DIARIO DE SESIONES DE LAS CORTES GENERALES

COMISIONES MIXTAS

Año 2018 | XII LEGISLATURA | Núm. 116 | Pág. 1

DE SEGURIDAD NACIONAL

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

Sesión núm. 21

celebrada el martes 23 de octubre de 2018 en el Palacio del Congreso de los Diputados

---

Página

ORDEN DEL DÍA:

---

cve: DSCG-12-CM-116

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

El señor **PRESIDENTE:** Buenos días, señorías. Vamos a dar comienzo a la sesión de hoy, 23 de octubre, de la Comisión Mixta de Seguridad Nacional. El objeto es la comparecencia de don Enrique Cubeiro —quien nos acompaña—, capitán de navío y jefe de operaciones del Mando Conjunto de Ciberdefensa, para informar sobre diversas cuestiones relativas a la ciberseguridad en España.

El señor Cubeiro tiene la palabra.

El señor **CUBEIRO CABELLO** (capitán de navío y jefe del Estado Mayor del Mando Conjunto de Ciberdefensa): Muchas gracias, señor presidente.

Tengo que corregir al presidente una cosa —ha sido fallo mío—, y es que he sufrido un movimiento horizontal dentro la organización del Mando Conjunto de Ciberdefensa, y ahora mismo soy el jefe del Estado Mayor del Mando Conjunto de Ciberdefensa. Pero hasta hace nada era el jefe de operaciones.

En primer lugar, quiero agradecer a la Comisión el honor que se me otorga al comparecer hoy ante ustedes.

Me incorporé al mundo de la ciberdefensa hace tan solo cinco años, lo cual supone un recorrido extraordinariamente breve, en comparación con el de otros comparecientes anteriores, máxime en un campo tan especializado y complejo como es este. Por lo tanto, me siento un tanto incómodo con esa calidad de experto que se me atribuye al comparecer ante esta Comisión. Por otra parte, esa condición de recién llegado me permite ver las cosas con otra perspectiva, con una perspectiva diferente, por lo que, dicho con toda la modestia, creo que algo puedo aportar, y es lo que voy a intentar en los próximos minutos, no muchos, pues, antes de contarles de nuevo cosas que ya han oído, prefiero que sean ustedes los que me dirijan las preguntas que sean de su interés.

Quiero dejar claro antes de empezar que las opiniones que voy a exponer en su mayoría serán personales, y no las del Ministerio de Defensa. Cuando sean las del ministerio, así lo diré explícitamente.

El año 2013, momento en que me incorporé al Mando Conjunto de Ciberdefensa como jefe de operaciones, fue muy importante para la ciberseguridad en España. Se promulgó la Estrategia Nacional de Ciberseguridad —antes la Estrategia de Seguridad Nacional—, el departamento de Seguridad Nacional comenzaba a dar sus primeros pasos y ese mismo año se crearon el CERT de Seguridad e Industria y el Mando Conjunto de Ciberdefensa. En aquel entonces la ciberdefensa militar estaba absolutamente en pañales y, con la excepción de la banca, existía una falta generalizada de concienciación e, incluso, de preocupación por la ciberseguridad en la mayoría de los sectores de actividad. Comparando aquella etapa con la presente y a pesar de que el camino no ha sido nada fácil, resulta evidente que en estos cinco años la situación ha evolucionado de forma muy notable y que hemos mejorado mucho. Empezando por mi propia casa, en el año 2013, liderados por el general Medina, quien ya compareció ante ustedes hace unos meses, comenzamos a construir una unidad nueva que operaba en un ámbito nuevo, y no fue nada sencillo, pues en algunos terrenos partíamos de un folio en blanco. Se trataba de crear una unidad especializada en la realización de operaciones militares en el ciberespacio, sobre la cual no había demasiadas referencias. Además, esa unidad nacía también con responsabilidades en otros muchos campos no puramente operativos pero que exigían también mucha dedicación y esfuerzo. Hace unos días me correspondía el honor de despedir al general Medina por su pase a la reserva, prácticamente el día que celebrábamos nuestro quinto cumpleaños, y le agradecía su visión, al ser el primero en entender que aquel grupito de hombres y mujeres que aparecimos en septiembre en la base de Retamares iba a ser el embrión de lo que en el futuro seguramente será una gran unidad militar, pues no me cabe ninguna duda de que la importancia del ciberespacio en la resolución de conflictos va a seguir aumentando, y ello supondrá que habrá que dedicar un progresivo aumento de los recursos dedicados a ese campo.

Hoy, cinco años después, contamos con una aceptable capacidad militar de ciberdefensa, dotada de unas buenas infraestructuras y medios que incluyen el CERT del Ministerio de Defensa, infraestructuras que darán un enorme salto cualitativo el año que viene cuando dispongamos del nuevo edificio, que está en avanzado estado de construcción en la base conjunta de Retamares. Contamos con un simulador muy versátil y sofisticado, nuestro *cyber range* o campo de maniobras virtual, que apoya desde el entrenamiento básico individual hasta el avanzado e, incluso, el planeamiento operativo. Hemos desarrollado planes de formación, concienciación y adiestramiento especializado en ciberdefensa. Contamos con una plantilla aún incompleta pero de gran calidad. Hemos establecido múltiples canales de cooperación, tanto a nivel nacional como internacional, y muy especialmente en el ámbito iberoamericano. Precisamente estos días, ahora mismo, se está desarrollando en nuestras instalaciones de la base de Retamares un ejercicio, un

cve: DSCG-12-CM-116

ciberejercicio en el que participan equipos de Argentina, Brasil, Portugal, Colombia, Chile, México y, por supuesto, España. El Mando Conjunto de Ciberdefensa es además el modelo de referencia para varios de estos Estados iberoamericanos, que están iniciando sus pasos en la ciberdefensa.

En lo que respecta a las operaciones, el ciberespacio está ya completamente aceptado como quinto ámbito operativo, y se ha conseguido una integración notable de la ciberdefensa en el planeamiento y la ejecución de las operaciones. Esta ha sido probada con éxito recientemente durante el ejercicio conjunto más ambicioso que se ha desarrollado en nuestras Fuerzas Armadas, el Mopex 2018, en el que se evaluaba el mando de operaciones como cuartel general y se validaba la estructura operativa nacional de mando y control basada en mandos componentes. Ese ejercicio supuso precisamente la presentación en sociedad del Mando Conjunto de Ciberdefensa como mando componente del ciberespacio. En este sentido, tengo que decir que las fuerzas de ciberdefensa de nuestras Fuerzas Armadas, bajo el control táctico del comandante del Mando Conjunto de Ciberdefensa, desarrollan veinticuatro horas al día, siete días a la semana, trescientos sesenta y cinco días al año una de las misiones permanentes de nuestras Fuerzas Armadas: la defensa del ciberespacio de interés militar, del mismo modo que el Ejército de Tierra, la Armada o el Ejército del Aire defienden los espacios terrestre, naval y aéreo de soberanía, con la particularidad de que, a diferencia de los otros ámbitos operativos, en el ciberespacio existe una permanente y persistente actividad hostil, amparada por motivos a los que me referiré más adelante. En paralelo a esta evolución, progresamos hacia la obtención de una infraestructura integral de telecomunicaciones que responda a las necesidades operativas de nuestras Fuerzas Armadas y en las que la ciberseguridad ha sido elemento fundamental desde la fase conceptual, obtención liderada por el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones, el CSTIC, cuyo director, el general Goberna, ya compareció ante ustedes. Debido a esas comparecencias anteriores, no voy a extenderme más en lo que respecta a la ciberdefensa y a la ciberseguridad en el Ministerio de Defensa, puesto que ya fueron asuntos ampliamente tratados en las comparecencias anteriores. No obstante, por supuesto, estaré encantado de atender a cualquier pregunta que quieran hacerme al respecto.

Déjenme ahora que me salga de los límites del ministerio y les traslade desde mi perspectiva personal cómo veo, en general, el estado de la ciberseguridad en nuestro país. En el ámbito estatal contamos con un Consejo Nacional de Ciberseguridad que ejerce de comité sectorial para asesoramiento del Consejo de Seguridad Nacional y que ya ha tenido ocasiones de demostrar su eficacia, como ha sido en el caso de WannaCry o en las recientes campañas de ataques *hacktivistas*. A día de hoy contamos con tres CERT de la administración ya maduros, un modelo de gobernanza que funciona y en el que están claras las responsabilidades, cometidos y ámbitos de actuación de los diferentes actores sin que existan solapamientos o zonas sin cubrir, así como un clima de confianza, colaboración y respeto mutuo entre organismos que mejorará aún más, si cabe, con la próxima creación del centro de operaciones de seguridad de la Administración General del Estado y las medidas que deriven del desarrollo del nuevo Real Decreto-ley de trasposición de la Directiva NIS, como puede ser la guía única de gestión de incidentes, el uso de herramientas y plataformas comunes y la creación de una red de coordinación y gestión de incidentes. Cada vez es mayor el número de CERT de las comunidades autónomas. Comienza a existir en España una cultura de ciberseguridad que se plasma en datos tales como que España ocupa el noveno puesto internacional y cuarto europeo por número de empresas y organizaciones certificadas en la norma 27001. Contamos en nuestros Cuerpos y Fuerzas de Seguridad del Estado con unidades punteras a nivel mundial para la lucha contra la ciberdelincuencia, el *hacktivismo* y el ciberterrorismo. Hemos incorporado nuevos tipos delictivos en nuestro Código Penal para responder al ciberdelito y existe una fiscalía especializada en criminalidad informática. Ya se habla mucho y muy en serio de ciberseguridad en sectores como el de la energía, la sanidad o el marítimo. Estamos viendo que la trasposición de la Directiva NIS de la Unión Europea está resultando relativamente sencilla, pues la madurez alcanzada en aspectos tales como normativa sobre infraestructuras críticas y servicios esenciales, gestión de incidentes o certificaciones superaba en la mayoría de los casos las exigencias que ahora se plantean. Contamos también con empresas punteras en un espacio de negocio en el que las pymes tienen mucho que decir, toda vez que existen numerosos nichos de negocio en los que, por la enorme especialización de este ámbito, una pyme puede competir con una gran empresa en condiciones de igualdad.

