Por lo tanto esto ya es un proceso que está incorporado al desarrollo y a la forma de ser de las nuevas generaciones y, por tanto, un proceso que no vamos a poder modificar. Esto también ha cambiado el concepto, las herramientas para gestionar y gobernar la seguridad. La seguridad de hace muy poco, de ayer mismo, era una seguridad que todavía estaba concentrada en entornos muy específicos, mientras que ahora la seguridad se tiene que extender a todos los ámbitos de actividad, a los procesos completos de cada uno de estos ámbitos. Antes casi bastaba con proteger los accesos y los puntos sensibles, pero ahora tenemos que proteger el dato, ese dato que captamos, que almacenamos, que procesamos, que comunicamos, que transmiti-

mos y con el que gestionamos todo. El dato en sí mismo es el que va a tener que estar protegido durante todo su recorrido y en todas sus formas y condiciones. Por eso el ciberespacio se ha convertido en el conector de los dominios clásicos que se aplicaban a la seguridad. Incluso, como bien saben en el ámbito de la defensa, el elemento que conecta y que hace común cada vez mas funciones de los tres ejércitos es la ciberdefensa. Esto nos está obligando a redefinir los conceptos de cómo categorizamos la seguridad, nos está obligando a incorporar diferentes y nuevas tecnologías que antes no formaban parte de los ámbitos de seguridad y nos está obligando a definir y a gobernar procesos distintos a los que antes manejábamos en este ámbito.

Saben ustedes mejor que yo que los ataques cibernéticos son cada vez más variados, más sofisticados, más números y que su impacto potencial es cada vez mayor. Aunque no soy partidario de sobrevalorar estos riesgos –pues hay una cierta sobrevaloración en algunos ámbitos–, es cierto que el riesgo es creciente, tanto en la frecuencia en la que se produce como en su materialización efectiva. Y es creciente también en el alcance y en el impacto. Tenemos un reto muy complicado, que es dotar de seguridad a la gran parte de los sistemas en los que hoy se basa esta sociedad de la información. Son sistemas que nacieron y fueron desarrollados sin que la seguridad fuera un requisito prioritario; y a veces es mucho más complejo incorporar un elemento esencial a un sistema ya diseñado que diseñarlo desde el origen con ese requisito incorporado. Esto inevitablemente nos está obligando, y nos va a obligar cada vez más, a ser muy selectivos. Tenemos que reconocer que no todo lo vamos a poder proteger, que, desde luego, no todo lo vamos a poder proteger bien, y que esto va a requerir no sólo una gestión técnica de la seguridad sino una gestión social y política.

En esta actividad hay tres segmentos que me gustaría diferenciar. Son segmentos definidos desde la demanda y, por lo tanto, también de la oferta y del mercado, que se adaptan a esa

definición de la demanda. Hay un segmento de primer orden que a mi juicio es casi únicamente institucional, que es el que constituyen los sistemas complejos de seguridad y los sistemas que se integran en la ciberseguridad, integrados asimismo en los sistemas globales de seguridad y defensa nacionales. Este primer nivel es responsabilidad directa y está gestionado directamente por los gobiernos, pero no aisladamente, sino cada vez más en cooperación entre unos y otros gobiernos. Hay un segundo nivel, que es aquel que tiene que ver con las infraestructuras, los servicios, los procesos y las operaciones críticas para cualquier sistema económico o social. Aquí hay componentes de demanda institucional y hay componentes de demanda privada, normalmente a través de grandes corporaciones. Y hay un último segmento, un tercer nivel donde se aplica la ciberseguridad, que son todos aquellos ámbitos relacionados con el consumo y con las relaciones sociales que principalmente se materializan hoy a través de las redes sociales. Dadas estas características que hemos visto, este crecimiento rápido y acelerado, y el gran volumen que ha alcanzado un mercado que dentro de muy poco va a representar 100.000 millones de dólares, este tercer nivel atrae, como es lógico, a un gran número de actores y jugadores y, además, con una variedad tremenda. Con sectores de origen muy diferentes, algunos vienen de ámbitos específicos o relacionados directamente con la seguridad, pero otros muchos vienen de sectores conexos o de sectores relacionados que comparten características o capacidades que son aplicables al de seguridad. Son pues actores o jugadores de muy distinta base y origen tecnológico: algunos de tecnologías de seguridad que evolucionan, otros de tecnologías puramente, vamos a decir, nativas digitales, que antes se aplicaban en otros sectores y ahora tienen utilidad y virtualidad en éste. Me refiero a compañías de servicio, a compañías de producto, a compañías enfocadas a las redes sociales –no a ámbitos que tenían que ver inicialmente con la seguridad– y a compañías de muy distinto tamaño y características. En to-

das ellas el crecimiento en la ciberseguridad es la obsesión. Se crean un número grandísimo de nuevas compañías y todas las compañías grandes que tenían que ver con este sector tienen múltiples iniciativas de desarrollo interno de nuevas capacidades. Hay un mercado muy dinámico de adquisiciones y de integración de compañías y desarrollos, que se producen tanto en ámbitos más reducidos como en centros de conocimiento, en investigación, universidades, etcétera. Las compañías pequeñas que nacen y tienen éxito tienen un reto y una exigencia muy compleja, muy intensa, que se deriva del hecho de crecer aceleradamente, lo cual dificulta a veces su desarrollo y sostenibilidad. Por otra parte, las empresas grandes tienen una obsesión por integrar y absorber todo aquello que aparece en el horizonte y que tiene éxito o que parece que puede tenerlo.

Esto está imponiendo una dinámica de cooperación en este sector: el éxito en estas industrias depende de ser capaces de cooperar como seguramente no se había hecho desde el comienzo de la revolución industrial en los sectores de infraestructuras. Una cooperación que se da entre sectores de actividad y especialidad muy distintos, pues hoy en día es necesario ser multidisciplinar y casi ninguna compañía tiene o domina todas estas disciplinas. Hablo de una colaboración como hace mucho que no se recordaba entre clientes y proveedores. Hay ahora una relación entre ellos que es mucho mas una alianza que una relación tradicional de suministro de bienes y servicios. Y también hay una forma de cooperar distinta y nueva entre grandes y pequeñas empresas, una relación distinta y diferente a la que es habitual en otros muchos sectores. En el ámbito de esos tres componentes de la demanda también hay una relación nueva entre lo público y lo privado, porque ni el sector publico solo ni el sector privado solo pueden acceder y absorber todas las características de la demanda. Incluso entre los agentes estrictamente públicos, o solamente públicos, tiene que haber alianzas entre países o entre distintos ámbitos de la administración que antes ac-

tuaban y gobernaban los requerimientos de seguridad desde estancias separadas, diferenciadas, y que cada vez tienen que estar más integradas.

Hoy en día no hay ninguna organización que sea capaz de atraer y desarrollar todas las habilidades necesarias para hacer frente a todos los retos a los que nos enfrentamos. No hay ninguna organización capaz de establecer con eficacia los incentivos necesarios para atraer los recursos y captar las tecnologías que se necesitan. No hay ninguna que pueda adoptar simultáneamente las formas de gestión y de gobernanza que hacen falta para tener éxito en estas actividades. Por lo tanto, esta cooperación será la tónica dominante en el futuro. Actualmente hay un debate muy interesante en Estados Unidos, donde incluso aquellos elementos centrales responsables de la seguridad nacional están encontrándose con grandes dificultades para atraer y retener a los profesionales que necesitan para esta función. No hay forma de competir para las agencias federales, para los ejércitos, para los mandos de seguridad... Con todo este ecosistema empresarial de altísimo crecimiento, de alto rendimiento, de alta compensación y retribución, no hay manera de competir a la hora de atraer a los profesionales valiosos y de éxito. Éste es un problema que vamos a tener que saber resolver, pero que por ahora sólo se puede resolver mediante esa cooperación cada vez más estrecha, y también nueva e imaginativa, entre lo público y lo privado.

Ustedes saben que todo cambio de paradigma, sea económico, industrial o social, siempre plantea el reto de cómo hacerle frente. Sin duda, ante cualquier cambio, uno tiene que ser un usuario inteligente, tiene que saber incorporarlo con rapidez, con inteligencia, y aprovechando para su desarrollo todo lo que el nuevo cambio le posibilita. La experiencia nos dice también que los países que aspiran a ser relevantes, los países que tienen un proyecto global y un proyecto propio –aunque luego lo compartan con otros en un proyecto de mayor alcance–, intentan abar-

car ese proceso completo que genera el cambio de paradigma, en este caso tecnológico e industrial. Por lo tanto, esos países no sólo se preocupan de generar una demanda inteligente y de ser usuarios avanzados de la nueva frontera de la tecnología, sino que también procuran estar en el lado de la oferta y aprovechar más y mejor las potencialidades de esta nueva ola de innovación. ¿Por qué? Pues porque la experiencia ha demostrado que eso permite lograr un desarrollo más sostenible de las nuevas capacidades, que permite generar o ser activo en la dinámica de innovación, en la dinámica competitiva que los nuevos paradigmas o las nuevas innovaciones genera. Así se gana pues más históricamente en los ámbitos más relacionados con la seguridad y la defensa y en cualquier sector de alta sensibilidad; hablamos de un sector que es crítico, que tiene componentes estratégicos. Por lo tanto, los grandes países, o los países que son y quieren ser relevantes, se están planteando cómo pueden no ser sólo usuarios avanzados e inteligentes en el ámbito de la ciberseguridad, sino cómo pueden también generar un tejido industrial innovador en este campo, para poder influir sobre él y tener un acceso privilegiado y preferente.

Los tejidos industriales e innovadores –sobre esto hay suficiente experiencia empírica en muchos sectores– requieren que se den tres elementos simultáneamente y que se gestionen y gobiernen adecuadamente para que se produzcan, tengan lugar y se desarrollen de manera sostenible y eficiente. Lo primero es que tiene que haber demanda temprana, una demanda que demande –perdón por la reiteración– innovación y que lo haga de forma continuada en el tiempo, de forma sostenida, y al margen de los ciclos económicos; o al menos que no esté plenamente contaminada por esos ciclos. Además, tiene que ser una demanda integrada y con óptica y alcance global. El segundo elemento que se requiere es que halla en ese mismo entorno capacidad de generar, que exista conocimiento o capacidad para generar de manera sostenida y, por tanto, para desarrollar las capacidades tec-

nológicas y atraer, retener y producir talento profesional, en número y calidad suficiente y de forma sostenida en el tiempo. Por último tiene que haber capacidad industrial o empresarial para todo lo anterior, desarrollada de una manera eficiente y competitiva, y por lo tanto también sostenible desde un punto de vista económico. En estos tejidos innovadores hace falta que seamos capaces de crear empresas nuevas de base tecnológica y que algunas de ellas se consoliden, crezcan y se hagan relevantes. Como también es necesario que las empresas grandes sepan hacer un uso inteligente e intensivo de las innovaciones.

Cuando se producen todos estos elementos, los países o las economías crean tejidos industriales e innovadores en los sectores en cuestión. De esto hay muchos ejemplos globales en distintas industrias y sectores. Recientemente, en esta ola de innovación tecnológica tan fuerte que ha significado la sociedad digital, todos ustedes saben que hay países que están teniendo más éxito que otros. Y en los países que tienen éxito siempre se dan estos tres elementos que he mencionado antes. Ese ecosistema necesario para que este modelo de desarrollo sea sostenible requiere, como decía, capacidad para crear muchas empresas nuevas de base tecnológica; unas pueden desarrollarse autónomamente y otras pueden integrarse en compañías más grandes, pero todas tienen que tener un proyecto de crecimiento y nacer con una ambición global. Para eso hace falta también que tengamos un número suficiente de empresas relevantes en el sector y que tengamos también un número de empresas grandes y relevantes en los sectores conexos, o relacionados, para que ejerzan un efecto tractor.

Ya para finalizar, la pregunta que nos tenemos que hacer todos es en qué condiciones estamos en España para poder generar y si creemos que nos conviene elegir esa opción estratégica, que implica no ser sólo un usuario avanzado e inteligente de las nuevas tecnologías de ciberseguridad, sino tener una presencia en ese tejido industrial innovador que está dando toda esta diná-

mica a la que me he referido. Y, por otra parte, debemos preguntarnos si tenemos los elementos necesarios para desarrollar ese tejido industrial y para crear ese ecosistema empresarial que permita un desarrollo sostenible del mismo. Yo creo que tenemos bastantes elementos a favor, pero tampoco nos sobran. Por lo tanto, tenemos que ser capaces de saber aprovechar lo que tenemos, de gestionarlo bien y de hacerlo con eficacia y, sobre todo, con agilidad, porque no tenemos mucho tiempo. En los tres niveles tenemos primero usuarios muy relevantes que pueden ser generadores de esa demanda temprana a la que antes me refería. Y también tenemos instituciones y organismos muy capacitados en los ámbitos tradicionales de la seguridad y, sobre todo, de vigilancia, supervisión, gestión de situaciones complejas y situaciones críticas, manejo de información, etcétera. Por lo tanto, tenemos experiencia y conocimientos y podemos ser regeneradores de nueva demanda, o de demanda innovadora. Lo mismo ocurre en los ámbitos de gestión de infraestructuras de todo tipo, de transporte y trafico, de comunicaciones, de energía. España tiene grandes infraestructuras y grandes operadores que son muy eficientes en esas infraestructuras. Tenemos también, en algunos de los servicios más crítico para una sociedad del siglo XXI –como son los servicios financieros y transaccionales, los servicios de comunicaciones y de sanidad–, experiencias muy relevantes y capacidades muy notables. También tenemos elementos para no ser pesimistas en cuanto a las capacidades tecnológicas. En España, por distintas circunstancias y por propósitos adoptados que han salido bien, tenemos una buena capacidad de tecnología, tanto de conocimientos científicos como aplicados y de personas cualificadas, así como la capacidad de producir talento en los ámbitos de vigilancia y supervisión de sistemas de control de desarrollo de *software* y, lo cual es muy importante, en los servicios asociados a todo esto. En el sector empresarial yo creo que tenemos capacidades muy justas. Es verdad que en este ámbito, como en otros, tenemos muy pocas em-

presas nuevas de base tecnológica. Creamos muy pocas empresas de base tecnológica y, al ser ése un sector de alta tasa de mortalidad empresarial –pues muchos proyectos no culminan–, nos quedan muy pocas que se consoliden como empresas relevantes en estos sectores tecnológicos. Tenemos pues poca natalidad empresarial y poca relevancia. Y las grandes compañías utilizadoras de estas tecnológicas tampoco se han caracterizado, a mi juicio, por hacer un uso intensivo, acelerado y suficientemente decidido de estas capacidades. En cuanto a la generación de talento, creo que tenemos una capacidad base buena, aunque seguramente los sistemas de incentivos para atraer ese talento, para retenerlo y para crear masas críticas suficientes, sean muy mejorables. Además, las instituciones en España que generan conocimiento avanzado, que generan desarrollo tecnológico en sus fases tempranas, están muy fragmentadas. Al igual que los sistemas de incentivo a la investigación y desarrollo en los ámbitos de investigación. Y, luego, como decía antes, tenemos también algunas limitaciones muy grandes en aquellos entornos que gestionan estos recursos de alto talento, que tienen grandes limitaciones para desarrollar los sistemas de incentivo y motivación y para evitar que los talentos sean objeto de fuga y de dispersión.

Dicho esto, que nos debe llevar a la reflexión y a corregir estos factores, creo que tenemos posibilidades razonables y una alta potencialidad como país para poder tener una presencia en este sector industrial y en estas tecnologías, cuya cercanía y capacidad de influencia por parte de los usuarios relevantes nos dará también unas ventajas en el potencial de un futuro mejor.

MIGUEL ÁNGEL NOCEDA
Moderador

Pasamos al turno de preguntas.

ÁNGELES BAZÁN
Informativos de Fin de Semana de RNE

Señor Monzón, me gustaría conocer más sobre la participación de Indra en el proyecto de sistemas de automatización de control fronterizo en los aeropuertos; creo que se llama ABC4EU. Tengo entendido que, en un principio, identificara los pasaportes y los DNIs del personal europeo, pero que es susceptible de ampliarse al resto de países. Me gustaría saber si, además del control –por lo que significa éste en cuanto de agilización del paso de las fronteras–, es susceptible también de conectarse con redes de seguridad y de defensa, o sí sencillamente estamos hablando de un control de identificación.

JAVIER MONZÓN
Presidente de Indra

Sabe usted más que yo, pues yo no conozco los detalles. Creo que, en efecto, tiene las características que usted dice. La arquitectura tecnológica permite que sea un proyecto de los que llamamos multipropósito. Es decir, que hoy tiene una finalidad, que es la que nos ha contratado el cliente, pero que goza de una arquitectura y una funcionalidad que permitirían aplicarlo a un ámbito mayor; en este caso de pasajeros. También creo que el sistema ya estaría listo en este caso. Como sabe, los pasaportes digitales llevan ya incorporada una serie de información, no sólo de parámetros biométricos, sino en este caso también de información de seguridad. Además, es un sistema que también permite el acceso en tiempo real a las bases de datos, tanto de seguridad como, en su caso, de otros ámbitos de protección, como puede ser el ámbito de la defensa, si así lo requiriera el cliente. Creo que es así.

GEORGINA HIGUERAS
Periodista *freelance*. Excorresponsal de *El País* en Asia

Ha hablado usted de las dificultades de tener empleados con una gran capacidad tecnológica. Un ejemplo sería el de las universidades en India, donde las empresas privadas se implican desde el primer momento en la formación de los ingenieros: les ofrecen becas, les orientan dentro de los mismos estudios y les ofrecen prácticas, de tal forma que las propias empresas van formando a los ingenieros con una series de capacidades que son las que necesitan las empresas para su expansión. ¿Por qué en España no hay una mayor vinculación entre el ámbito académico y la empresa privada? ¿Cuál es la vinculación de Indra con las universidades? ¿Cómo se consiguen los cerebros que Indra necesita para su expansión?

JAVIER MONZÓN
Presidente de Indra

Tiene usted mucha razón en cuanto a la situación general que hay en España. Sería un poco largo que le diera mi opinión sobre cuáles son las razones por las que en España la universidad y la empresa están todavía más alejadas de lo debido. Durante mucho tiempo ambas casi han mirado hacia lugares opuestos; se daban más la espalda que la cara. Indra está muy activa en este campo. Creamos hace tiempo con Ana Patricia Botín la Fundación Conocimiento y Desarrollo, cuya finalidad es acercar y fomentar más la relación entre la universidad y la empresa. Porque ustedes saben que en España el sistema de innovación tiene algunas carencias, y una es que el sector privado investiga poco. España tiene poca actividad investigadora. No llegamos a los dos tercios de la media de la OCDE. De hecho, de toda la actividad investigadora que se lleva a cabo en España, la pública es mayor que la privada, lo cual es atípico en países desarrollados,

donde la investigación privada tiene más peso que la pública. En España, de la investigación pública, dos tercios se hacen en la universidad, lo cual también es atípico, porque en otros países hay centros de desarrollo tecnológico de investigación o de conocimiento que tienen más participación en estos procesos. Efectivamente, la lógica diría que las empresas tienen que estar más cercanas a la universidad. Ustedes saben que nosotros, en España, tenemos una intensidad innovadora de la economía del 1,2-1,3% del producto interior bruto, cuando la media de la OCDE es del 2,3%; los países europeos más relevantes están en torno al 3-4%. Indra es una empresa innovadora, pues dedica a la innovación aproximadamente un 7% de sus ingresos. Y, sí, tenemos una relación muy intensa con las universidades. Gran parte de nuestro proceso de innovación y desarrollo tecnológico lo hacemos fuera de nuestros ámbito estricto, utilizando centros de conocimiento y de excelencia de universidades y de otras instituciones del conocimiento. Tenemos 110 de esas estructuras organizadas; de ellas sesenta en España y cuarenta fuera de España. En nuestro caso, sí es habitual la relación directa con la universidad. ¿Cómo lo hacemos? Hay recursos que nos parece más interesante que sean propios de la compañía y que estén dentro de la organización y hay otros recursos que nunca vamos a poder desarrollar internamente con la excelencia o el alto nivel deseables. Me refiero a aquéllos que requieren una carrera más científica, más estructurada como carrera científica, en donde no sólo intervienen aspectos vocacionales sino también de disponibilidad de recursos, de equipamiento, etcétera. Por eso, en esos casos utilizamos estos centros especializados. Pero tengo que decir que sí estamos notando una cierta descapitalización de alguno de estos centros, tanto por razones de menos disponibilidad de recursos presupuestarios y de otro tipo como por la dinámica que se está produciendo en el mundo de los centros de investigadores de excelencia; lo cierto es que en España, en algunos casos, las universidades no son la mejor estructura para se-

guir esas tendencias, pues tienen rigideces tanto en la forma de gobernarse como en los sistemas de incentivos de los investigadores y en la forma de estructurar sus carreras profesionales. Yo creo que ése es un ámbito al que en España debemos prestarle mucha atención. Luego está la otra derivada que usted decía de la formación. No me refiero sólo a los recursos de investigación, sino a conseguir que los profesionales que se forman en nuestro sistema educativo, y en particular en la universidad, sean más rápidamente y más eficazmente empleables en las industrias que demandan recursos de alta cualificación. En eso hay también algunas rigideces y algunas características de nuestro sistema universitario que lo hacen más complejo. Pero sí, las empresas tenemos que aprender a acercarnos más a la universidad y a incorporar más estas funciones que he mencionado.