Llegados a este punto es el momento de saber cómo estamos en comparación con otros. Pues bien, desde hace unos años un reputado grupo de expertos elabora un índice nacional de ciberseguridad, el *cybersecurity index,* para lo cual tienen en consideración multitud de factores de toda índole relacionados con la ciberseguridad. Según su último informe, España ocupa el séptimo puesto mundial en

cve: DSCG-12-CM-116

ciberseguridad, siendo Francia y Alemania las únicas grandes potencias que nos superan en la clasificación, puesto que la mayoría de los Estados que ocupan las primeras posiciones son pequeños Estados del norte de Europa, como es el caso de Estonia o Lituania. Tenemos, pues, motivos para estar muy orgullosos de lo conseguido. Pero sería una irresponsabilidad por mi parte dejarles con esta impresión tan positiva y complaciente. Estamos haciendo las cosas bien, es indudable, pero todavía queda mucho por hacer, en primer lugar y sobre todo porque nos enfrentamos probablemente a la amenaza más compleja que existe, y es que, como mister Hyde, el ciberespacio tiene dos naturalezas antagónicas. Es un espacio que impregna y estimula todas las actividades del ser humano y diluye fronteras pero también campo abonado para nuevos y muy serios riesgos y amenazas. Sus muchas cualidades: generalización, inmediatez, interactividad, horizontalidad, descentralización, interinfluencia y automatización posibilitan maravillosas realidades como las redes sociales, las ciudades inteligentes, el periodismo ciudadano, Wikipedia o un sinfín de aplicaciones que facilitan muchas de nuestras tareas cotidianas, pero esas mismas cualidades lo convierten también en un terreno abonado para el desarrollo de lo más perverso de la naturaleza humana, perversión que se traduce en continuos robos de credenciales de usuario, constantes campañas de *phishing,* ataques masivos de *ransomware,* cada vez más frecuentes y agresivos, ataques de denegación de servicio, con intensidades que ya superan ampliamente el terabyte por segundo, y ataques a infraestructuras críticas, que aumentan de forma exponencial; ataques, además, que cubren todos los sectores de actividad: energía, banca, telecomunicaciones, sanidad, comercio, transporte. Ya sabemos que se pueden *hackear* coches, aviones y barcos, sistemas de ayuda a la navegación, teléfonos móviles y hasta marcapasos, frigoríficos o televisores y, en general, todo ese cada vez más amplio y heterogéneo conjunto de dispositivos que se engloban bajo esa denominación del internet de las cosas y que se estima en varias decenas de miles de millones. Pero la cosa no acaba ahí, ahora ya sabemos que a través del ciberespacio se pueden atacar campañas electorales y elecciones democráticas, y hasta a la opinión pública, con el agravante de que parece ser, según se desprende de algún estudio reciente, que los españoles somos especialmente propensos a dar pábulo a los bulos y a las noticias falsas.

En unos días se cumplirán treinta años del primer ataque informático del que se tiene constancia. En noviembre de 1988 un joven estudiante de informática, Robert Morris, desarrolló como divertimento un sencillo programita de tan solo noventa y nueve líneas que causó graves destrozos en la Arpanet, la precursora de Internet. Desde entonces las ciberamenazas vienen creciendo de forma casi exponencial tanto numérica como cualitativamente, llevando a cabo ataques cada vez más sofisticados, sigilosos y difíciles de detectar, que obligan a su vez a incorporar medidas y elementos de ciberseguridad cada vez más amplios y complejos. No es extraño, pues, que la Estrategia Nacional de Seguridad contemple las ciberamenazas como una de las más importantes, tanto por su elevada probabilidad de ocurrencia, como por su alto impacto potencial. Pero es que, si analizamos el resto de amenazas: terrorismo, crimen organizado, espionaje, conflictos armados, vulnerabilidad energética, podemos ver que a todos ellos podemos anteponer el prefijo ciber, con el agravante además de que detrás de un ciberataque puede existir un sinfín de motivaciones; amenazas en cuyo ecosistema han aparecido nuevos actores en los últimos años, actores con enormes recursos, no ya capaces de explotar vulnerabilidades conocidas o de descubrirlas, sino incluso de crearlas, actores muchos de ellos que forman parte de eso que se ha dado en llamar amenaza híbrida y que se traduce en actividades —muchas de ellas en el ciberespacio— que, por su naturaleza, solo pueden realizar Estados totalitarios o Gobiernos cuya ética acepte que el fin justifica las cosas o los medios. Debido a las muchas zonas grises que aún existen en torno al uso del ciberespacio, esto coloca en una situación de ventaja a aquellos Estados y organizaciones con menos escrúpulos y ética o escasamente sometidos o condicionados por el escrutinio de la opinión pública, ello agravado por esa propia naturaleza artificial del ciberespacio, que se traduce en infinidad de imperfecciones y, por tanto, de vulnerabilidades. Pero a esas vulnerabilidades de *hardware, software* y usuarios a las que generalmente se dirigen los esfuerzos de ciberseguridad tenemos que sumar muchas otras, en primer lugar la tremenda dependencia: la conectividad permanente y ubicua ya se ha convertido en una necesidad para una gran parte de la población. Ello implica a su vez una superficie cada vez más extensa que defender y lleva a que las organizaciones, empresas y hasta ciudadanos desconozcan muchas veces su propio perímetro en el ciberespacio, con un creciente número de factores de riesgo: navegación, correo, *hardware, software,* redes sociales, telefonía móvil, interconexiones, *clouds,* redes wifi, dispositivos USB, trabajadores de terceras empresas y una sobreexposición que afecta enormemente a los individuos, que, como ya no paramos de oír, constituyen el eslabón más débil de la cadena de la ciberseguridad y que en

cve: DSCG-12-CM-116

muchos casos son utilizados por los atacantes como vectores de entrada, y es que el ciberespacio reúne un sinfín de ventajas para los atacantes, en primer lugar el anonimato. Recurriendo a la famosa viñeta de Peter Steiner, en Internet nadie sabe que eres un perro. Los ataques pueden llevarse a cabo en tiempo muy reducido e independientemente de la ubicación del atacante, algo que solo ocurre en el ciberespacio. Unas simples líneas de código pueden comprometer el más sofisticado de los sistemas: basta con encontrar un medio para introducirlo, y existen muchos. El ciberespacio es el entorno en el que es más sencillo que David derrote a Goliat, motivo por el cual la denominada ciberguerra es el paradigma de la guerra asimétrica. Existen infinidad de técnicas para dificultar la trazabilidad de un ataque, incluso con recursos económicos escasos. El resultado de todo ello es una enorme impunidad de los atacantes, que en nada favorece a la disuasión. La disuasión funciona muy mal en el ciberespacio, y, además, la impunidad ejerce un fuerte efecto llamada.

Es por todo ello por lo que todos los avances y logros que citaba al principio resultan insuficientes y haya que seguir avanzando constantemente. Pero para eso es preciso que antes de empezar con el tratamiento tengamos claro el diagnóstico, y, a mi juicio, existe una tendencia a considerar, en especial en los altos niveles de decisión, que esto de la ciberinseguridad es un problema técnico y que, por tanto, se soluciona con técnicos y tecnología; y no digo que no sea cierto en parte, pero para mí resulta evidente que esto ha de ir mucho más allá. Lo primero, por supuesto, es poner las cosas difíciles a los atacantes, incrementando la dificultad de penetrar en los sistemas y reduciendo los efectos en el caso de que lo consigan. Para ello resulta esencial desarrollar las capacidades de defensa y la capacidad de resiliencia, y en este ámbito, desde luego, los técnicos y la tecnología tendrán mucho que decir, aunque no todo. Ello ha de traducirse en arquitecturas y configuraciones seguras, en el uso de tecnologías y herramientas específicas y, no menos importante, en el desarrollo de procedimientos y políticas, para lo cual resulta necesario que exista una potente organización de ciberseguridad y resulta fundamental la formación y capacitación de nuestros profesionales, teniendo en cuenta que trabajamos en uno de los campos de actividad más efímeros, volátiles y cambiantes y, al mismo tiempo, más amplios, lo cual implica una doble necesidad: actualización continua y especialización. Ya he oído a varios expertos evaluar en varias decenas de miles los profesionales de ciberseguridad que serían necesarios para cubrir las carencias en toda España, pero eso todavía no se está traduciendo en un crecimiento de la demanda de estos profesionales. Ello implica una sobrecarga de trabajo para los existentes, y estructuras que deberían existir y cosas que se deberían estar haciendo en organizaciones y empresas no se están realizando.

Pero no solo hemos de centrarnos en los especialistas en ciberseguridad sino en todos los niveles de la organización, desde el usuario hasta el estratégico, trabajando, y mucho, en eso que se conoce como concienciación. El horizonte de ambición ha de ser mucho más amplio, tenemos que conseguir en nuestra sociedad una cultura de ciberseguridad que, como todo lo importante, debe comenzar en los colegios. Es esencial destruir esa idea de que en el ciberespacio todo vale, y para ello el señalamiento público y el ejercicio de acciones judiciales contra los autores de ciberataques es un paso fundamental. No obstante, es condición previa y necesaria contar con unas sólidas capacidades de análisis forense e ingeniería inversa que permitan la trazabilidad y la determinación de la autoría de los ciberataques. Y, por supuesto, tenemos que potenciar la ciberinteligencia como elemento fundamental para conocer al adversario o adversarios, sus capacidades, sus técnicas y sus intenciones, con el fin de poner las medidas preventivas adecuadas y tener un cierto margen de alerta previa; cuanto mejores sean nuestras capacidades de prevención, menor uso tendremos que hacer de las de reacción. Y debemos explorar lo que las nuevas tecnologías, muchas de ellas a punto de eclosionar, pueden aportar a la ciberseguridad; hablo de inteligencia artificial, de las tecnologías *blockchain,* de todas las disciplinas asociadas al *big data,* la computación cuántica, el *machine learning* o los sistemas inteligentes de ayuda a la toma de decisiones. Deberíamos ir a un modelo global de gobernanza —algo verdaderamente complicado—, un modelo de gobernanza global del ciberespacio que elimine todas las zonas grises y establezca unos principios sobre todos esos asuntos que nos preocupan: un marco normativo internacional, un equilibrio razonable entre seguridad y privacidad, el derecho al olvido. El manual de Tallin, la Convención de Budapest sobre ciberdelito o la Directiva NIS son los mimbres sobre los que habría que seguir construyendo.

Otro aspecto a tener en cuenta es la cooperación; muchos de los adversarios son comunes a nuestros aliados. Las formas de ataque empleadas por el cibercrimen, el *hacktivismo,* el ciberterrorismo y la ciberguerra son en muchos casos sustancialmente las mismas, por lo que afectan de igual forma al sector público, a los ciudadanos, a las empresas y a las Fuerzas Armadas, y no conocen de fronteras. Hemos tenido varios ejemplos recientes de ciberataques a escala global, como han sido WannaCry o NotPetya.

cve: DSCG-12-CM-116

Por eso, esta cooperación no puede limitarse únicamente a la compartición de información sobre amenazas, sino que ha de extenderse a todos los demás aspectos que acabo de mencionar: gobernanza, persecución de los atacantes, formación, concienciación, adiestramiento, investigación, desarrollo. Se espera contar con una nueva Estrategia nacional de ciberseguridad para mediados del año que viene, lo cual propiciará una oportunidad excelente para poner en marcha un plan integral de ciberseguridad nacional que aborde todos estos aspectos que acabo de esbozar y alguno más. La Estrategia de ciberseguridad nacional, como bien saben, es básicamente un análisis de la situación y una evaluación de los riesgos y amenazas, de los que derivan a su vez unos objetivos y unas líneas de acción que permitan alcanzarlos. Pero es importante entender que en sí misma la estrategia no es más que una declaración de intenciones. De nada vale si tras ella no existe una identificación de medidas y acciones concretas, asignación de responsabilidades, medios y recursos —recursos económicos incluidos—, así como unas métricas para evaluar su grado de cumplimiento y de eficacia.

En este sentido, hace cuatro años ya tuvimos una oportunidad similar cuyo punto de partida fueron las líneas de acción que planteaba la Estrategia de ciberseguridad del año 2013. Tengo que decir, porque participé directamente en varios grupos de trabajo, que se hizo una labor excelente de desarrollo de sus seis líneas de acción, que se tradujo en todo ese proceso que acabo de mencionar. Pero al final, la verdad es que nos ahogamos en la orilla, porque el plan, que había sido desarrollado con enorme seriedad y un alto grado de detalle, nunca llegó a ser ejecutado, y en ello tuvo mucho que ver el cambio de legislatura. Hace unos días, mi buen amigo el coronel de la Guardia Civil, Luis Fernández Hernández, planteaba en esta misma sala la necesidad de un pacto de Estado de ciberseguridad, y no creo que sea una mala idea. Desde luego, daría esa estabilidad y continuidad que necesitaría ese plan de acción, que se presume tan ambicioso como complejo para su ejecución.