JOSÉ MANUEL VERA
One Magazine

Quería preguntar, aprovechando la presencia del Ministro de Defensa, por la idea de la que se habla en todos los medios de comunicación respecto a la posibilidad de que Indra capitanee un polo industrial muy fuerte en la industria de la defensa en España. ¿Cuál es su opinión? ¿Qué futuro le ve a esta idea? Sobre todo teniendo en cuenta que también se habla de una posible compra de acciones de Indra por parte del Ministerio de Defensa.

JAVIER MONZÓN
Presidente de Indra

Nosotros siempre hemos dicho que todo lo que implique dinamizar y reforzar la industria de defensa nos gusta mucho y que lo apoyaremos. Y lo estamos apoyando. Creo que tenemos una relación muy positiva y muy fructífera con el Ministerio de Defensa y con los otros ámbitos de la administración española que

tienen responsabilidad en estos ámbitos. Quería decir eso en primer lugar. En segundo lugar, nosotros ya hemos demostrado como empresa que tenemos vocación de liderazgo en los sectores en los que actuamos, y la defensa es para nosotros uno de los sectores más relevantes. Aparte de por razones históricas y de otro tipo –pues nos sentimos muy cercanos al sector– lo cierto es que creo que hemos demostrado que somos competitivos y eficientes, de manera que toda oportunidad que tengamos de poder participar en esos procesos, y de hacerlo con liderazgo, es algo que haremos encantados.

10. CONFERENCIA DE CLAUSURA

PEDRO MORENÉS
Ministro de Defensa

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

DIEGO CARCEDO
Presidente de la Asociación de Periodistas Europeos (APE)

El Ministro del Interior, Pedro Morenés, antes de su intervención en el XXVI Seminario Internacional de Defensa

MIGUEL ÁNGEL AGUILAR
Moderador

Querido Ministro, queridos amigos ponentes y participantes en este XXVI Seminario Internacional de Defensa, que celebró su primera sesión en el Palacio de Fuensalida de Toledo en 1983, cuando todavía no era sede de la Junta de Castilla-La Mancha. Desde entonces, hemos celebrado 26 ediciones del seminario, siempre con la colaboración decisiva del Ministerio de Defensa; porque la Asociación de Periodistas Europeos no es la patronal, la CEOE, ni es la Fundación Botín, sino que es una cosa muy modesta de periodistas que vive de tener iniciativas y de que éstas sean capaces de atraer la atención y conseguir el patrocinio necesario para mantenerse. Y, en este asunto de la defensa, muchas veces las empresas no quieren ser vistas, como tampoco quieren ser vistas en la publicidad taurina. Es por eso por lo que este asunto de la defensa da un poco de vértigo. Nosotros hemos intentado curar ese vértigo normalizando la situación y la relación de los profesionales de los ejércitos con los periodistas y, también –porque ése es el círculo en el que nos movemos– con la gente de la universidad, de institutos estratégicos y del mundo de la diplomacia. Pues hemos querido siempre que este seminario tuviera amplia participación, una participación amplia e

internacional. Por supuesto, nos hemos acercado también a ese mundo conocido como la industria de la defensa, a las empresas de la defensa. Así, en este XXVI Seminario Internacional de Defensa hemos abierto un ángulo nuevo para ocuparnos de las ciberamenazas y sus respuestas.

El desfile de ponentes de ayer ha sido apasionante por el acercamiento a un mundo que no habíamos explorado anteriormente. El Almirante Fernando García Sánchez, Jefe del Estado Mayor de la Defensa, hizo una referencia que creo que ilustraba bien el ángulo que hemos elegido: «A comienzos del siglo XX resultó que volábamos, de ahí que se montara la fuerza aérea, ya que los aviones pueden llevar personas, ovejas, coliflores o misiles o bombas. Era un espacio nuevo, un arma nueva y algo sobre lo que había que reflexionar para establecer cómo responder a las amenazas que nos pudieran venir por el aire». Lo que vino a decir, amigos del ciberespacio, es que por ahí también aparecen esas posibilidades y amenazas, esa nueva dimensión, como también aparece la necesidad de darle respuesta a los conceptos de la ciberdefensa.

Querido ministro, como sabes, en unos meses recibirás un compendio de estos debates en forma de libro que publicamos cada año para que lo hablado aquí tenga más capacidad de ser consultado y discutido. Te agradecemos mucho la compresión y el apoyo que prestas a este seminario e intentaremos seguir mereciéndolo. Agradecemos que hayas acudido a Toledo para darnos tu punto de vista sobre esta cuestión.

DIEGO CARCEDO
Presidente de la Asociación de Periodistas Europeos

Por mi parte sólo reiterar todo lo que ha dicho; Miguel Ángel: agradecer al ministro que haya podido desplazarse a Toledo y dedicarnos unos minutos que estoy seguro serán de enorme interés para todos los asistentes. Y, por supuesto, agradecerle mu-

chísimo la atención con la que el ministerio, y el ministro en particular, están contribuyendo a que nuestro seminario pueda seguir adelante y con importante participación. Muchas gracias, señor ministro. Estamos deseando escucharle.

PEDRO MORENÉS
Ministro de Defensa

Muchísimas gracias. Señor presidente de la Asociación de Periodistas Europeos, secretario general, queridos Diego y Miguel Ángel, señor Jefe del Estado Mayor, Almirante y director de mi gabinete, Segundo Jefe del Estado Mayor, autoridades militares, presidente de Indra, autoridades, señor embajador de Israel, agregados, periodistas, medios de comunicación...

El JEMAD me ha pisado el ejemplo que yo había discurrido, porque era exactamente ése: a finales del siglo XIX se descubre un espacio como elemento de comunicación, como elemento útil para la supervivencia, que es el espacio aéreo. A partir de ahí se desarrollan unas serie de actividades, de tecnologías, de preocupaciones y de búsquedas que acaban con los 75 años que se cumplen en 2014 de la fundación del Ejército del Aire, años en los cuales precisamente el dominio del aire ha permitido establecer que, como con todos los instrumentos, hay algo bueno y algo malo para la sociedad.

De lo que voy a hablar hoy aquí es del elemento de búsqueda de seguridad de las sociedades a las que sirven dichas Fuerzas Armadas. Ese espacio nuevo que se ha abierto a todos –como también se ha abierto el espacio exterior– ha dado lugar a una serie de enormes preocupaciones. Los espacios en los que tiene lugar la actividad humana tienen formas cada vez más sutiles y difíciles de controlar mediante los viejos sistemas. De ahí que se requiera, primero, valentía para hacer frente a esa nueva realidad y, luego, un esfuerzo permanente de innovación y adaptación a la realidad, que tiene que estar basado en lo mejor que tiene el

ser humano, que es el talento. A partir de esta premisa desarrollaré la visión que tenemos en las Fuerzas Armadas y en el Ministerio de Defensa sobre lo relativo al ciberespacio y su utilización para hacer el mal y, sobre todo, para evitarlo por parte de quienes tienen la responsabilidad de hacer precisamente eso, que son las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado; los gobiernos, en definitiva, que tienen que mirar por el bien de sus sociedades.

Antes de proseguir, quiero felicitar a la Asociación de Periodistas Europeos. Tuve el honor de ser invitado al XXV aniversario de estos encuentros y creo que celebrar este XXVI seminario es toda una proeza. Lo cual exige una felicitación, cosa que hago encantado. Y exige también un compromiso con quienes durante 26 años han estado al frente de un proyecto que permite que España cuente con foros como éste, que sirven para generar conciencia en los ámbitos en los que ponen su atención. Creo recordar que en los años que he estado presente sólo habéis tenido aciertos. Y este año no es la excepción. Por lo tanto, felicidades una vez más. Y mucho ánimo. Contáis con el Ministerio de la Defensa, sea quien sea el ministro, porque éste siempre entenderá la importancia de que alguien piense en la seguridad y la defensa como elementos esenciales de una sociedad sana.

La dimensión «cíber» forma parte de nuestro quehacer diario, en el ámbito profesional y en el personal, en todos los aspectos de la vida. Hasta tal punto es así que, si en estos momentos hubieses un apagón en el ciberespacio, no retrocederíamos diez años atrás, sino más bien sesenta, porque hemos depositado en el mundo cíber mucha parte de lo que antes se hacía mediante otro tipo de actividad humana. Y lo hemos hecho considerando que ese espacio, entre otras cosas, es un espacio seguro. Pero nada más lejos de la realidad. Ese espacio está siendo utilizado por elementos perturbadores del orden y de la paz, de la justicia y libertad, precisamente para desestabilizar éstas con objetivos absolutamente reprobables. Es muy difícil hoy en día hacer fren-

te a esa amenaza con los viejos odres, utilizando el símil evangélico de «no se ponga vino nuevo en odre viejo». Pues aquí pasa lo mismo. Este vino nuevo hay que ponerlo en odre nuevo, porque si no nos va a superar a todos. De hecho, estamos viendo algunas cosas que desestabilizan nuestras sociedades que serían impensables hace solamente diez, doce o quince años.

A las amenazas clásicas a las que estamos sometidos hay que sumar nuevos actores y organizaciones transnacionales, pues además del nuevo espacio hay nuevos elementos de amenaza. Eso es la guerra asimétrica, lo que está justo delante de nosotros. El acceso y utilización de los sistemas de los que ahora estamos hablando puede ser aprovechado por personas a título individual. Es cierto que también se pueden usar por los Estados, pero a título individual puede hacerse un daño enorme; a las pruebas sobre seguridad de la información me remito.

En el ámbito de la seguridad y la defensa, el ciberespacio y el resto de dimensiones están intimidante interrelacionados y forman parte indisoluble del mismo entono en el momento de iniciar cualquier proceso de toma de decisiones y en su posterior ejecución. Haré una pequeña reflexión sobre lo que estamos hablando en la OTAN. Hay una discusión en la organización sobre si cada país tiene que atender a su propia seguridad en el ciberespacio o no. La Alianza tiene un elemento permanente de interrelación que hace que, en cada momento, el eslabón más débil de esa cadena se convierta precisamente en la debilidad de toda la cadena. Es decir, también de los países que tiene una muy desarrollada capacidad de ciberseguridad. Por lo tanto, la cooperación en el ámbito de la ciberseguridad es un elemento esencial para que todos estemos protegidos. Hay millones de puertas para entrar en nuestras infraestructuras más críticas, en nuestro sistema operativo, financiero... Si bien la visión integral es un elemento común de todas las dimensiones, en el caso de la ciberseguridad esta visión cobra un valor añadido. El ciberespacio es donde se están produciendo los cambios más amplios de

este mundo globalizado e interdependiente, cuyo creciente dinamismo incide directamente en nuestras sociedades con dos factores principales: la continua dependencia de esta dimensión por parte de nuestras sociedades y su fácil accesibilidad por cualquier persona. En la Directiva de Defensa Nacional del año 2012 se contempla que la seguridad de los españoles es una responsabilidad inalienable, intransferible e irrenunciable del Gobierno de la nación. Y, al igual que en la estrategia de seguridad nacional, las ciberamenazas constituyen, allí donde se establecen, un desafío y un reto creciente para nuestra seguridad. El Gobierno trazó en la Estrategia de Seguridad Nacional, como objetivo de una de sus líneas de actuación, el hecho de garantizar un uso seguro de las redes y de los sistemas de información a través del fortalecimiento de las capacidades de prevención, detención y, también, respuesta a los ciberataques. Así pues, desde el Ministerio de la Defensa se han impulsado una serie de medidas que contribuyen a la gestión integral de la ciberseguridad. Ello no sólo concierne a la protección y la seguridad de los sistemas puramente militares, sino a todo aquello que la normativa vigente establece como competencias y responsabilidades de este ministerio respecto a la seguridad y la defensa nacionales.

Este impulso, entre otras medidas, se tradujo en la creación en el mes de febrero de 2013 del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas bajo el auspicio del Jefe del Estado Mayor de la Defensa. El Mando de Ciberdefensa no sólo tiene la misión de llevar a cabo las acciones relativas a la ciberdefensa militar, sino que va a contribuir también a las respuestas adecuadas en el ciberespacio ante las amenazas o agresiones que puedan afectar a cualquier interés nacional.

Finalmente, el Gobierno aprobó el pasado mes de diciembre la Estrategia de Ciberdefensa Nacional, que sirve para desarrollar las previsiones contempladas en dicha estrategia en materia de protección del ciberespacio. Con la publicación de este último documento estratégico, el ministerio se integra perfectamente en

la coordinación de esfuerzos que entre todos debemos aportar para garantizar la seguridad de nuestro entorno. Dentro del proceso permanente de adaptación y transformación en el que se encuentran nuestras Fuerzas Armadas, la implementación de todas estas medidas relacionadas con la ciberdefensa posiciona a nuestros militares en la vanguardia de la seguridad en el ciberespacio, junto con los países aliados de nuestro entorno. Ello se traduce en una participación muy activa de nuestras Fuerzas Armadas en la preparación, planificación, gestión y respuesta a las ciberamenazas, tanto a nivel nacional como internacional. Podemos debatir sobre la tecnología, sobre los medios y todo aquello que envuelve a la ciberseguridad, pero desde el Ministerio tenemos muy presente dos elementos claves, tanto de esta nueva dimensión como de los dominios clásicos: la persona, que es el actor principal, y la voluntad de hacer daño que tenga nuestro adversario.

De este modo, desde el departamento consideramos que el militar con cometidos en la ciberdefensa constituye el pilar decisivo de todo el sistema y, por ello, debe contar con las mejores herramientas para poder llevar a cabo su función; y digo «el militar» porque aquí hay miembros también de la Guardia Civil. La educación, el adiestramiento y la instrucción son facetas imprescindibles para la preparación de nuestros militares, que, junto con la innovación e investigación, ofrecen una constante dedicación al ámbito de la ciberdefensa. Tal y como refleja la Estrategia de Ciberseguridad Nacional, las respuestas frente a las ciberamenazas deben configurarse desde un esfuerzo común de todos los actores con responsabilidades en el ámbito de la ciberseguridad. Nuestra atención no puede sólo enfocarse a la tecnología, a las redes y a los medios de esta nueva realidad, sino que debemos emprender un salto cualitativo para poder adentrarnos en un nuevo pensamiento donde el ciberespacio se integre y adquiera su verdadero valor.

Nos ha llevado tiempo conocer el nuevo entorno de la ciberseguridad. Posteriormente hemos establecido una estrategia y

ahora entramos en la fase de la acción. Actualmente las amenazas y ataques en el ciberespacio se están gestionando tanto a nivel nacional como internacional, a través de los equipos de reacción ante las emergencias cibernéticas. Defensa aporta a esos equipos para el ámbito de la ciberdefensa y la defensa nacional y, junto con el CERT, relacionado con las administraciones públicas del Centro Criptológico Nacional, e INTECO, la Secretaría de Estado de Seguridad, en lo relativo a la ciberseguridad de los ciudadanos y el sector privado constituyen los principales pilares en que se sustenta hoy en España la respuesta ante las ciberamenazas. Todo ello quedaría incompleto sin tres aportes muy necesarios en el conjunto del esfuerzo común, que me gustaría resaltar muy especialmente: la importancia de la innovación tecnológica, la investigación y el permanente y continuo aprendizaje de nuestros responsables en la ciberseguridad. Tanto desde el sector de la industria como desde la universidad, se están realizando grandes esfuerzos que aportan y consolidan unas capacidades imprescindibles para que, en el caso de la defensa, nuestros militares tengan los mejores recursos y la mejor formación para enfrentarse a los retos y desafíos en este ámbito.

Tal y como hemos confirmado en este seminario, nos encontramos en una etapa de anticipación –que es la mejor de las respuestas–, de previsión para poder detectar a tiempo las amenazas que en el ámbito del ciberespacio debemos afrontar. Ahora más que nunca, una visión global, un esfuerzo común y cohesionado de todos es necesario en aras de la seguridad y en beneficio de las personas a las que nos debemos, que son nuestros conciudadanos. El aprendizaje continuo, la perseverancia, el conocimiento, la innovación y la integración de todas nuestras capacidades son pues los principales ingredientes en una época donde hay que plantearse las ciberamenazas no como un problema, si no como una oportunidad para poder fortalecernos ante un desafío que indefectiblemente tendremos que sobrellevar. Eventos e iniciativas como las que nos han reunido aquí durante estos dos

días son un claro ejemplo de la necesidad de aglutinar esfuerzos en aras de la seguridad y el bienestar de nuestros conciudadanos en este nuevo espacio al que tenemos que atender.

Gracias de nuevo a los organizadores de este seminario. Felicito a la Asociación de Periodistas Europeos por el acierto de la temática seleccionada y le manifiesto el compromiso del Ministerio de Defensa de seguir apoyándoles en el futuro. Estoy seguro de que ello va en beneficio de todos nosotros. Por eso, muchas gracias una vez más, porque entre nosotros incluyo a las Fuerzas Armadas y a la seguridad y defensa de España como asignatura importante para tener en cuenta.

MIGUEL ÁNGEL AGUILAR
Moderador

Muchas gracias, ministro. Tenemos todavía tiempo para las preguntas que ustedes quieran formular.

EMILIO ANDREU
Corresponsal para Asuntos de Defensa de RNE

Le quería preguntar al ministro sobre la vinculación de la ciberdefensa y el presupuesto. Ayer el presidente del Gobierno dijo que íbamos a tener una defensa creíble y nuestra, pero no hablo de incrementar los presupuesto. Dentro de poco el ministro de Hacienda, Montoro, va a presentar el escenario macro. ¿El año que viene habrá un incremento de presupuestos para la defensa o seguiremos igual?

PEDRO MORENÉS
Ministro de Defensa

El año que viene va a haber una priorización en los presupuestos de defensa en la potenciación de la ciberdefensa. El resto

pregúnteselo al ministro Montoro cuando llegue el momento. Yo haré lo mismo.

GEORGINA HIGUERAS
Periodista *freelance*. Excorresponsal de *El País* en Asia

Buenas tardes. Ministro, ha hablado de cómo la aviación hizo que se creará la fuerza aérea. Entonces, ¿la ciberdefensa va a hacer que este quinto dominio, como lo llamamos hoy en día, necesite también un cuerpo especial, un cibercuerpo?

PEDRO MORENÉS
Ministro de Defensa

La exploración del espacio aéreo empieza hace muchísimos años, con uno de los diseños más fantásticos, que se puede ver como arte o como tecnología; dos temas muy unidos. Me refiero al aparato volador de Leonardo da Vinci. No se va a crear una Fuerza Armada para el ámbito del ciberespacio, como tampoco se hizo un Ejército del Aire cuando empezó a explorarse el aire, porque el Ejército del Aire cumple 75 años, pero ya se volaba antes. El Ejército del Aire es hijo del Ejército de Tierra. Capitanes de caballería e ingenieros eran los que volaban antes de que se crease el Ejército del Aire. Por lo tanto, creo que hay un proceso evolutivo y nosotros tenemos que hacer frente con las estructuras que tenemos a esta nueva amenaza. Yo ahora podría decir que vamos a crear un cuarto ejército para hacer frente al ciberespacio, con su propio Jefe del Estado Mayor, pero esto no va por ahí. Los procesos son evolutivos y, sobre todo, el esfuerzo que se hace con la amenaza tiene que ser razonable. Pero sí digo que dentro de 75 años las Fuerzas Armadas no serán como las que hoy conocemos, porque, dentro de los ámbitos en los que tenemos que estar proveyendo seguridad y defensa a nuestra sociedad, se habrán producido unos cambios profundos en todos

los niveles; de la misma manera que en el resto de la sociedad. Es decir, nuestra sociedad ya no es la misma que hace veinte años. No tiene nada que ver.