Voy a finalizar ya, a modo de síntesis, insistiendo en que España está en el vagón de cabeza en lo que se refiere a ciberseguridad, que tenemos un buen modelo de gobernanza y un elevado grado de madurez, y que se constata una seria preocupación e interés por la ciberseguridad en todos los sectores que se ha intensificado mucho en los últimos años. Pero también quiero recordar que nos enfrentamos a una amenaza muy compleja, muy activa, en continua evolución y crecimiento, que por la transversalidad del ciberespacio afecta a todos los sectores de actividad y a organizaciones, empresas y ciudadanos, y que en muchos casos, además, es incluso transnacional. Por tal motivo, es necesaria una alerta permanente y una acción coordinada en multitud de aspectos, entre los que destacaría mejorar las capacidades de defensa y resiliencia, la gobernanza, la formación, la investigación y desarrollo, la concienciación, la cooperación y el desarrollo normativo. Como ya he dicho, la nueva Estrategia de ciberseguridad nacional propiciará un marco excelente para continuar avanzando, y debemos exprimir al máximo esa oportunidad que se nos vuelve a ofrecer.

Muchas gracias por su atención. Quedo a su disposición para cualquier pregunta que quieran hacerme.

El señor **PRESIDENTE:** Empezamos el turno de intervenciones, en el que los portavoces de los diversos grupos expondrán sus posiciones y plantearán los interrogantes que consideren convenientes. A continuación le daré a usted la palabra y volveremos a hacer un brevísimo segundo turno, cerrando usted la comparecencia.

En primer lugar, tiene la palabra el representante de Esquerra Republicana, el señor Castellana.

El señor **CASTELLANA GAMISANS:** Me acojo a una de sus expresiones, la de la necesidad de una gobernanza global. De las comparecencias y de los debates que ha habido, se deriva que es evidente —bueno, no sé si es evidente, me gustaría saber si comparte esa opinión— que la gobernanza global es el talón de Aquiles de la ciberseguridad, porque si analizamos la capacidad de amenaza de los conceptos que usted ha enumerado —ha hablado de ciberdelincuencia, *hacktivismo,* ciberterrorismo y ciberguerra, pero no se ha referido a la ciberguerra—, yo creo que podemos afirmar que la principal amenaza para la ciberseguridad mundial son algunos Estados que están sentados en sillones de las Naciones Unidas. Por eso, ya que es un ámbito transversal en el que hay de todo —usted mismo ha dicho que a veces los directivos o directivas piensan que es una cuestión técnica, y no, es una cuestión completamente transversal—, la diplomacia tendría un espacio muy importante. Quisiera que cuantificara un poco qué amenazas vienen de los Estados, porque esto nos diría que más que una amenaza fantasma es una amenaza muy concreta. Usted ha hablado de Estados totalitarios, y supongo que quiere referirse a Estados autoritarios o a algunos Estados en forma de democracia que no respetan los derechos humanos.

cve: DSCG-12-CM-116

Por ejemplo, las acciones o las omisiones de ayer son las amenazas de hoy; los intereses geoestratégicos del mundo occidental de ayer han permitido ciertas cosas hoy. Me gustaría que valorase —seguramente no es una ciberamenaza para los ciudadanos del Reino de España—, el hecho de que el Estado chino tenga la capacidad de reconocimiento facial —la tiene todo el mundo ya hoy día—, que la utilice sistemáticamente para controlar dónde van y de dónde vuelven sus ciudadanos y que eso permita generar como un carné por puntos de quién es buen ciudadano y quien es mal ciudadano, cosa que les permitiría hacer una segunda revolución cultural como la que hizo Mao, aunque en lugar de apartar a todos, apartarían solamente a aquellos que tuvieran inquietudes colectivas para no reproducir el desastre económico que se produjo en ese momento.

También ha hablado de señalamiento público por las cuestiones de impunidad. Si la principal amenaza son los Estados, tenemos que acabar con esa impunidad de los Estados. Quisiera saber si tienen algunas recomendaciones que hacer o si hay alguna línea de trabajo que abra la diplomacia para que podamos estar en un espacio más pacífico.

Simplemente quería reivindicar una vez más, o si quiere usted desmentirlo, que el mito del *hacker* solitario no existe, que las capacidades para hacer ciberdaño o daño en el mundo real a través del ciberespacio son muy costosas, y que, por ejemplo, una de las principales amenazas a la seguridad es —me gustaría también que la valorase— la denuncia de que el año pasado la NSA, la Agencia de Seguridad Nacional de los Estados Unidos, perdió el control —vaya eufemismo— sobre herramientas muy potentes que utilizaba. Por ejemplo, si descubrimos un lanzamisiles no sé dónde, sabremos qué empresa lo ha construido y lo podremos imputar. Que herramientas desarrolladas en este caso en Estados Unidos acaben en manos de ciberdelincuentes o de ciberterroristas, al final quizás es una de las amenazas más importantes con la que nos encontramos en este mundo.

Gracias.

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

El señor Gutiérrez tiene la palabra.

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

Señor Cubeiro, en primer lugar quiero darle las gracias por su comparecencia y felicitarle por su exposición, que yo creo que ha sido muy clara. Coincido con usted en que no estamos tan mal, en que muchas veces todos somos muy derrotistas, y creo que algunas veces incluso la información que en ocasiones trasladamos a la sociedad no es la adecuada. Pienso que potenciar o poner en valor los instrumentos del Estado, de las empresas españolas, de la propia Administración es muy importante y resulta muy aconsejable. En ese sentido, le felicito por su intervención, que ha sido novedosa respecto de otras en las que nos amenazan con el hundimiento del mundo. Yo creo que todos somos conscientes de los riesgos y de las amenazas que supone el ciberespacio. Es evidente que el delito, o el ciberdelito, ha aumentado y está aumentando de forma exponencial; también es verdad que cada día es más fácil recurrir a la tecnología necesaria para cometerlo, y eso hace que la probabilidad de que personas o delincuentes accedan a tecnología que antes no tenían es cada vez mayor. Creo que la prevención, como usted ha dicho —coincido con usted al cien por cien— es fundamental, y dentro de esa prevención, la formación. Por eso me parece que lo que usted ha mencionado de la cultura de ciberseguridad y de cómo debe fomentarse desde las etapas más iniciales de la formación de nuestros menores, resulta esencial. Creo que se está haciendo algún avance en ese sentido.

Me gustaría saber si usted, que seguro que lo conoce mejor que nosotros —evidentemente nunca es una valoración total—, cree que esa es la línea, cómo se puede mejorar eso, de qué forma cree que se debería incorporar en el currículum de los menores esta formación, porque yo creo que la base para poder tener un usuario que de verdad esté bien formado es una buena ciberseguridad, porque la ciberseguridad al final es responsabilidad de todos. Y cuando digo responsabilidad de todos lo digo no solo por los usuarios, sino también por las personas que trabajan en las empresas con *software*. Pienso que aunque las empresas son responsables de dar formación a sus propios empleados, una mejor cultura de base sería lo ideal.

Me interesa conocer su opinión sobre una cosa que usted ha mencionado. Cuando habla de la ética del Estado respecto a la ciberdefensa, quisiera que profundizara un poco más sobre cómo cree que debe ser esa ética del Estado y qué le parece que puede poner en práctica el legislador para conseguir una buena ética. Me gustaría saber, cuando un Estado debe defenderse, hasta dónde piensa usted que llega esa ética, porque yo creo que en la guerra hay poca ética. Cuando uno se defiende, no sé yo hasta qué

cve: DSCG-12-CM-116

punto se llega en ese conflicto entre qué es ético o no lo es. Me gustaría profundizar en ello, porque evidentemente es un espacio de indefinición que, desde luego, es muy interesante.

En ese mismo sentido, también me gustaría conocer su opinión sobre cuál es el papel del fabricante. Al final, claro, para que haya una amenaza debe existir un dispositivo que tiene un *hardware* y un *software,* que es el que se utiliza, evidentemente, tanto para atacar como para defenderse. Quisiera saber hasta qué punto los Estados deben ser responsables de exigir a los fabricantes determinadas cosas. También me gustaría que nos hablara de la colaboración entre los fabricantes y los Estados, porque yo creo que ese es otro talón de Aquiles del que se habla poco; es decir, hasta qué punto Estados que pueden utilizar puertas traseras sobre determinados *softwares* que fabrican, que tienen acceso a esas propias puertas traseras, son capaces de utilizar, vamos a decirlo así, en su propio beneficio vulnerabilidades que los fabricantes, no digo que dejen aposta, pero que conocen que existen, ¿no?

Nada más. Simplemente me gustaría que me respondiera a esas dos cuestiones. De nuevo le doy las gracias por su exposición y, sobre todo, por mantener sobre esto un punto de vista distinto del que hemos percibido otras veces en esta Comisión. Muchísimas gracias.

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

La senadora Angustia tiene la palabra.

La señora **ANGUSTIA GÓMEZ:** Buenos días, señor Cubeiro, bienvenido a esta Comisión. Le deseo la máxima de las suertes en sus nuevas responsabilidades.

Me gustaría empezar por una pregunta muy concreta sobre la piratería marítima y lo que puede aportar su trayectoria al puesto que ocupa actualmente en el Mando Conjunto de Ciberdefensa. Ha colaborado no solo en el marco de la operación Atalanta, sino que a lo largo de su carrera se ha enfrentado a la resolución de situaciones de piratería. ¿En qué se puede colaborar desde el campo de la ciberdefensa? Creo que no me estoy equivocando, ¿verdad? ¿En qué se puede colaborar? Este es un aspecto que tal vez pudiese entrar en estos espacios del marco de defensa global, pero que muy pocas veces aparece mencionado específicamente en el campo de la ciberdefensa, y que sin embargo es muy importante por lo que atañe no solo a conflictos políticos, sino a conflictos económicos y a conflictos bélicos, incluso por las vinculaciones que en ocasiones pueda tener con el terrorismo. Nos gustaría conocer su opinión, y sobre todo cómo puede ayudar su experiencia a este respecto.

Entrando ya en el tema de la Directiva NIS, que usted mismo mencionaba durante su intervención, al leer el real decreto que traspone esta directiva, aprobado el pasado mes de septiembre —al que es cierto que hemos llegado un poco tarde, pero llegamos—, nos preocupa ver un carácter ciertamente militarizado, y sin embargo aparece muy poco respecto a los operadores jurídicos. Son los propios operadores jurídicos, jueces, fiscales, fiscalía, abogados, quienes quieren saber cuál es su función dentro de este espacio y han abierto un debate que a mí me resulta francamente interesante. Nos gustaría conocer su opinión sobre la propuesta que hacen precisamente los operadores jurídicos de empezar a valorar la reforma del Código Penal a raíz no solo de la Directiva NIS, sino del reglamento, del real decreto español.

Existe, evidentemente —esto no lo digo yo, lo dice usted mismo—, un carácter transversal dentro de la guerra híbrida. Por tanto, parece que solo integrando y coordinando los diferentes espacios de la inteligencia se podrá hacer frente a amenazas y a los espacios comunes. En concreto, en este momento, ¿sobre qué ataques, sobre qué espacios está trabajando operativamente el Mando Conjunto de Ciberdefensa en lo que se refiere a esta guerra híbrida?

En cuanto a la necesidad de profesionalización de la que se hablaba antes, el propio Mando Conjunto de Ciberdefensa participó el mes pasado en unas jornadas sobre estrategias de ciberseguridad y reservismo voluntario. Nosotros, más que reservismo voluntario, siempre hemos defendido y defenderemos la necesidad de formación, no solo, como se referían algunas intervenciones anteriores, como usuarios, sino a la propia especialización de trabajadores, de trabajadoras en el campo de la ciberdefensa. Evidentemente, las dotaciones presupuestarias serán imprescindibles para poder abordar el trabajo, y usted mismo llamaba la atención sobre esto en su intervención. La profesionalización, la especialización y, sobre todo, la capacidad de formación continua solo la dará un nuevo marco de formación en el sector, y debemos entender como marco de formación también la enseñanza reglada. ¿Cuál cree que es el papel del reservismo voluntario para poder hacer frente a las amenazas que se presentan, o simplemente, que es el marco en el que voy a entrar ahora, para dar respuesta a un espacio cada vez más enfocado a la comercialización de servicios y a la socialización de información para el conjunto de ciudadanos y ciudadanas? ¿Cuál es el papel que va a jugar esa formación necesaria y el reservismo voluntario?

cve: DSCG-12-CM-116

Por último, entro en ese marco al que me refería. Parece que cada vez más las operaciones, los programas desarrollados por la ESA van enfocados precisamente a la comercialización de la información; parece que el *big data* es ya un valor añadido enfocado a esta socialización de la información y cada vez más actores civiles, más experiencias, más sectores profesionales y más sectores estratégicos, energía, agricultura, pesca, etcétera, entran en esta necesidad de cobertura en el marco de la ciberseguridad. ¿Cuál es el papel que deben jugar las empresas en relación con la ciberseguridad? Me refiero en este caso a las responsabilidades civiles, a las empresas operadoras de telecomunicaciones. ¿Cuál es el papel que deben jugar en esta estrategia conjunta y cómo se relaciona con ellas el mando o qué importancia les da dentro de esta cuestión? Sobre todo, quisiera saber de qué forma entran precisamente en este espacio europeo que cada vez va más enfocado a esa socialización de la información para usos y fines civiles y, por tanto, comerciales. ¿Cuál es el papel que juegan? ¿Cuál es el grado de coordinación con esos espacios de la Unión Europea? Menciono específicamente, por ejemplo, el Programa Copérnico, que acabó resultando ser prácticamente de uso comercial; parece que toda la operación a partir de la puesta en marcha del programa Copérnico ha tenido fines comerciales, y con fines comerciales me refiero a un uso socializado de todos los sectores de la sociedad. ¿Cuál es su grado de implicación con estas operaciones conjuntas y cuál es el papel que juegan en cada una de ellas?

No me extiendo más, porque además creo que no me queda mucho tiempo. Le agradezco no solo su comparecencia de hoy, sino su exposición clara en esta Comisión. Gracias.

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

Tiene la palabra el señor Cortés.

El señor **CORTÉS LASTRA:** Capitán Cubeiro, bienvenido a esta Comisión. Antes de comenzar, quisiera agradecer al general Medina su trabajo hasta hace unos meses como comandante del Mando Conjunto de Ciberdefensa. Creo que su capacidad y trabajo han sido una de las claves en el avance tan significativo del Mando Conjunto de Ciberdefensa desde su inicio hasta la actualidad.

La verdad es que después de escucharle, capitán, me vienen a la cabeza afirmaciones que usted hoy ha hecho aquí en esta Comisión y que venimos escuchando también a otros comparecientes, por ejemplo, que el ciberespacio se ha convertido en un lugar peligroso en el que hay cada vez más amenazas, o que el ciberespacio lo inunda todo, que es al mismo tiempo un espacio artificial pero real, sin tiempo, sin fronteras, sin distancias, y que desde el punto de vista operativo siempre hay actividad y siempre hay ataques.

Pero centrándonos en su responsabilidad, en la misión permanente de defender el ciberespacio, dependiente del Ministerio de Defensa, donde el mando conjunto es una pieza combatiente en el ciberespacio, por decirlo así, que necesita una inteligencia táctica para poder operar, me gustaría plantearle cinco preguntas para saber cuál es el punto de vista que usted tiene al respecto. En primer lugar, quisiera preguntarle —espero que entre un poco a fondo porque a mí siempre me ha llamado la atención— cómo han conseguido integrar la capacidad operativa de ciberdefensa con las aportaciones que hace la fuerza conjunta de los Ejércitos de Tierra, del Aire y de la Armada. Creo que es importante que usted nos haga un resumen, al menos de estos cinco años, de cómo ha podido integrar esta capacidad operativa en ciberdefensa.

En segundo lugar, en su intervención ha venido a decirnos que la disuasión no funciona en el ciberespacio. Lo que quisiera es que usted ampliara un poco más los motivos de que esto sea así, y saber si hay alguna forma de cambiar esa situación.

En tercer lugar, y lo decía previamente, también quiero ahondar un poco en el tema de la ciberreserva, porque en los últimos meses hemos oído hablar mucho sobre esto. Sin embargo, según la fuente que escuchamos, los modelos difieren de una manera bastante notable. Quisiera saber, igual que la colega de Podemos, sobre qué parámetros debería definirse ese modelo de ciberreserva, cómo lo entiende usted.

En cuarto lugar, según informaciones que he recibido, la OTAN está comenzando a pensar en la forma de integrar capacidades ofensivas para operar en el ciberespacio. Quisiera que nos comentara algo al respecto.

Por último, ustedes han optado por disponer —lo decía al principio de su intervención— de un simulador avanzado propio, un *cyber range* o campo de maniobras, creo que así lo denominan ustedes, un poco en contra de esa corriente en las naciones de nuestro entorno de elegir cubrir una necesidad mediante una solución más compartida con varias naciones. Quisiera saber si puede decirnos en qué argumentos basaron esta decisión.

cve: DSCG-12-CM-116

Para terminar, haré un breve comentario sobre dos cuestiones. Por un lado, la cultura de la ciberseguridad. Creo que es necesario que sigamos ahondando en ello porque tenemos un enorme camino por delante. Mi grupo parlamentario siempre ha defendido utilizar como un acuerdo global las conclusiones de esta Comisión para conseguir aquello que usted dice, que creo que también es necesario para nuestro país, que es ese pacto de Estado de ciberseguridad.

Muchas gracias.

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

Señora Vázquez, tiene la palabra.

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

Agradezco la comparecencia del capitán de navío don Enrique Cubeiro. Antes de nada, para que conste en el Diario de Sesiones, me gustaría manifestar el reconocimiento del Grupo Parlamentario Popular al capitán. A lo mejor nos pasó desapercibido, pero algunos ya le conocíamos de otra época en la que estaba al mando del buque Patiño, creo recordar, con la operación Atalanta —quiero recordar también aquí a la fallecida ministra de Defensa en aquel momento, Carme Chacón—. Gracias a usted, capitán, por primera vez se ha juzgado y se ha condenado en España un delito de piratería. Vaya por delante el reconocimiento del Grupo Parlamentario Popular a su labor, a la del anterior Gobierno y a la de la fallecida ministra Carme Chacón.

Antes de preparar la comparecencia de hoy, en el mes de septiembre leí una entrevista suya en el suplemento *Retina* de *El País*, creo recordar, en la que usted decía que no somos conscientes de que la amenaza más importante está en las conexiones a Internet. Cuando ves ese titular te quedas y ya lees toda esa noticia. Creo que entrevistas como la suya, tanto en ese medio de comunicación como en otro que recuerdo, en *La Voz de Galicia*, de mi tierra, antes del verano, crean conciencia de ciberseguridad, que es lo que le falta a este país. Necesitamos que se hable, no solo en el Congreso, sino fuera de él, que gente como usted salga hablándoles a los españoles del problema que tenemos con la ciberseguridad, que es la principal amenaza a la que está expuesto en estos momentos cualquier país democrático estable. Ya no hablamos de una guerra híbrida, porque usted decía en alguna entrevista que a lo mejor la próxima guerra estaba a punto de un clic. Estamos hablando de cosas muy importantes, no solo para el Estado, sino para las empresas, para cualquier ciudadano que se puede ver afectado. Tenemos que creernos que esto es un problema.

Desde todas las instituciones, tanto desde el Incibe, como desde el Ministerio del Interior y del de Defensa, deben salir personas como ustedes, que están todos los días luchando, como dice, veinticuatro horas al día los 365 días del año, a crear conciencia. Entrevistas como las que ustedes conceden a los medios de comunicación crean conciencia de un problema que hasta ahora era desconocido. Hasta que apareció en mayo pasado el WannaCry nadie teníamos conciencia de esto, no se hubiera creado una ponencia de ciberseguridad en la Comisión de Seguridad Nacional.

Sé que desde que se creó en el año 2013 se ha hecho mucho. Otros Estados comenzaron en 2009, y usted hacía referencia en alguna entrevista al cibercomando de Estados Unidos, que no es similar al nuestro, y además tiene unos recursos ilimitados comparados con los nuestros. Tengo que felicitarle porque con los escasos recursos disponibles, en una situación de crisis como la que hemos vivido desde 2013 hasta ahora, se ha hecho mucho y ha sido gracias a personas como ustedes, que trabajan en los distintos organismos e instituciones y que han creído desde el primer momento en el problema de la ciberseguridad.

Respecto a lo del pacto de Estado, ya lo he dicho y lo reitero: hemos apoyado la convalidación del real decreto. Era un real decreto prácticamente copiado, excepto el párrafo tercero de la exposición de motivos, del proyecto de ley que el Partido Popular en el Gobierno había desarrollado de esa directiva. El Gobierno va a tener el apoyo total del Grupo Parlamentario Popular en ciberseguridad, no va a haber ningún tipo de duda.

Sí nos gustaría, si puede, que respondiera a alguna de las preguntas. Cuando hablamos de ciberdefensa también estamos hablando de un ciberataque, y a mí me gustaría preguntarle si España está preparada para producir armas —ojo, no se asusten ustedes— para defender el ciberespacio. Si no es así, ¿cómo podríamos disponer de esa capacidad de respuesta en caso de agresión?

Después me gustaría que nos comentara algo sobre la carrera profesional, si los equipos de ciberdefensa a los que usted hacía referencia están bien o si considera que se deberían modificar, que nosotros en la ponencia deberíamos hacer algún tipo de aportación sobre la carrera profesional.

cve: DSCG-12-CM-116

Me alegro de que ahora ya más partidos, más grupos parlamentarios se estén sumando a la idea que apareció hace meses de la captación de talento, de poner los medios; podemos hablar de ciberdefensa o de cibercooperante, si no queremos denominarlo con un carácter más militar, aunque no sé exactamente el nombre que le podríamos dar. Quisiera saber si usted considera que, al igual que en otros países de la Unión Europea como Francia, Alemania, Reino Unido, o el propio Estados Unidos, sin ser de la Unión Europea, tienen esas capacidades de talento puestas a disposición de los Estados —no digo que haya que ser altruista, pero a esa gente habría que compensarla—, habría que crear en España esta figura.

Después me gustaría conocer algo sobre los recursos asignados. Yo sé que no lo vamos a comparar con Israel, que es la máxima en recursos asignados a ciberseguridad, pero ¿considera suficiente los recursos de su departamento de Ciberseguridad o tendríamos que tener en cuenta desde el Congreso de los Diputados, ahora que se va a traer un proyecto de presupuestos, un incremento hacia el departamento de Ciberdefensa?

Usted hablaba de la viñeta de Peter Steiner que decía «en Internet nadie sabe que eres un perro». Yo hablo mucho de esto, del anonimato y de la identidad digital. ¿Considera que debemos avanzar ya hacia una identidad digital que nos dé tranquilidad cuando entramos en una red? Yo no tengo nada que ocultar y como yo no tengo nada que ocultar, me gustaría poder entablar una conversación con la otra persona que está del otro lado, sabiendo efectivamente quién es, si es una persona o es un perro. Me gustaría saber, si tiene alguna propuesta que nos pueda hacer al respecto.