JOSÉ MANUEL VERA
One Magazine

La pregunta es muy sencilla. El Ministerio de Defensa tiene una serie de organismos de investigación en los que se está trabajando la reorganización –INTA, Canal de Experiencias Hidrodinámicas, La Marañosa–, todos centrados en tecnologías que son de nuestros días. En esta reorganización, ¿se contempla que alguno de estos organismos también sea un sitio de investigación en temas de ciberespacio, como ya existe en otros países, aunque de momento en España esto está en las universidades y el sector privado? ¿Defensa va a contar con un centro de investigación en serio del espacio? Gracias.

PEDRO MORENÉS
Ministro de Defensa

Actualmente, hablar de defensa por un lado y de la sociedad por otro no tiene sentido. La sociedad tiene que ser un todo integral, tal y como pasa en Estados Unidos. Ahí la investigación de defensa se hace en las universidades, se hace en las Fuerzas Armadas y se hace en todos lados. En la fórmula I+D+i, la primera I es investigación básica que sirve luego en sus aspectos duales directamente para la defensa. Yo creo que la defensa tiene que estar más en los desarrollos tecnológicos y en la propia innovación. Nosotros hemos firmado un acuerdo con la Universidad Politécnica de Madrid precisamente para trabajar en aspectos que nos interesan en este ámbito. Da igual donde se haga la investigación básica, siempre que sirva para los intereses generales de la sociedad. Mi idea es contribuir permanentemente a

que se desarrolle un conocimiento integral en la universidad, en el ministerio, en las empresas, en todos aquellos ámbitos en los que se pueda contribuir, no sólo al bien de la defensa, sino al bien de la sociedad, a una sociedad libre en la que se pueda vivir en paz. Ése es objetivo de las Fuerzas Armadas, de los Cuerpos de Seguridad del Estado y del Estado en sí mismo; a eso es a lo que debemos contribuir todos. El gran secreto es la integración del conocimiento, no la separación del conocimiento.

MAYTE CARRASCO
Reportera de guerra *freelance*

Soy reportera de guerra en zonas de conflicto. El año pasado, en este mismo escenario, hablábamos sobre cómo afrontar las nuevas amenazas con drones, es decir, de nuevas formas de luchar desde el aire. A mí me daba la impresión de que, al final, la forma de luchar era la de siempre, en las trincheras, con Kalashnikovs o con bombas. Este año hablamos de ciberamenazas y ahora me pregunto sobre las amenazas que recaen sobre el Estado español hoy en día. ¿En qué medida son importantes esas ciberamenazas o siguen siéndolo más las amenazas de toda la vida? Como, por ejemplo, el terrorismo islámico, ¿Lo situaría como la primera amenaza? En caso de no hacerlo, ¿cuáles son las principales amenazas que sufrimos?

PEDRO MORENÉS
Ministro de Defensa

La aparición de un nuevo ámbito de riesgo y amenaza, de creatividad y libertad, como es el ciberespacio no excluye otros problemas que tenemos en la sociedad. No se puede comparar el ciberterrorismo con el yihadismo, ya que en el ciberespacio está todo el mundo; los yihadistas también. Es pues un instrumento. No es en sí una amenaza. Sólo lo es cuando se utiliza para hacer

daño a la sociedad. Por lo tanto, son conceptos distintos. Quienes quieren hacer daño usarán los instrumentos que tengan a mano; algunas personas están en la trinchera con el Kalashnikov y otros, o incluso los mismos, están también en el ciberespacio. Este es el asunto relevante. Ninguna amenaza excluye a otra. Ahora es cierto que hoy en día alguien que sepa manejar un ordenador y sepa cómo entrar en determinados ámbitos puede hacer muchísimo más daño que con un Kalashnikov.

ENRIQUE PERIS
Excorresponsal de TVE en Londres

Señor Ministro, quería preguntarle hasta qué punto es dramáticamente urgente esa aportación presupuestaria para el asunto de la ciberdefensa que usted espera que se materialice el año que viene, una vez concienciado el Ministro de Hacienda. Además, en la sesión anterior del seminario hablábamos de hasta qué punto la empresa privada tendría que contribuir económicamente, haciéndose cargo de la ciberdefensa en el sentido de evitar los sabotajes. Como decía el director del Centro Nacional para la Protección de Infraestructuras Críticas a la ciberdefensa hay que quitarle el prefijo cíber y aplicar los criterios que se aplican para la defensa en general. Por lo tanto, la mejor ciberdefensa será el ciberataque. ¿Estamos preparados para atacar a los potenciales saboteadores? Pongo el ejemplo de los llamamientos yihadistas que hacen que activistas de los territorios españoles vayan a luchar en los escenarios de Oriente Medio, como Siria. ¿Hasta qué punto estamos preparados para luchar activamente en ese campo?

PEDRO MORENÉS
Ministro de Defensa

La pregunta contiene varias facetas. La primera ya ha sido contestada: dentro del presupuesto de defensa vamos a prestar una

especial atención al ámbito de la ciberseguridad para seguir desarrollándola en la medida en que el conocimiento y nuestras alianzas en OTAN y en Europa nos permitan ir desarrollando una capacidad dentro de la estrategia común. Toda la administración está comprometida e involucrada en el desarrollo de la estrategia de ciberdefensa. Dentro de ese esfuerzo, es muy relevante también el sector privado, que tiene un gran interés en proteger el valor creado en sus propias empresas. No es responsabilidad única del Ministerio de Defensa elaborar toda la defensa del ciberespacio. Es, al contrario, una responsabilidad de toda la sociedad, una responsabilidad compartida por el Estado, por la sociedad civil y por las empresas. Todo esto se tiene que integrar dentro de una autodefensa, como en todos los órdenes de la vida. España se está preparando, como el resto de la OTAN, para los nuevos ataques detectados. A veces tenemos problemas, como los hay en la propia OTAN, pues esto es una permanente adaptación a las amenazas, una carrera permanente de I+D+i, de presencia, de convicción en lo que se hace. Justo hoy venía en el coche leyendo que la OTAN recibe millones de ataques a su red cada mes, decenas de miles al día. A eso es a lo que nos estamos refiriendo. Se están produciendo una serie de ataques y debemos estar preparados, compartiendo objetivos con la sociedad, para tratar de evitarlos. El Ministerio de Defensa es un eslabón importante que se tiene que centrar en que la propia defensa no se vea debilitada por estos ataques, al tiempo que contribuye desde el conocimiento a lo que otras organizaciones del Estado puedan requerir. Éste es el proceso. La clave es la integración de los saberes. Ningún país o institución es capaz de hacer frente por sí solo a una amenaza global que se multiplica geométricamente. Ahora no existen fronteras, sino libre conocimiento. Eso tiene grandes virtudes y grandes riesgos. Y es en eso en lo que tenemos que ser capaces de integrar nuestras capacidades. Nosotros solos, incluso dedicando todos los recursos de la defensa a la ciberseguridad, no alcanzaríamos una protección absoluta de nues-

tros intereses. Como tampoco lo consigue Estados Unidos, que tiene que compartir estas capacidades entre diversas agencias y la sociedad en general.

En cuanto al último tema, ha hablado usted de los yihadistas. La geografía sigue siendo una cuestión extremadamente importante y la situación de España sigue siéndolo también. Hablando claramente, nosotros en la OTAN hemos expuesto la situación en Ucrania, explicando que, por muy inesperado que haya sido lo que se ha dado, se ha dado y hay que afrontarlo. Pues también hay un ámbito de inseguridad permanente y de largo recorrido que se concentra en el sur y el este del Mediterráneo. En resumen, hay que tener claro que las amenazas nos elijen a nosotros, y no al revés.

MIGUEL ÁNGEL AGUILAR
Moderador

Querido Ministro, muchas gracias. En contraprestación a todo lo que has dicho en nuestro favor, decirte que tenemos invitado al ministro Montoro en la Asociación de Periodistas Europeos y que le mentalizaremos sobre el esfuerzo que tiene que hacer en estas áreas. Muchas gracias, ministro, y muchas gracias a todos por vuestra asistencia y participación en el seminario.

11. BIOGRAFÍAS DE LOS PONENTES

MIGUEL ÁNGEL AGUILAR

Inició su carrera periodística en 1966 en el diario *Madrid*, donde fundó la Sociedad de Redactores de este diario meses antes de que fuera cerrado por el Gobierno del General Franco en noviembre de 1971. Dirigió *Diario 16* desde 1976 hasta 1980 y *El Sol* entre 1990 y 1991, y fue director de información de la Agencia Efe entre 1986 y 1990. Ha trabajado además en *Cambio 16, El País* y *Posible,* presentó los informativos nocturnos y de fin de semana de Tele 5 y ha colaborado en *Tiempo*, Radio España, Cadena COPE, Antena 3, Telecinco y CNN Plus, entre otros. En la actualidad es colaborador de *El País, La Vanguardia, Cinco Días* y la Cadena SER. Es secretario general de la APE desde su establecimiento en 1981. Ha publicado varios libros, entre los que cabe destacar el último, *España contra pronóstico.*

SULEYMAN ANIL

Miembro del equipo responsable de Ciberdefensa en la OTAN, antes de entrar en la Alianza Atlántica trabajó como experto en nuevas tecnologías para Alcatel, donde participo en diversos proyectos internacionales. Tras catorce años trabajando en el marco INFOSEC, actualmente es jefe del Equipo de Repuesta de Incidentes Cibernéticos de la OTAN. Como responsable de la coordinación internacio-

nal de la Alianza en el ámbito de la ciberdefensa, Anil es el encargado de establecer vínculos de trabajo entre organismos de ámbito nacional e internacional relacionados con la ciberseguridad y la ciberdefensa.

GREG AUSTIN

Especialista en lucha contra el terrorismo y crimen organizado en el marco del G-8, Austin es Miembro Investigador del East-West Institute de Nueva York, institución de la que ha sido vicepresidente de Seguridad Global y en la que ha liderado el equipo de trabajo encargado del estudio de Gobernanza Global y Ciberseguridad. Autor y coautor de diversas obras sobre las estrategias de China y Rusia, incluyendo elementos de desarrollo militar y estrategia, en 2003 lideró el equipo de asesoramiento al Gobierno británico para la prevención de conflictos. Austin también ha trabajado para el Gobierno de Australia.