Por último, hablaba sobre ciberataques o noticias falsas, quería saber si tienen constancia de algún ciberataque en España referido a noticias falsas o injerencias de algún país extranjero para desestabilizar o crear una opinión distinta en países democráticos de la Unión Europea.

Muchas gracias.

El señor **PRESIDENTE:** Muchísimas gracias, señoría.

A continuación tiene la palabra el compareciente para responder a las preguntas e inquietudes de los portavoces.

El señor **CUBEIRO CABELLO** (capitán de navío y jefe del Estado Mayor del Mando Conjunto de Ciberdefensa): Muchas gracias.

A ver si me acuerdo de las preguntas, he tomado aquí unas notas muy rápidas y no entiendo ni mi letra. Señor Castellana, ese modelo de gobernanza global es poco utópico porque estamos hablando probablemente de cuatro ideas completamente diferentes de cómo debería ser ese modelo y cada una de ellas están lideradas por un actor principal: Estados Unidos tiene una visión, la Unión Europea tiene otra diferente, China tiene otra distinta y Rusia tiene otra. Además, una cosa es lo que se dice en público y otra diferente lo que se hace en privado. En ese sentido, se sabe —lo he dicho en mi intervención— que cada vez hay más actores estatales en el ciberespacio. El Mando Conjunto de Ciberdefensa es un actor estatal, lo que ocurre es que está perfectamente sometido al escrutinio de la opinión pública y su actividad está perfectamente regulada por los poderes de un Estado democrático. Esto no es igual en otros países y no voy a cometer el error de citar qué países son, porque luego me encuentro con un titular de algún periódico y se me vuelve en contra.

Efectivamente, sí que hay una aproximación asimétrica a esas zonas grises de la legislación, en las cuales casi son las propias autolimitaciones que se pone una organización Estado a practicar esa actividad. Ante eso encontramos dos posiciones completamente diferentes: la posición de los Estados u organizaciones éticas y las que no lo son tanto. En ese sentido, ante una zona gris hay dos posibles opciones: una, decir «esto no está claro y no lo voy a hacer», o dos, decir «esto no está claro, voy a aprovecharme de ello y lo voy a hacer». Eso es lo que se está empezando a llamar en el campo de la normativa la guerra asimétrica, el término *asymmetric warfare*. Esta es una aproximación diferente a la normativa existente de las zonas grises. Por eso yo hablaba de esa ventaja que juegan esos Estados o esas organizaciones que no están sometidas a un escrutinio de la opinión pública, a los contrapoderes del Estado. Muchos de ellos utilizan el ciberespacio como elemento fundamental de actividad en apoyo a eso que se da en llamar guerra asimétrica. Ellos utilizan de manera coordinada y sincronizada todos los elementos del Estado para atacar o debilitar a un posible oponente, que lo puede ser en cualquier terreno, en el militar, en el económico, en el político o en el diplomático.

Ha dicho que el *hacker* solitario no existe, aunque yo no me atrevería a afirmar tanto. Hubo una época en que casi todos eran *hackers* solitarios y aunque yo no me atrevería a decir que no los haya, está claro que se tiende cada vez más a buscar organizaciones o que esos *hackers,* que antes eran solitarios,

cve: DSCG-12-CM-116

sumen sus capacidades o sus ambiciones. A partir de ahí, como dije antes, existe una casuística enorme en el ciberespacio, tenemos desde ese ecosistema, esa pirámide de ciberamenazas, hasta los chavales de toda la vida de la película de *Juegos de guerra,* los *wannabes* o los *script kiddies* que utilizan herramientas que puede encontrar uno fácilmente metiéndose en Google para capturar credenciales, penetrar en sistemas que no estén protegidos, activar cámaras webs y ese tipo de cosas.

A partir de ahí luego vamos creciendo, tal y como dije, con las grandes organizaciones y las famosas amenazas persistentes avanzadas que generalmente están asociadas a agencias gubernamentales militares y a inteligencia, muchas veces enfocadas a la obtención de información sobre el adversario. En ese sentido, la amenaza es de lo más heterogénea. Por ejemplo, el Ministerio de Defensa aunque está expuesto en alguna red de propósito general en Internet, no siempre se está defendiendo de agresiones que proceden de actores Estado. Al estar expuestos en Internet estamos expuestos a lo mismo que el resto, es decir, a todos los riesgos asociados a la navegación, como por ejemplo en el correo electrónico al robo de credenciales mediante campañas de *phishing* o de *spam,* y todo este tipo de cosas. Por tanto, a nuestra superficie de Defensa que es importante tenemos que sumar el que nos puedan llegar ataques de todo tipo. Un ataque se categoriza de acuerdo con su motivación o su intencionalidad. Muchas veces un ataque que persigue un beneficio económico no difiere mucho de uno que persigue la obtención de información. Al final, esa misma acción dependiendo de para qué y qué actores la desarrollen es la que la categoriza como ciberdelito, *hacktivismo*. Un ataque de degradación de servicios puede responder a cualquiera de ellas, depende de lo que se persiga y de quiénes son los actores.

Por último, me ha trasladado la cuestión del supuesto robo de las ciberarmas de la NSA. Hay una serie de informes de inteligencia que atribuyen una de esas famosas amenazas persistentes avanzadas (APT) a grupos multidisciplinares muy capacitados que cuentan con muchos recursos y que no son solo capaces de explotar vulnerabilidades sino incluso de crearlas. De todas esas APT —se conocen bastantes a través de informes de inteligencia que son conjeturas basadas en evidencias porque yo no tengo ninguna evidencia de que así sea— la NSA contaría con una que se llamaba Equation Group, que probablemente fuera la más sofisticada y cualificada de todas las que existían según esos informes de los analistas de ciberinteligencia. Pues bien, supuestamente las ciberarmas de la NSA fueron sustraídas al parecer por un trabajador de una tercera empresa que tuvo acceso a aquello. Evidentemente, el que las ciberarmas o las cibervulnerabilidades identificadas por probablemente el actor más importante y con más capacidades que existía hace dos años, coloca en una situación de un riesgo mayor todo el juego comercial del espacio. De repente se ha liberado conocimiento que estaba al acceso de muy pocos y muy cualificados, lo cual no es una cosa buena. Espero haberle contestado a todo. Gracias.

En cuanto al representante de Ciudadanos, no he querido ser muy fatalista o alarmista. Efectivamente, tenemos que ver todo lo bueno que hemos hecho, que es mucho, pero también hay que pensar que este es un terreno en el que queda por hacer mucho más porque la situación es muy complicada, por no decir otra palabra peor. Yo creo sinceramente que es muy importante que desde pequeños formemos a nuestros niños sobre conocimiento de algo que ya forma parte fundamental de sus vidas, ya que hay muchos niños que se comunican más a través del ciberespacio que con la propia presencia física. Al igual que inculcamos a los niños unas nociones de seguridad vial, sería importante también educarles en los riesgos de la navegación. Al igual que el señor presidente tiene el título de Patrón de yate, para navegar por el ciberespacio sería importante que tuviéramos algún tipo de certificación que nos diga que esa persona tiene conocimientos suficientes para saber dónde se mete. El conocimiento de lo que determinadas acciones nuestras pueden suponer para nuestra seguridad y privacidad deberían partir desde los primeros escalones.

Hablábamos de la ética de los Estados, pero creo que en parte ya he contestado al responder a la pregunta anterior. Usted ha afirmado que en la guerra no hay mucha ética. ¿No la hay? No lo sé, pero debería de haberla. Desde luego normas tenemos y el cumplimiento exhaustivo de todas las normas internacionales y nacionales por parte de las Fuerzas Armadas le aseguro que es una auténtica obsesión.

También se ha referido a si hay que involucrar a los fabricantes en este tema. Desde luego que sí. Hemos hablado de que existen varias decenas de miles de dispositivos conectados a Internet, el famoso Internet de las cosas. Tenemos televisores, marcapasos y pulseras inteligentes, todo eso cuando se desarrolla se hace pensando exclusivamente en la funcionalidad, nadie piensa en seguridad e incluso se hace también con el *software*, cuando sabemos que ya existen patrones para el desarrollo seguro de *software* que deberían ser exigidos. En este caso la normativa, no sé si a nivel europea pero sí a nivel nacional, debería exigir estos desarrollos. ¿Qué ocurre? Que normalmente esto supone mayores

cve: DSCG-12-CM-116

imposiciones a los fabricantes, que se traduce en un retraso en el desarrollo de productos y un mayor coste, con lo cual al final puede ser que el propio usuario o ciudadano sea el que lo pague.

Ha hablado también de las puertas traseras, algo en lo que estamos permanentemente en riesgo. En España el principal criterio a la hora de adquirir material informático o de ciberseguridad en la Administración General del Estado en los últimos años ha sido el coste económico. Hay determinados países que tienen vetados a determinados fabricantes, pero aquí en España eso es verdaderamente complicado porque para vetar a un fabricante hace falta algo en lo que apoyarme para que legalmente pueda dejar a un fabricante fuera. Por tanto, solo queda ser muy cuidadoso en la definición de los requisitos a la hora de contratar, exigir garantías a los fabricantes y desde luego poner todas las medidas para que aunque ese material que yo he adquirido venga trufado de fábrica, como dicen mis muchachos, que venga con puertas traseras, yo sea capaz de detectar esos comportamientos anómalos y ponerles solución. Con esto creo que he contestado también a sus preguntas.

La senadora Angustia me ha preguntado si mi trayectoria con los piratas puede ser utilizada directamente en mi experiencia en el Mando Conjunto de Ciberdefensa. Bueno, el Mando Conjunto de Ciberdefensa es una unidad eminentemente técnica, pero como todo, en los niveles más altos de decisión el conocimiento técnico no es tan importante y pasa a ser secundario a favor de otros condicionantes, como por ejemplo haber tenido experiencia en operaciones, el estar habituado en dirigir grupos de personas, la visión más general de la organización, tener una visión más amplia de cuáles son las relaciones entre actores. Ese tipo de cualidades, que yo he adquirido debido a mi larga experiencia profesional porque ya voy siendo viejo, son algo que yo puedo aportar, pero mi experiencia en operaciones navales realmente no tiene una aplicación especialmente directa en este campo, que es completamente diferente.

Sí que existen en los dos campos piratería, hay piratería informática y hay piratería somalí, por ejemplo. Ambas se producen por el mismo efecto: la falta de una autoridad que pueda ejercer su carácter disuasorio. En Somalia la piratería empezó a decrecer cuando disminuyó drásticamente el índice de éxito de los piratas, ya que en los años 2008 y 2009 tenían un índice de éxito del 50 %, es decir, de cada dos intentos se producía un secuestro. Sin embargo, cuando en el año 2012 se incorporaron los equipos de seguridad a bordo el índice empezó a bajar radicalmente e incluso los piratas empezaron a ver que se estaban jugando la vida porque muchos de esos equipos eran muy expeditivos en sus actuaciones, por decirlo de una manera educada. Mientras no consigamos potenciar la disuasión —luego hablaré del tema porque fue otra de las preguntas que me han hecho—, estará muy complicado acabar con ese efecto llamada que hace que el ciberdelito sea ahora mismo el delito más lucrativo y probablemente el que quede más veces impune.

También me ha preguntado por la Directiva NIS y me ha dicho algo que no he sabido interpretar bien, referido a que tiene un carácter militarizado el real decreto. No sé a qué se refiere, lo único que le puedo decir es que identifica en uno de sus artículos de manera bastante escueta al Mando Conjunto de Ciberdefensa como unos de los CERT que tiene responsabilidades a nivel nacional y cuyo ámbito de actuación es el Ministerio de Defensa, así como aquellas otras infraestructuras que se le puedan encomendar, que es en lo que estamos trabajando ahora. Actualmente trabajamos en grupos de trabajo para identificar cuál es ese ámbito de actuación, pero obviamente está enfocado a aquellas infraestructuras a las que un ciberataque podría poner en riesgo aspectos de seguridad nacional como puede ser el propio funcionamiento u operatividad de las Fuerzas Armadas.

Ha hablado también de la reforma del Código Penal. Efectivamente, las reformas del Código Penal normalmente tienen que ir por detrás de los acontecimientos. No podemos legislar sobre futuribles, o sobre cosas que todavía no se han producido, pero sí estar preparados para reaccionar cuanto antes. En este sentido, la legislación siempre va un poco por detrás y a veces mucho por detrás. Es muy importante definir nuevos tipos delictivos que van evolucionando, ya que van apareciendo nuevos delitos y hay que ir actualizando el Código Penal para que los responsables paguen por ellos, en el caso de que podamos demostrar, más allá de toda duda razonable como exige nuestro Código Penal, la autoría de alguna acción.

Me ha preguntado por el papel del Mando Conjunto de Ciberdefensa en cuanto a la guerra híbrida. Al igual que la amenaza híbrida se materializa de una forma coordinada y sincronizada de muchos actores y un Estado, a nuestro entender la contraguerra híbrida o la defensa ante la amenaza híbrida debe contemplar algo parecido, debe de actuar sobre esos elementos de defensa como una orquesta bien engrasada en la que cada elemento del Estado se ocupe de la parte que le compete, pero manteniendo

cve: DSCG-12-CM-116

una coordinación que tiene que estar en un nivel muy alto de decisión. En ese sentido el Mando Conjunto de Ciberdefensa se ocupa de su ámbito de actuación, que es fundamentalmente todo aquello que tenga que ver con ciberataques a sistemas propiedad del Ministerio de Defensa, o a otros que se le pueden encomendar porque puedan afectar en algún caso a la defensa nacional.

En este sentido es importante que hagan una distinción porque las noticias falsas no son ciberamenazas, algo que en mi opinión a veces se confunde. Una ciberamenaza es algo que afecta a un *software* o un *hardware,* pero la difusión de un bulo realmente no es materia de ciberseguridad. Otra cosa distinta es que se produzca a través del ciberespacio, o que en algunos casos se utilicen ciberataques para esa difusión. Por ejemplo, supongamos que una difusión de una noticia falsa se hiciera suplantando la identidad del Ministerio de Defensa en su cuenta de Twitter, eso sí que sería una cuestión que tendría que ver con ciberseguridad. Sin embargo, que un bulo se difunda a través de Twitter o Facebook, que se retuitee y se pase a través del wasap, eso no es un asunto de ciberseguridad. Esto es algo distinto, aunque todo esté muy entrelazado y en ocasiones sea difícil establecer límites y fronteras.

Me ha planteado alguna cuestión sobre la ciberreserva, una pregunta que también se ha repetido por parte de varios portavoces. En España se empezó a hablar de la ciberreserva en el año 2015, a partir de un artículo que escribió el señor Enrique Ávila —que también ha comparecido— en la revista *CIBER Elcano,* donde hablaba de la ciberseguridad. Él entendía la ciberreserva como una posibilidad de aprovechar talento, especialmente talento joven. En los primeros desarrollos de esa idea (por algún motivo que le tendrán que preguntar a quienes la desarrollaron, proceso en el cual el Mando Conjunto de Ciberdefensa no intervino para nada, no es algo que haya partido del Ministerio de Defensa ni del Mando Conjunto de Ciberdefensa, sino del ámbito particular) se empezó a hablar de una ciberreserva que estaría adscrita o gestionada por el Mando Conjunto de Ciberdefensa. Esta idea empezó a ser recogida por la prensa de una manera que no se entendió bien, o quizás se explicó mal, que pueden ser las dos cosas. Hasta el punto de que el año pasado más o menos a estas alturas de año habíamos conseguido que calara en la opinión pública una idea basada en tres ideas fundamentales, aunque las tres eran falsas para mí, ya que hablábamos de 2000 *hackers* gratis. Yo ya he defendido en alguna intervención que ni son 2000, ni son *hackers,* ni son gratis.

Si me pregunta si considero que la ciberreserva es una buena idea y cómo la llevaría a la práctica, le voy a dar mi opinión particular de Enrique Cubeiro, ciudadano español, no es la del Ministerio de Defensa ni la del Mando Conjunto de Ciberdefensa, que ignoro qué postura tienen. En mi opinión, esta idea no es nueva y ya existe en varios países de nuestro entorno y cada uno la ha adaptado a sus condicionantes y a su cultura. El primero que la adaptó fue Estonia. Hasta el año 2007 o 2008 los únicos concienciados en ciberseguridad y ciberdefensa del mundo eran la banca, porque iba a su cuenta de balance, y Estonia, porque había estado prácticamente dos semanas o tres *offline*. A partir de ahí Estonia creó un entramado de personas que voluntariamente decidieron poner sus conocimientos al servicio del Estado para casos similares. Francia tiene una ciberreserva de dos modelos. Por un lado, un modelo que está muy enfocado a esa cibercolaboración de la que hablábamos, gente que pone su conocimiento y voluntad, por ejemplo, para impartir conferencias en colegios o este tipo de actitudes para crear una cultura de seguridad nacional —estamos hablando del orden de centenas de personas—, y por otro lado, hay un pequeño número de personas —estamos hablando del orden de decenas— que trabajan en aspectos operativos, que trabajan para la unidad homóloga en Francia a lo que es el Mando Conjunto de Ciberdefensa.

¿Yo cómo lo veo? Veo que puede haber situaciones en las que los recursos del Estado pueden verse superados y tenemos varios ejemplos que ya se han producido en Estonia, Georgia o Kyrgyzstán. Han existido ya varios ataques sostenidos a Estados en los que hubiera sido deseable tener esa reserva, lo que tengo en el banquillo y disponer de él en un caso excepcional. Obviamente, no se puede improvisar de la nada, es decir, que yo para activar una ciberreserva necesito haberla tenido preparada para lo cual nosotros pensamos, porque hemos hecho un ejercicio intelectual sobre la ciberreserva ya que veíamos que se nos podía asignar, cómo nos gustaría que fuese ese modelo. Estamos hablando de un número muy reducido de personas, igual que hicieron los franceses. Hablo solo de decenas porque gestionar dos mil personas exige un departamento de recursos humanos que probablemente exceda en tamaño al propio Mando Conjunto de Ciberdefensa, ya que es imposible gestionar a dos mil personas, con todo lo que conlleva aspectos como seguridad y demás.

Esas personas no tienen que ser *hackers,* tienen que responder a un montón de perfiles, que ya hemos visto que están relacionados con la ciberseguridad. Hay un montón de profesiones y especializaciones, por ejemplo hay gente especializada en Derecho del ciberespacio. Necesitamos gente

cve: DSCG-12-CM-116

experta en ciberseguridad en su perfil defensivo, más que atacante. Estamos hablando de una situación de emergencia en la que el Estado es atacado. Tenemos que tener perfectamente organizados, conocidos e integrados y previamente investigados a ese número de personas, que además tienen que ser conscientes de que si se apuntan a esto, su disponibilidad tiene que ser muy elevada. Es decir, no puedo apuntarme y decir «hoy no me viene bien», por lo que sea. Por tanto, si alguien da su nombre y se apunta a esta ciberreserva, tiene que saber que está comprometiendo su disponibilidad.

Por último, creemos que puede haber dos opciones, dependiendo de si al final esta ciberreserva de adscribiera al Mando Conjunto de Ciberdefensa. Se podría optar por dos modelos: un modelo civil que trabajaría en aspectos no relacionados directamente con las operaciones militares y un modelo militar similar al que ya existe de la reserva voluntaria militar. Estas son un poco las ideas sobre las que yo mismo me he hecho un ejercicio de *brainstorming* para ver hacia dónde vamos, porque hubo un determinado momento en que pensé que esto se me venía encima y que yo lo iba a tener que gestionar. Lo lógico fue tratar de adaptarlo a lo que yo pensaba que debía de ser, que tenía que ser muy eficaz, muy eficiente y muy enfocado a la operatividad y a un caso excepcional no para el día a día, sino para un caso excepcional en el que los medios y recursos propios se vean superados. Asimismo, hace falta crear una relación de confianza mutua y un *quid pro quo*. En ese sentido, hace falta que esas personas convivan con nosotros algún tiempo —estoy hablando de una hipótesis si se crea esto— durante unos periodos de activación anuales que pueden coincidir con ciberejercicios. Los ciberejercicios fortalecen mucho la integración y la confianza, ya que jugar como parte de un equipo ayuda a todo este tipo de aspectos.

Por último, de gratis, nada. Nadie se va a enriquecer con esto, pero desde luego habrá una compensación económica, que teniendo en cuenta que ya existen en otros modelos en el ámbito de la reserva militar, me imagino que se ajustará a ello. No se trata de que nadie lo haga gratis ni de que nadie pierda dinero. Habrá una compensación con la que nadie se hará rico, pero compensará razonablemente ese esfuerzo, dedicación y disponibilidad puesta al servicio de quien sea. También he oído otros modelos que lo adscriben al Ministerio del Interior. Yo no tengo ninguna idea preconcebida, creo que es algo positivo e incluso podría haber varios modelos funcionando simultáneamente.

Me ha hablado del *big data* y de los operadores. El otro día asistí a una conferencia de nuestro *hacker* nacional más famoso que se llama Alonso y hablaba de este mismo asunto. Ahora mismo el planeta o Estado más importante del mundo es Facebook o Google, que tienen varios miles de millones de habitantes. Está empezando a haber un traslado de poder de los Estados a empresas, empresas que fundamentalmente basan su poder en el manejo de los datos, que se obtienen de muchas maneras. Cuando estamos jugando al Candy Crush nos aparece una publicidad, cada vez que descargamos una aplicación para utilizar en nuestra *tablet* estamos aceptando que datos sobre nuestro comportamiento que se están produciendo a través de ese dispositivo pasen a determinadas empresas que teóricamente los desagregan, ya que les interesa el dato de que alguien ha hecho tal cosa. Pero sabemos que tampoco es así, porque muchas veces tenemos que aceptar cosas, como cuando nos dicen, por ejemplo: ¿Quiere usted que se permita recopilar datos para ofrecerle una publicidad más de su interés, y que no sea la genérica para todos? Pues bien, todo esto hay que regularlo, y ahora mismo estamos hablando de empresas trasnacionales que operan en todo el mundo y que, obviamente, requieren ese modelo de gobernanza global del que antes hablaba, que creo que es muy complicado pero que no por eso debemos renunciar a obtenerlo, y que obligará a buscar ese equilibrio razonable en cosas tan importantes como la privacidad, el derecho al olvido, todo este tipo de cuestiones sobre las que no somos conscientes de la cantidad de información acerca de nuestra vida que dejan nuestros dispositivos y los rastros. Se puede saber perfectamente de una persona a través solo de su geolocalización si está enfermo o no, dónde trabaja, dónde vive, si tiene un amante; todo ese tipo de información se puede obtener solo a través de la geolocalización. Entonces, hay que poner algún tipo de control a esto.