ÁNGELES BAZÁN

Tras comenzar su carrera periodística a los dieciséis años de edad en el informativo «España a las Ocho» de Radio Nacional de España, trabajó como redactora en distintos programas e informativos de RNE. Entre 1992 y 1997 dirigió y presentó el «Diario de la Tarde» de Radio Nacional, labor por la que obtuvo el Premio Ondas en 1996. En la actualidad trabaja en los Informativos de Fin de Semana de la radio pública. Sin abandonar nunca la radio, también ha trabajado en TVE como entrevistadora de actualidad en el programa «Buenos Días» (1990-1991) y como presentadora de «Hablando Claro», «La Hora de Vivir» y «Aquí hay Trabajo» (2002-2009). Simultaneamente, ha impartido clases de Periodismo en distintas universidades, tanto públicas como privadas.

JAVIER CANDAU

Jefe del Área de Políticas y Servicios del Centro Criptológico Nacional, Candau es Teniente Coronel de Artillería e ingeniero industrial especializado en electrónica y automática. Especialista en criptología, dispone de diversas certificaciones de especialización en seguridad de las Tecnologías de la Información y la Comunicación (TIC), campo en el que cuenta con más de diez años de experiencia. Candau además es supervisor de la Capacidad de Respuesta ante Incidentes Gubernamentales.

DIEGO CARCEDO

Periodista y escritor nacido en Cangas de Onís (Asturias). Inició su carrera en la redacción de *La Nueva España* y de la Agencia Pyresa, donde fue corresponsal volante. Ha sido corresponsal de TVE en Portugal y Estados Unidos, donde continuó después como delegado de la Agencia Efe, y enviado especial a numerosos conflictos. Fue director gerente de Relaciones Internacionales de RTVE, director de los Servicios Informativos de TVE, director general de Radio Nacional de España, donde creó *Radio 5 Todo noticias* y miembro del Consejo de Administración de RTVE. También es presidente de la Asociación de Periodistas Europeos. Entre sus últimas publicaciones figura el ensayo *Entre bestias y héroes*, por el que fue galardonado con el Premio Espasa.

JAVIER FERNÁNDEZ ARRIBAS

Licenciado en Periodismo, Fernández Arribas ha cubierto para distintos medios prácticamente todos los enfrentamientos bélicos de los últimos diez años. También ha sido subdirector de la agencia de noticias Colpisa (Gru-

po Correo), subdirector de Informativos de Onda Cero Radio y director de Informativos de Punto Radio, así como profesor del máster de Relaciones Internacionales de la Universidad Complutense de Madrid. En el año 2000 obtuvo el Premio de Periodismo Europeo Salvador de Madariaga. En la actualidad dirige la revista *Atalayar*, colabora con distintos medios, como RTVE y la COPE, y es vicepresidente Internacional de la Asociación de Periodistas Europeos.

ALMIRANTE FERNANDO GARCÍA SÁNCHEZ

Jefe del Estado Mayor de la Defensa, el Almirante García Sánchez ingresó en 1971 en la Escuela Naval Militar. Ha sido Comandante de la Unidad de Buceadores de Medidas contra Minas, así como del patrullero «Villamil», de la corbeta «Infanta Elena», del petrolero «Marqués de la Ensenada» y del Centro de Evaluación y Calificación para el Combate. También ha sido Jefe de Órdenes del Grupo de Escoltas y 41 Escuadrilla de la Flota, del Estado Mayor del Grupo Alfa, del Departamento de Operaciones de la Escuela de Guerra Naval, de la Sección de Planes Estratégicos de la División de Planes del Estado Mayor de la Armada y del Estado Mayor de la Fuerza de Acción Marítima. Hasta diciembre de 2011 fue Segundo Jefe del Estado Mayor de la Armada. Ese mismo año fue nombrado Jefe del Estado Mayor de la Defensa y promovido a Almirante General del Cuerpo General de la Armada.

JUAN ANTONIO GÓMEZ BULE

Licenciado en Ciencias Políticas y Sociología, Gómez Bule comenzó su carrera profesional en el campo de la seguridad en el departamento informático de la empresa DINSA. Más tarde trabajó en ASCOM y en Pro-

segur, donde ocupó el cargo de director general de la División de Tecnología. En la actualidad ostenta la presidencia de la empresa SIEG (Soluciones de Inteligencia Estratégica Global) y es consejero del Instituto Choiseul y presidente de S21sec, empresa especializada en servicios y tecnología de seguridad.

JOSÉ ANTONIO GUARDIOLA

Comenzó su carrera periodística en Guadalajara, publicando su primera nota en *Nueva Alcarria* en 1981. Trabajó como redactor en el diario *La Prensa Alcarreña* y continuó su carrera en la revista *Castilla-La Mancha*, antes de incorporarse en 1988 a los Servicios Informativos de TVE. Vinculado desde entonces a la información internacional, desde 1996 es enviado especial de TVE y ha cubierto los principales acontecimientos internacionales de las dos últimas décadas, fundamentalmente en zonas de conflicto. Asimismo, ha sido jefe de Información Internacional de los Servicios Informativos de TVE y director de «El Mundo en 24 Horas» y «Sur a Norte». Actualmente dirige el programa «En Portada».

TENIENTE CORONEL DE LA GUARDIA CIVIL LUIS HERNÁNDEZ

Jefe del Área de Ciberseguridad de la Guardia Civil, el Teniente Coronel Hernández tiene una dilatada experiencia en el mundo de las Tecnologías de la Información y la Comunicación (TIC). Diplomado en Informática Militar (Ministerio de Defensa) y especialista en Información (Ministerio del Interior-Guardia Civil), Policía Judicial (Ministerio de Justicia-Centro de Estudios Judiciales) e INFOSEC (Ministerio de Defensa-CNI/CCN), ha realizado más de una treintena de cursos técnicos, entre los que destacan los de Administrador e Ingeniero Certificado CNA/CNE (Novell), Administrador de Bases de Da-

tos (Oracle), Máster en Redes y Comunicaciones (Siemens-Nixdorf), Dirección de Proyectos (Bull y HP) y Gestión/Administración de Sistemas de Comunicaciones (Cisco). A lo largo de su trayectoria profesional, ha ocupado distintos destinos informáticos en la Guardia Civil, desde analista programador hasta Jefe de Proyectos Informáticos, con responsabilidades directas en el ámbito de la Protección de Infraestructuras Críticas. Actualmente es el responsable del diseño, desarrollo, administración, gestión/explotación y seguridad de los Sistemas de Información e Inteligencia de las Unidades de Investigación/Información de la Guardia Civil.

GEORGINA HIGUERAS

Licenciada en Ciencias de la Información por la Universidad Complutense de Madrid, Higueras estudió chino y completó 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)». Delegada de la Agencia EFE en Pekín entre 1982 y 1984, fue corresponsal diplomática de EFE en Washington entre 1984 y 1986 y delegada de EFE en Estrasburgo en 1987. Ese mismo año inició su etapa en *El País*. Como enviada especial en Asia, ha cubierto numerosos conflictos, entre los que destacan los de Oriente Próximo, el de Camboya-Vietnam o los de Afganistán. Asimismo, entre 1997 y 2001 fue corresponsal de la Cadena SER en Moscú y, en 2009-2010 ocupó el cargo de directora general de Comunicación de la Defensa, dentro del Ministerio de Defensa. Higueras es autora de los libros *China: la venganza del dragón* (2003), *El despertar de Asia* (2005) y *Haití: una apuesta por la esperanza* (2011).

FRANCISCO LÓPEZ LUQUE

Consultor de Accenture entre 1991 y 1996, desde entonces trabaja para Everis, donde comenzó como gerente responsable del sector de Utilities e Industria y ha desempeñado varios cargos, tanto en España como en México, donde fue director adjunto de la oficina mexicana. Desde 2010 es presidente de Everis Aeroespacial y Defensa.

ARANTZA MARTÍN

Licenciada en Periodismos por la Universidad de Navarra, ha desarrollado la mayor parte de su carrera profesional en la radio. Sus primeros pasos fueron en Radio Vitoria. También fue corresponsal de *ABC* en la capital vasca y formó parte del equipo fundacional de Antena 3 Radio en Vitoria. Ya en Madrid, formó parte del equipo que convirtió la originalmente gallega Radio Voz en una cadena de ámbito nacional. Desde el año 2000 está integrada en los Servicios Informativos de Onda Cero. En 2002 recibió la Antena de Plata, galardón que concede la Asociación de Profesionales de Radio y Televisión. Diplomada en Altos Estudios de la Defensa por el CESEDEN, en la actualidad está al frente de la información de Defensa e Interior de Onda Cero.

FRANCISCO MARTÍNEZ VÁZQUEZ

Licenciado en Derecho y Administración de Empresas, en 2004 ingresó por oposición en el Cuerpo de Letrados de las Cortes Generales, con el número uno de su promoción. Destinado en el Congreso de los Diputados, en 2005 fue nombrado director de Relaciones Internacionales de la Secretaría General del Congreso de los Diputados, puesto desde

el que dirigió y organizó las actividades internacionales de la Cámara. En esos años, Martínez Vázquez impartió también clases de Derecho Administrativo en la Universidad Pontificia de Comillas. En 212 fue nombrado director general del Gabinete del Ministro del Interior en 2012. En 2013 fue nombrado Secretario de Estado de Seguridad. Es autor de más de treinta de publicaciones sobre Derecho Constitucional y Administrativo.

GENERAL CARLOS MEDINA

Miembro de la 33 promoción de la Academia General del Aire, ha estado destinado en la Casa de S.M. el Rey (Guardia Real), ha formado parte del grupo de trabajo que redactó la documentación española del «Air Command and Control System (ACCS) Master Plan» y ha ejercido como experto español en la NATO ACCS Management Agency (NACMA). En mayo de 2009 fue designado Jefe del Grupo Central de Mando y Control (GRUCEMAC) y en 2011 Jefe del Sistema de Mando y Control. Ese mismo año fue ascendido a General de Brigada y recibió un nuevo destino en el Mando del Apoyo Logístico del Ejército del Aire, donde ocupó el puesto de subdirector de Gestión de Programas en la Dirección de Sistemas de Armas. En 2013 fue comisionado al Estado Mayor de la Defensa y designado Comandante Jefe del Mando Conjunto de Ciberdefensa.