Creo que he contestado a todas sus preguntas. No sé si queda alguna o si lo he hecho de la manera que usted estimaba que era la adecuada.

Señor Cortés, por supuesto, comparto con usted el sentimiento de agradecimiento y admiración hacia el general Medina, que, como ya he tenido ocasión de decirle, es quien pilotó la nave desde el hangar o incluso desde el taller donde la construimos hasta la cota de crucero. Su liderazgo ha sido fundamental a la hora de crear esta unidad, como digo, una unidad nueva que operaba en un ámbito nuevo y en la que muchas veces partíamos de un papel en blanco.

En cuanto a la integración de la ciberdefensa con las capacidades operativas convencionales y cómo lo hemos conseguido, en primer lugar dándonos a conocer. Ha sido importante hacer una labor de

cve: DSCG-12-CM-116

educación, en el sentido de indicar cuáles son las ciberamenazas y cuáles son las modalidades de actuación que podemos hacer tanto en el plano defensivo, como en el de obtención de información y en el plano ofensivo; capacidades, además, que están vivas, o sea hemos ido creciendo en capacidades. Por tanto, fundamentalmente, hemos hecho entender a nuestros mandos operativos de qué va esto, qué nos pueden pedir, en qué plazos, este tipo de cosas. A partir de ahí, la ciberamenaza ya se considera a la hora de desarrollar un plan de operaciones. Hay un anexo específico para ciberdefensa en todo plan de operaciones, en el que se establecen las acciones que se van a hacer, los medios de que se va a disponer, cuáles son las cadenas de mando, qué informes hay que hacer, o sea, la ciberdefensa ya está contemplada como uno más, como un ámbito más en el que hay que trabajar, en el que se puede operar y en el que hay que defender los activos propios de la acción del adversario; y, al mismo tiempo, los activos del adversario podrían ser, cuando se den las condiciones, atacados a través de este nuevo ámbito.

En cuanto a la disuasión, me pedía una aclaración. He dicho que en el ciberespacio no funciona, y esto es absolutamente así. La disuasión, en términos generales, se basa en dos pilares: la disuasión por negación, que es poner las cosas difíciles al atacante, que en ocasiones en el campo de la ciberdefensa se basa en poner muchas barreras técnicas —cuantas más barreras técnicas, más difícil es penetrar en mis sistemas—, y la disuasión por represalia, que viene a ser como: ojo, que, como hagas algo y te pille, tendrás el castigo correspondiente. ¿Qué ocurre? En primer lugar, está claro que, cuando en la mayoría de los casos no podemos hacer una atribución más allá de toda duda razonable, no podemos ejercer la disuasión por represalia, porque no tenemos conocimiento concreto de quién ha sido el atacante. Esto ya nos crea un verdadero problema: si no sé quién me ha atacado, no puedo responder. En otras ocasiones la respuesta además tiene que estar condicionada a una continuidad temporal que exige, por ejemplo, el ejercicio de la legítima defensa: yo no puedo ser atacado, dedicar un mes a analizar ese ataque y a continuación responder o dar respuesta; tendré que responder de otra manera, por ejemplo poniendo una denuncia en un juzgado, no podemos atacar en el ciberespacio. O sea, el Mando Conjunto de Ciberdefensa está sometido absolutamente a todo lo que es el control de la violencia por parte del Estado y en referencia a todas las garantías que hay que poner para que ello sea así. ¿Qué ocurre? Últimamente estamos empezando a ver que algunos Estados, sobre todo de corte anglosajón, como Canadá, Australia, Holanda y Reino Unido, han hecho acusaciones públicas, políticas o a través de canales de Asuntos Exteriores, diplomáticos sobre determinadas acciones que han atribuido a determinados actores. Empiezan a defender la idea de que la atribución no es tanto un problema técnico, que yo pueda demostrar con indicios obtenidos en una investigación digital profunda que determinada acción la ha cometido determinado actor, sino que con un número razonable de evidencias ya puedo efectuar un señalamiento público de que este actor ha producido tal estado, y eso está cambiando un poco el paradigma de lo que venía sucediendo hasta ahora, ya que prácticamente en las acciones no quedaba otra que aguantarse.

Sobre la ciberreserva, creo que ya he hablado bastante.

En cuanto a la integración de capacidades ofensivas en la OTAN, como saben ustedes, la OTAN no tiene fuerzas, no tiene barcos, no tiene aviones; bueno, algún avión tiene, pero realmente las fuerzas de la OTAN se forman a través de las aportaciones que hacen las naciones. En este sentido, se está empezando a hablar últimamente de la posibilidad de crear unidades capaces de efectuar acciones ofensivas en el ciberespacio integrando recursos proporcionados por las naciones. Esta es una idea sobre la que está bien que empecemos a pensar, aunque realmente la veo difícil de llevar a la práctica. En primer lugar, no es lo mismo incorporar un barco, que todo el mundo sabe lo que hace o lo que es capaz de hacer, un avión o un carro de combate que algo tan etéreo o tan heterogéneo como son capacidades de ataque. ¿Qué estoy prestando? ¿Estoy prestando cerebros, personas? ¿Estoy prestando ciberarmas? ¿Estoy prestando infraestructuras? No está claro. Haciendo un poco de trabajo intelectual sobre el tema, una de las ideas que se nos ocurre es relativa a cuando durante años la OTAN ha tenido sus *standing forces,* por ejemplo la STANAG *for land* o la STANAG *format,* agrupaciones de barcos —yo he vivido en ellas— en las que se integraba un barco que prestaba una nación durante tres o cuatro meses a esta organización, que fundamentalmente trabajaba en lo que era integración, el engrasamiento de lo que suponía trabajar en coordinación y en equipo, que creaba unas relaciones buenas de confianza y también se traducía en una mejora del comportamiento operativo de aquellas unidades. Se me ha ocurrido que algo parecido se podría hacer, pero para ello tendríamos que categorizar unidades de ciberdefensa en algún tipo, que una unidad de ciberdefensa se compusiera de cuatro personas, determinado equipamiento y fuera capaz de llevar a cabo determinadas habilidades. Esta es la primera idea que se me ha ocurrido

cve: DSCG-12-CM-116

sobre este tema, que, desde luego, ahora mismo está empezando a considerarse, con lo cual evolucionará con el tiempo hacia algo concreto.

Por último, me ha preguntado por el *cyber range,* por qué hemos optado por un *cyber range* propio, en lugar de, como han hecho otras naciones, ir a una solución de *pooling and sharing,* una solución compartida. En 2014 o 2015 tuvimos que tomar una decisión al respecto. Para entonces el Mando Conjunto de Ciberdefensa ya tenía un *cyber range* bastante evolucionado, bastante maduro, en el cual se habían gastado bastantes recursos, que provenían de la etapa anterior, porque el Mando Conjunto de Ciberdefensa de nutrió en un principio de gente que provenía de la división CIS del Emacon, y en aquel momento se nos ofreció participar en un proyecto multinacional de un *cyber range*. Como he dicho al principio, nuestro *cyber range* apoya desde el adiestramiento básico individual al adiestramiento múltiple avanzado, es capaz de soportar ejercicios muy complejos e, incluso, de apoyar el planeamiento operativo, reproduciendo escenarios reales. En ese sentido, al disponer de un recurso que no estaba muy claro que nos fuera a costar menos haciéndolo solos que acompañados —cuando uno va a un proyecto acompañado, le dicen lo que va a pagar al principio, y luego acaba pagando mucho y está sometido a los caprichos de las catorce naciones que participan en el proyecto, que cada una busca responder a su necesidad—, era muy importante disponer de absoluta soberanía, absoluto control sobre ese simulador y, al mismo tiempo, mantener la reserva sobre lo que en él se llevaba a cabo, porque, entre otras cosas, se practicaba adiestramiento ofensivo y se probaban capacidades ofensivas. Por lo tanto, creo que fue una decisión muy inteligente, y prueba de ello es que nosotros tenemos un simulador funcionando y operativo y los Estados que se embarcaron en esa aventura no lo tienen.

Respondiendo a la señora Vázquez, hemos hablado de la necesidad de una conciencia nacional de ciberseguridad. Países concienciados en ciberseguridad, Estonia y Georgia; probablemente ahora mismo son los dos países más maduros en ciberseguridad. Aquí solo aprendemos cuando nos han dado, de una manera un poco reactiva. En WannaCry nos dieron, nos dieron un poco a todos, se repartió bastante. España, que, como saben, fue uno de los primeros Estados —organizaciones y empresas españolas fueron de las primeras en sufrir los efectos del ataque—, unos días después no estaba en el *top* 20 de naciones que habían sufrido el impacto en mayor medida; eso indica una madurez de nuestra cultura. Pero WannaCry fue en muchos aspectos una llamada de atención, y en muchas empresas y organizaciones se empezó a pensar en ciberseguridad a raíz de sus efectos, aunque luego hemos sabido que fue un ataque no demasiado complicado, que su impacto podía ser muy grande si uno tenía bajas las defensas pero que realmente era fácil de neutralizar.

Ha comentado que en una de mis entrevistas decía que la próxima guerra comenzará con un clic. Estos son los riesgos de someterse a entrevistas. Realmente ese titular tan llamativo respondió a una pregunta que me hizo el periodista, que fue directamente: ¿Usted diría que la próxima guerra comenzará con un clic? Y yo contesté: Es probable. Y a partir de ahí se me entrecomilló: «Y la próxima guerra comenzará con un clic». En este sentido, ya he visto que algunas de mis declaraciones luego son interpretadas muy curiosamente.

Me ha pregunta cómo se obtienen ciberarmas, cómo se obtienen capacidades de respuesta. La capacidad de respuesta en el Ministerio de Defensa la tuvimos que crear prácticamente de la nada, porque, así como sí existía una cultura y medios muy maduros sobre seguridad informática, *information assurance,* que fue la evolución de la parte defensiva de la ciberdefensa, en la parte de ataque realmente trabajamos desde cero, hubo que crearla de la nada. ¿Y cómo la creamos? Voy a hacer un símil un poco curioso, no sé cómo explicarlo. Es como si ustedes ahora en el Congreso de los Diputados tuvieran que organizar una orquesta. La formarían con la gente que sabe tocar el violín y otros instrumentos en su vida particular, en su vida privada. Nosotros en principio nos dotamos de lo que llamo *hackers* —esta es una palabra que tiene diversas acepciones, y para mí es experto en intrusión de sistemas—, gente que tenía conocimientos sobre ingeniería social porque desde pequeños lo practicaban en sus ratos libres, o sea, que tenemos *hackers* por afición. Luego fue relativamente sencillo que con el apoyo de estos y partiendo de los *hackers* éticos, que hasta entonces estábamos utilizando sobre todo en la parte defensiva —expertos en *pentesting* y en *hacking* ético—, se convirtieran en medios, en recursos humanos para la capacidad de respuesta ofensiva en el ciberespacio.

¿Cómo se obtienen las ciberarmas? En parte, de una manera parecida, y hay muchas formas de obtenerlas. Primero, las que se pueden obtener uno poco menos que buscando en Google. A partir de ahí, las que usa el adversario para atacarme, porque al final no estamos hablando de algo físico, estamos hablando de unas líneas de códigos y de unos métodos para introducirlas. Hay también tecnologías de

cve: DSCG-12-CM-116

doble uso: las mismas cosas que se usan para hacer test de penetración pueden servir para desarrollar un ataque, siempre y cuando, como digo, el objetivo no tenga unas defensas muy maduras o sofisticadas; puede valer para atacar blancos poco defendidos. También se pueden hacer desarrollos propios; tenemos desarrolladores de *software* que son capaces de desarrollar esas herramientas. Normalmente, una ciberarma se compone de dos partes: lo que se llama *payload* y el *exploit*. Es lo que permite llevarlo al destino y lo que hace que en el destino haga algo. Igual que un misil lleva un lanzador y la carga explosiva, de forma parecida sería una ciberarma: la manera de introducirlo en el sistema y lo que hace en el sistema objetivo. A partir de ahí, también se podrían obtener de otras formas, que, llegado el caso, se podrían activar. Creo que con esto, sin contar información clasificada, estoy dando una idea más o menos de cómo se pueden obtener.

Sobre la carrera profesional, ahora mismo nosotros tenemos que jugar con los mimbres de nuestra propia normativa, y no se adaptan demasiado bien a nuestras necesidades, por decirlo de una manera suave. Realmente, en cuanto a la Ley de la Carrera Militar, nuestros procesos de evaluación no sé si decir que penalizan pero, por lo menos, no benefician la especialización y el permanecer mucho tiempo en un determinado tipo de unidad. Por otra parte, para lograr especialistas cualificados en ciberdefensa es absolutamente imprescindible contar con una enorme continuidad y especialización, que solo se consigue manteniendo a la gente desde el principio hasta el final de su carrera en este ámbito operativo. Hoy en día es algo en lo que tenemos que trabajar, pero la Ley de la Carrera Militar y toda la normativa que la desarrolla dejan poco campo a las excepciones, precisamente porque prácticamente habría que considerar todo como excepcional. Podríamos aplicar excepciones al arma submarina, al arma aérea, a un montón de campos de actividad que están en situaciones parecidas.

Podríamos mejorar también el reclutamiento y la retención. El hecho de que el Mando Conjunto de Ciberdefensa pertenezca al ámbito conjunto significa que está integrando personal que procede de los Ejércitos y de la Armada, en un momento además en el que se está potenciando todo lo conjunto, con lo cual rivalizamos en esa obtención de recursos de unos Ejércitos y de la Armada que obviamente han sido creados para su utilización dentro de su propio ámbito, no en conflicto pero sí en un proceso de rozamiento y discusión, del cual tampoco salimos muy beneficiados. Obviamente, nuestra plantilla tiene que crecer y habrá que buscar las maneras de llevarlo a cabo.

Hemos hablado también de la ciberreserva y del cibercooperante. Ya existen organizaciones que están fomentando la cibercooperación. El Incibe tiene un programa de cibercooperantes enfocado un poco a esto que antes decía sobre mejorar la concienciación, por ejemplo, dando charlas y conferencias en colegios y universidades para mejorar ese conocimiento acerca de los riesgos que especialmente tiene Internet.

Sobre asignación de recursos, realmente no me quejo para nada de los que tiene asignados el Mando Conjunto de Ciberdefensa. Tenemos un presupuesto que, siendo muy modesto, nos permite alcanzar nuestros objetivos. Sí podría buscarse un mejor uso de esos recursos, y me explico. Ahora mismo no existe una partida presupuestaria que se llame ciberdefensa; el presupuesto del Mando Conjunto de Ciberdefensa está diluido en diferentes casillas presupuestarias, pero no hay una que se llame de así. Esta ha sido una aspiración por la que el general Medina peleó mucho desde el inicio, pero, por supuesto, es algo que tiene que resolverse dentro de mi propia casa, y no voy a corregir a mis superiores.

Sobre la identidad digital, efectivamente sería muy bueno que tuviéramos una identidad digital que impidiera, por lo menos, el uso malicioso de las identidades falsas; habría que controlar esto. Ya empieza a haber una preocupación por parte de las redes sociales fundamentales —Facebook, Twitter— por desmontar esas identidades falsas, esas redes de *bots* que aprovechan funcionalidades de las propias redes sociales para crear ejércitos de opinión, y se está trabajando en ello.

Y sobre las noticias falsas, ya lo he contestado un poco antes. Hay que entender que este no es un problema de ciberseguridad salvo cuando una noticia falsa se aproveche de una acción que se pueda calificar como ciberataque. A través del ciberespacio se pueden ejercer muchas acciones en esto que se llama amenaza híbrida o guerra híbrida, que tienen muy diferente y muy heterogénea puesta en práctica. Por ejemplo, una intrusión en un sistema, en los correos electrónicos de una campaña electoral puede permitir al atacante obtener información confidencial o información que pueda dañar la reputación o la imagen, y se puede utilizar como herramienta para una negociación, para un chantaje, ese tipo de cosas, es decir, la gama de posibilidades es amplísima.

Por supuesto, se sabe que hay Estados y organizaciones, incluso no necesariamente militares ni gubernamentales sino puramente de *marketing*, que trabajan a través de lo que se llama *puppets,*

cve: DSCG-12-CM-116

marionetas, trols, que intentan modificar la opinión pública mediante un esfuerzo de opinión aparentemente espontáneo y real; pero realmente son eso, marionetas que están gobernadas por un operador que hay detrás que tiene que lanzar determinados mensajes. Tenemos muchos ejemplos en Internet de un mensaje supuestamente lanzado por veinticinco individuos en el mismo instante que decían lo mismo y aparentemente responden a identidades reales, pero realmente no lo son.

Creo que he contestado a todos.

El señor **PRESIDENTE:** Sobradamente.

Voy a abrir el segundo turno, dando la palabra al señor Castellana por si quiere hacer alguna aclaración.

El señor **CASTELLANA GAMISANS:** Muchas gracias, señor presidente.

Muchísimas gracias por la información detallada y reveladora que ha dado. Respecto al tema de la prudencia, creo que ha dicho lo que tenía que decir y que es el mundo de la política el que tiene que responder, utilizando las herramientas de disuasión que también usted ha comentado.

Respecto al *hacker* solitario, creo que estamos hablando el mismo idioma desde el mismo momento en que alguien ha tenido que generar esas herramientas y dejarlas ahí para que otros las utilicen. Hagamos, por ejemplo, el símil con explosivos o armas ligeras, que fuesen tan fáciles de conseguir.

En resumen, de su comparecencia y aportaciones me quedo con que es importantísima la alfabetización en seguridad digital, algo que va más allá de la creación de herramientas y a lo que desde el mundo de la política y de la planificación se debería responder.

En cuanto a las buenas prácticas en el sector corporativo, si desarrollar un medicamento conlleva requisitos, si desarrollar un vehículo conlleva requisitos que encarecen el desarrollo del producto pero garantizan seguridad, también deberíamos ser suficientemente valientes desde el mundo político para obligar al sector corporativo a utilizar estas buenas prácticas, aunque les cueste algo de dinero, porque la seguridad cuesta más y después la pagamos entre todos.

Finalmente, no solamente ciberarmas —aludiendo también a sus palabras—, sino diplomacia y política. Desde el mundo de la política no debemos tener miedo, sino todo lo contrario, por exigir un comportamiento en favor de la paz y de los derechos humanos, y no blanquear a ningún actor político que se salte estas normas aunque sea porque haya contratos comerciales en vigor.

Muchas gracias.

El señor **PRESIDENTE:** Gracias.

Tiene la palabra la señora Angustia.

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

Tomo la palabra solo para agradecer al compareciente, al capitán Cubeiro, no solo su primera explicación, sino lo exhaustivo de las respuestas.

Y me permito una aclaración. Cuando me refería al Real Decreto 12/2018, me hacía eco de una crítica realizada desde el espacio de los operadores jurídicos, ya que, con respecto a cuando dicen militarizado —no eran mis palabras, sino precisamente en referencia a esa crítica de operadores jurídicos—, es cierto que en el artículo 11 del real decreto aparece muy bien establecida esa parte de competencias dependientes del Ministerio de Defensa o de espacios relacionados con el aspecto más militarizado en el campo de la defensa, pero queda muy poco centrada, muy poco especificada o muy poco participada —se quejaban otros— por parte de los operadores jurídicos. Solo trasladábamos esa queja y la petición de opinión sobre su participación respecto de las reformas pertinentes en el Código Penal.

Por lo demás, de verdad, muchas gracias. Creo que no siempre se es tan exhaustivo en las respuestas, usted lo ha sido hoy y, por lo tanto, ha llegado casi más lejos de lo que muchas pretendíamos con nuestras preguntas.

El señor **PRESIDENTE:** Gracias.

El señor Cortés tiene la palabra.

El señor **CORTÉS LASTRA:** Yo también seré muy breve para agradecerle, en primer lugar, la intervención que ha tenido y, en segundo lugar, también las respuestas tan exhaustivas que nos ha dado a cada uno de los miembros de esta Comisión.

cve: DSCG-12-CM-116

Quiero remarcar, si cabe, la necesidad; creo que tendríamos que ir un poco más allá en la cultura de la ciberseguridad. Independientemente de la labor que ustedes puedan realizar, el compromiso del conjunto de la sociedad debe estar en primera línea. Y sí es verdad que cuando hablamos de la alfabetización en ciberseguridad debemos plantearnos nuestra propia alfabetización, incluso la de los diputados en esta casa, y también en otros muchos lugares, en las administraciones públicas, en las empresas, como comentaba también nuestro colega. Es decir, creo que tenemos un verdadero problema y mucho trabajo por delante. Es cierto que hay una base fundamental, que es el inicio desde la educación de los niños, y que también debemos ahondar más, posiblemente incluso debiéramos trabajar en comunicación con la propia Comisión de Educación para dar más énfasis, si cabe, a este asunto. En definitiva, creo que es un reto que tenemos por delante muy importante.

De nuevo le agradezco su intervención. Es verdad que igual podemos permitirnos no avanzar o avanzar en menor medida en otros aspectos, pero donde no podemos permitirnos avanzar a un ritmo lento es en este ámbito. Creo que tenemos un compromiso que debemos respetar todos. Muchas gracias.

El señor **PRESIDENTE:** Gracias.

La señora Vázquez tiene la palabra.

La señora **VÁZQUEZ BLANCO:** Simplemente, quiero agradecer la valiente comparecencia que ha tenido hoy aquí el capitán de navío don Enrique Cubeiro. Nos ha respondido con creces a todas las preguntas que le hemos formulado, que fueron muchas. Nuevamente le agradezco el trabajo que hacen, también en los medios de comunicación, personas entregadas y con vocación para crear un Estado creo que con la misma madurez que en Estonia y Georgia. Ojalá que con personas como usted, que salen en los medios de comunicación, no solo aquí, mucha gente tenga esa conciencia. De verdad, están haciendo un trabajo extraordinario desde el Ministerio de Defensa en esta materia. No solo es un problema civil, es un problema también de defensa, y ver a gente como usted en los medios de comunicación crea conciencia del problema grave al que en estos momentos estamos sujetos.

Muchas gracias.

El señor **PRESIDENTE:** Gracias, señora Vázquez.

Visto el éxito de crítica y público que ha tenido el compareciente, me imagino que su intervención se limitará a agradecer su inteligencia a los diputados que han intervenido.

El señor **CUBEIRO CABELLO** (capitán de navío y jefe del Estado Mayor del Mando Conjunto de Ciberdefensa, MCCD): Muchas gracias a ustedes. Ya he captado la indirecta de que exhaustivo equivale a muy pesado, así que no me voy a extender más. Creo que han hecho ustedes unas muy buenas preguntas, que he tratado de contestar lo mejor que he podido. Gracias.

El señor **PRESIDENTE:** Muchas gracias.

Señorías, se levanta la sesión.

Eran las doce del mediodía.

cve: DSCG-12-CM-116