CARLOS MIRANDA

Nacido en El Cairo, Miranda ha estado destinado en las representaciones diplomáticas españolas en Washington y Argel. Ha sido subdirector general de Naciones Unidas en la Dirección General de Organizaciones y Conferencias Internacionales, director general para Iberoamérica, asesor del Ministro de Defensa y director general para Asuntos de

Seguridad y Desarme. En 1991 fue nombrado embajador de España en la OTAN. En 2001 fue destinado a Ginebra como embajador-delegado de España en la Conferencia de Desarme y, de 2004 a 2008, fue embajador de España en el Reino Unido. Asimismo, fue el embajador representante permanente de España en el Consejo de la OTAN desde 2008 hasta 2012.

JAVIER MONZÓN

Monzón ha desarrollado su actividad profesional en los ámbitos financiero y empresarial. Tras completar sus estudios de Economía, fue director financiero y presidente de Telefónica Internacional, así como director general de Desarrollo Corporativo de Telefónica. Presidente de Indra desde su creación en 1993, tras la fusión de Inisel y Ceselsa, también ha sido consejero de otras sociedades cotizadas, tanto españolas como internacionales, así como de diversas asociaciones empresariales y fundaciones.

PEDRO MORENÉS

Licenciado en Derecho por la Universidad de Navarra y en Dirección de Empresas por la Universidad de Deusto, Morenés ha dedicado la mayor parte de su carrera a la actividad empresarial. Durante los últimos ocho años ha sido secretario general del Círculo de Empresarios y presidente del Consejo de Administración de Construcciones Navales del Norte. Antes de su nombramiento como Ministro de Defensa dirigía la filial española de la empresa europea de misiles MDBA y Seguribérica, encargada de la seguridad de los atuneros españoles que faenan en el Índico.

MIGUEL ÁNGEL NOCEDA

Periodista cántabro, Noceda siempre ha estado ligado a la información económica y trabaja desde 1989 en *El País*, donde ha sido redactor jefe de Economía y actualmente es corresponsal económico. También ha sido presidente de la Asociación de Periodistas de Información Económica (APIE) y actualmente es vicepresidente tercero de la Asociación de la Prensa de Madrid.

DAVID RAMÍREZ MORÁN

Ingeniero de Telecomunicación con diploma de Estudios Avanzados por la Universidad Politécnica de Madrid y máster de Administración de Sistemas de Seguridad y Defensa por la Universidad Rey Juan Carlos, se incorporó al Ministerio de Defensa en 2005, dirigiendo proyectos de Comunicaciones IP y de Radio Software en el Instituto Tecnológico de La Marañosa, además de participar en grupos de trabajo nacionales e internacionales. A partir de 2009 estuvo a cargo del Registro de Empresas del Área de Gestión Industrial de la Dirección General de Armamento y Material, y en noviembre de 2013 se incorporó como Analista Principal al Instituto Español de Estudios Estratégicos, donde investiga sobre temas de ciberseguridad, ciberdefensa y economía e industria de la defensa.

ALBERTO RUBIO

Periodista de dilatada experiencia tanto en radio como en medios de comunicación escritos, Rubio dirige actualmente la publicación digital *The Diplomat in Spain*, dirigida a expatriados y miembros del cuerpo diplomáticos. Comenzó su labor periodística en la COPE, cadena para la que fue corresponsal en Bruselas y Londres, y posteriormente

formó parte de la redacción del periódico *La Razón*, diario en el que fue jefe de Internacional y corresponsal diplomático.

TENIENTE CORONEL DE LA GUARDIA CIVIL FERNANDO JOSÉ SÁNCHEZ

Teniente Coronel de la Guardia Civil, ha desarrollado funciones en el campo de la Seguridad de Infraestructuras e Instalaciones de Carácter Estratégico en la Dirección General de la Guardia Civil, Dirección Adjunta Operativa (Estado Mayor). Poseedor de diversos masters y cursos superiores, tiene reconocido el título de Director de Seguridad. En su cargo actual como director del Centro Nacional para la Protección de Infraestructuras Críticas, ejerce como coordinador en la elaboración y desarrollo de la normativa española sobre Protección de Infraestructuras Críticas, área de la que es el Punto de Contacto del Estado Español con la Unión Europea.

GENERAL FÉLIX SANZ ROLDÁN

Director del Centro Nacional de Inteligencia, con rango de Secretario de Estado, Sanz Roldán ingresó en la Academia General Militar en septiembre de 1962. En mayo de 2004, tras su ascenso a Teniente General, ocupó el cargo de director general de Política de Defensa. En junio de 2004 fue nombrado Jefe del Estado Mayor de la Defensa (JEMAD), ascendiendo al empleo de General de Ejército. Durante su etapa como JEMAD se aprobaron la Directiva de Defensa Nacional, la Ley de Defensa Nacional y la Ley de Tropa y Marinería.

12. RELACIÓN DE ASISTENTES

El secretario de Estado de Seguridad, Francisco Martínez, y el JEMAD, Almirante Fernando García, atendiendo a la prensa

Aspecto del salón del Parador de Toledo donde se celebró el XXVI Seminario Internacional de Seguridad y Defensa

AGUILAR, MIGUEL ÁNGEL
Secretario general de la Asociación de Periodistas Europeos

ALFARO, JESÚS
Director de Comunicación de Navantia en Cádiz

ANDREU, EMILIO
Corresponsal para Asuntos de Defensa de RNE

ANIL, SULEYMAN
Miembro del Centro de Ciberdefensa de la OTAN en Mons

AUSTIN, GREG
Miembro Investigador del East-West Institute (Australia)

AZNAR LADRÓN DE GUEVARA, FERNANDO
General. Director de la Academia de Infantería de Toledo

BAR, ALON
Embajador de Israel en España

BAZÁN, ÁNGELES
Informativos Fin de Semana de RNE

BOIXADOS, ÁNGEL
Director de Comunicación de Indra

CANDAL AÑÓN, LUIS MANUEL
Coronel. Subdirector y Jefe de Estudios de la Academia de Infantería de Toledo

CANDAU, JAVIER
Jefe de Ciberseguridad, Centro Criptológico Nacional

CARCEDO, DIEGO
Presidente de la Asociación de Periodistas Europeos

CARRASCO, MAYTE
Reportera de guerra *freelance*

CIAMMAICHELLA, ROBERTO
Agregado de Defensa de la Embajada de Italia en España

CUESTA, JUAN
Director de *Europa en Suma*

DOS SANTOS POLETTO, RICARDO
Secretario de la Embajada de Brasil en España

ESCOBAR RAMOS, FRANCISCO
Agregado de Defensa de la Embajada
de Chile en España

FERNÁNDEZ ARRIBAS, JAVIER
Director de *Atalayar*

FERNÁNDEZ, NURIA
Infodefensa.com

GARCÍA MARTÍN, ESTHER
Agencia EFE

GARCÍA SÁNCHEZ, FERNANDO
Almirante. Jefe del Estado Mayor de la Defensa

GILOUPPE, PHILIPPE
Coronel. Agregado de Defensa de la Embajada
de Francia en España

El ministro de Defensa, Pedro Morenés, a su llegada al Parador de Toledo

Charla animada del Jefe del Estado Mayor de la Defensa

GÓMEZ, MARÍA SOLEDAD
Ministerio de Defensa

GÓMEZ BULE, JUAN ANTONIO
Presidente de S21sec

GONZÁLEZ, PEDRO
Columnista de *ZoomNews*

GUARDIOLA, JOSÉ ANTONIO
Director de «En Portada», TVE

HERNÁNDEZ, LUIS
Jefe del Área de Ciberseguridad de la Guardia Civil

HIGUERAS, GEORGINA
Periodista *freelance*. Excorresponsal de *El País* en Asia

JIMÉNEZ GARÓFANO, JOSÉ LUIS
Coronel. Jefe de Adiestramiento y
Doctrina de la Academia de Infantería de Toledo

LANCHA ESCRIBANO, YOLANDA
La Tribuna de Toledo

LÓPEZ LUQUE, FRANCISCO
Presidente de Everis Aeroespacial y Defensa

MACUA, ÁNGELES
Directora de KalmaTV

MAIA NETO, JACINTHO
Coronel. Agregado de Defensa de la Embajada de Brasil

MARTÍN, RAQUEL
Tele Toledo y Televisión Regional Castilla-La Mancha

MARTÍN GALLEGO, ESTHER
Redactora de *La Tribuna de Toledo*

MARTÍNEZ, ANTONIO
Universidad Rey Juan Carlos

MARTÍNEZ MÉNDEZ, FRANCISCO
Teniente Coronel. Jefe del Departamento de Táctica de la Academia de Infantería de Toledo

MARTÍNEZ NOGALES, ARANTZA
Responsable de Interior y Defensa de Onda Cero

MARTÍNEZ VÁZQUEZ, FRANCISCO
Secretario de Estado de Seguridad

MEDINA, CARLOS
General. Jefe del Mando Conjunto de Ciberdefensa

MIRANDA, CARLOS
Embajador. Exrepresentante Permanente de España en el Consejo de la OTAN

MONRROY PÉREZ, JUSTO
La Tribuna

MONZÓN, JAVIER
Presidente de Indra

MORENÉS, PEDRO
Ministro de Defensa

NOCEDA, MIGUEL ÁNGEL
Periodista de *El País*

OÑATE, JUAN
Director de la Asociación de Periodistas Europeos

ORGAMBIDES, FERNANDO
Periodista y escritor

ORTEGA CARCELÉN, MARTÍN
Universidad Complutense de Madrid
y Real Instituto Elcano

PENEDO, CARLOS
Analista de Defensa de *Estrella Digital*

PERALTA, PEPI
Asociación de Periodistas Europeos

PERIS, ENRIQUE
Excorresponsal de TVE en Londres

PINTOR, LUIS
Europa en Suma. Exredactor jefe de RNE

PITARCH, PEDRO
Teniente General en la reserva

RAMÍREZ MORÁN, DAVID
Analista Principal del Instituto Español
de Estudios Estratégicos

RAMOS, ANA
Eduardo Serra Asociados

El General Félix Sanz Roldán, director del CNI, responde a las preguntas de los periodistas

El ministro de Defensa, Pedro Morenés, saluda al embajador de Israel, Alon Bar

REGALADO, ANTONIO
Colaborador de *ABC*

REVENGA CUBERO, DAVID
Redactor de Audiovisual de Radio de Castilla-La Mancha

ROMERA SIBILA, MIGUEL ÁNGEL
Teniente Coronel. Jefe del Núcleo de Sistemas
e Información de la Academia de Infantería de Toledo

ROMERO, SERGIO
Coronel de Aviación. Agregado Naval de la
Embajada de Chile en España

RUBIO, ALBERTO
Director de *The Diplomat in Spain*

SAHAGÚN, FELIPE
Miembro del Consejo Editorial de *El Mundo*

SÁNCHEZ, FERNANDO JOSÉ
Teniente Coronel de la Guardia Civil.
Director del Centro Nacional para la Protección
de Infraestructuras Críticas (CNPIC)

SÁNCHEZ SÁNCHEZ, CLAUDIO
Teniente Coronel. Jefe de la Plana Mayor de la
Academia de Infantería de Toledo

SANZ ROLDÁN, FÉLIX
General. Director del Centro Nacional de Inteligencia

SILVA VIDAL, MIGUEL
Analista militar

TORRES BRUNA, MARÍA PILAR
Everis Aeroespacial

TOVAR JARDÓN, ANTONIO
Indra

URIARTE, MARÍA INES
Agregada Naval Adjunta de la Embajada de Argentina en España

VEGA, DIEGO DE LA
Asociación de Periodistas Europeos

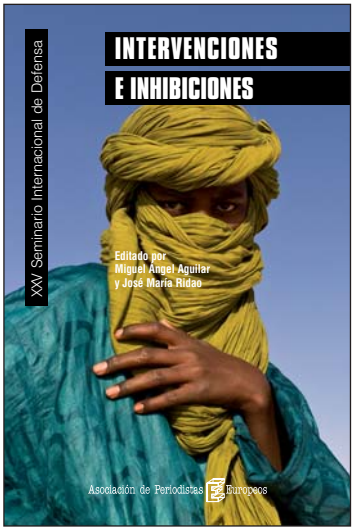
VERA, JOSÉ MANUEL
One Magazine

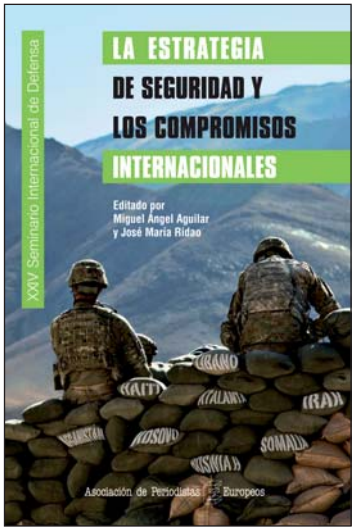
VUSKOVIC SALGADO, IVO YAKO
Capitán de Navío. Embajada de Chile en España

WERNER MÜLLER, JENS
Agregado adjunto de Defensa de la Embajada de Alemania en España

ZUBER, HELENE
Periodista alemana de *Der Spiegel*

ALGUNAS EDICIONES ANTERIORES DEL
SEMINARIO INTERNACIONAL DE DEFENSA

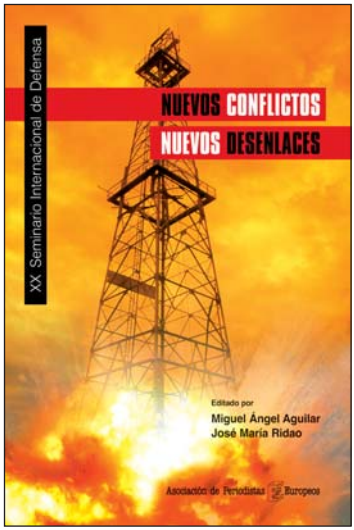

XXV Seminario Internacional de Defensa
INTERVENCIONES
E INHIBICIONES
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

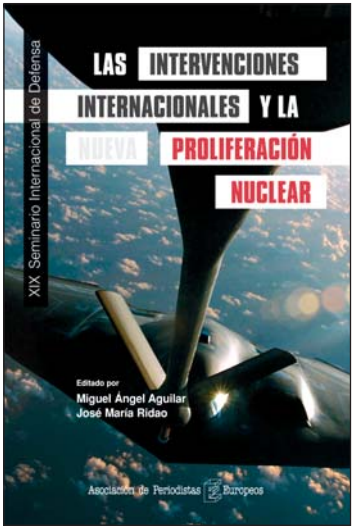

XXIV Seminario Internacional de Defensa
LA ESTRATEGIA
DE SEGURIDAD Y
LOS COMPROMISOS
INTERNACIONALES
Editado por
Miguel Ángel Aguilar
y José María Ridao
IRÁN
SOMALIA
Asociación de Periodistas Europeos


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

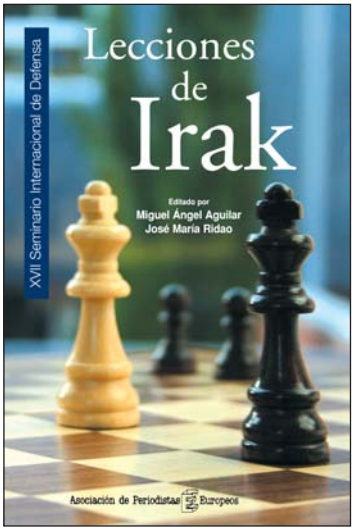

XXII Seminario Internacional de Defensa
¿UN HORIZONTE
DESNUCLEARIZADO?
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

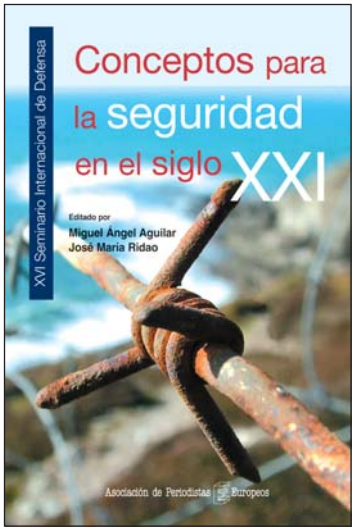

XXI Seminario Internacional de Defensa
LAS MIRADAS DE EUROPA
Y SU VOZ FRAGMENTADA
Editado por
Miguel Ángel Aguilar
y José María Ridao
Asociación de Periodistas Europeos

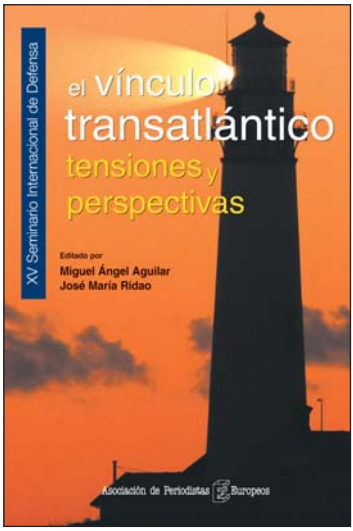

XX Seminario Internacional de Defensa
NUEVOS CONFLICTOS
NUEVOS DESENLACES
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos


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

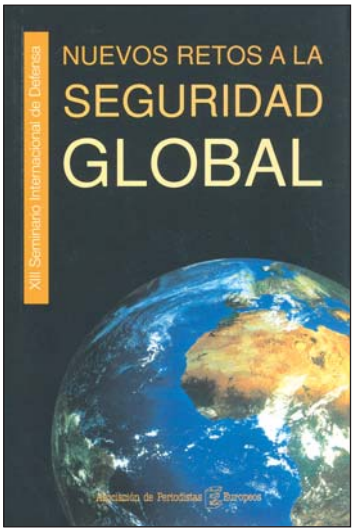

XVIII Seminario Internacional de Defensa
EUROPA Y
LOS NUEVOS ACTORES
DE LA IN SEGURIDAD
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos

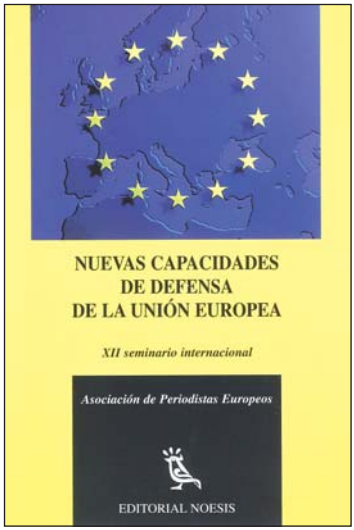

XVII Seminario Internacional de Defensa
Lecciones de Irak
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos

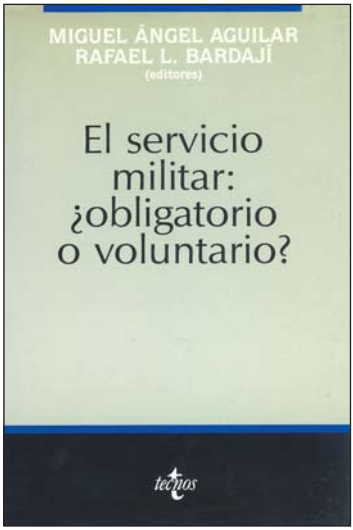

XVI Seminario Internacional de Defensa
Conceptos para la seguridad en el siglo XXI
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos

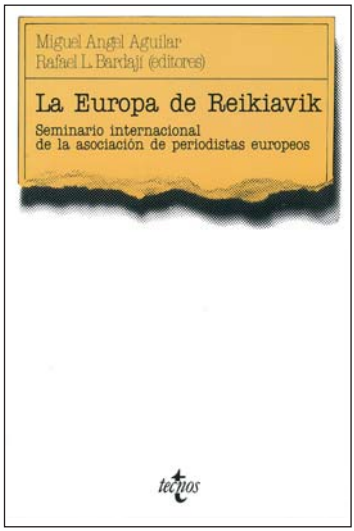

XV Seminario Internacional de Defensa
el vínculo transatlántico
tensiones y perspectivas
Editado por
Miguel Ángel Aguilar
José María Ridao
Asociación de Periodistas Europeos


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


MIGUEL ÁNGEL AGUILAR
RAFAEL L. BARDAJÍ
(editores)
El servicio
militar:
¿obligatorio
o voluntario?
tecnos


Miguel Angel Aguilar
Rafael L. Bardaji (editores)
La Europa de Reikiavik
Seminario internacional
de la asociación de periodistas europeos
tecnos