LA CIBERDEFENSA, UN RETO PARA LAS FF. AA.

Manuel GÁLVEZ REINA

Introducción

DESDE hace una década venimos asistiendo a un importante incremento del desarrollo tecnológico en todos los ámbitos de la sociedad, principalmente de los países avanzados, que ha motivado un cambio en sus hábitos, usos y costumbres. Es por ello por lo que, a esta sociedad se le conoce también como «la de las nuevas tecnologías». El acceso a través de la *web* a servicios básicos y a otros más complejos o críticos, como pudieran ser los bancarios, implica que este tenga que realizarse a través de sistemas informáticos convenientemente protegidos mediante protocolos que no sean fácilmente vulnerables a posibles ataques de terceros, estos últimos conocidos por la gran mayoría como *hackers*. Recientes estudios han demostrado que un país puede ser colapsado mediante ataques cibernéticos a servicios imprescindibles como los de gestión y producción energética, gubernamentales y/o financieros. Esta circunstancia se ha venido produciendo, cada vez con más asiduidad, durante los últimos cinco años, principalmente en los países occidentales de nuestro entorno; y es que una de las dicotomías actuales tiene su base en que dada la facilidad de acceso a Internet, y con ello a la información que en ella circula, cualquier persona con conocimientos avanzados de informática podría ser considerada una amenaza.

Paralelamente, y conforme avanza la tecnología, los escenarios bélicos también evolucionan, adaptándose en este caso a la nueva era digital. Por eso, las amenazas actuales ya no solo se extienden al espacio aéreo, marítimo o terrestre, sino que también lo hacen, y cada vez con mayor auge, a nuevos

escenarios, como el ciberespacio, mediante el uso de la tecnología. Este cambio se ha venido materializando en ataques cibernéticos cada vez más complejos y difíciles de detectar, que obligan a estudiar y profundizar en los nuevos entornos de combate; todo ello con el objetivo de adaptar los medios actuales a la nueva amenaza. El enemigo ya no se circunscribe a una ubicación concreta en un país determinado, sino que mediante el acceso a Internet puede atacar desde miles de kilómetros de distancia. Esta circunstancia ha hecho reflexionar a los gobiernos de diferentes países y por ende a sus Fuerzas Armadas (FF. AA.), que han visto la gran vulnerabilidad existente a nivel tecnológico, que les exige adoptar medidas urgentes para intentar minorar los posibles ataques cibernéticos. España, y en particular nuestras FF. AA., se ha visto obligada a adaptarse de igual forma a esta nueva realidad tecnológica. La reciente creación del Mando Conjunto de Ciberdefensa se intuye como el máximo exponente de esta realidad, pues a través de una estructura dimensionada y apoyada por los Ejércitos y la Armada se da inicio a una ardua tarea con el objetivo de contribuir a proteger las estructuras básicas del Estado, mediante técnicas no solo de defensa, sino de ataque si fuera necesario.

La Armada, no ajena a esta realidad, también ha iniciado su particular contribución con la creación de una Sección de Ciberdefensa, dentro del Grupo de Seguridad en las Tecnologías de la Información y Comunicaciones, más conocido como grupo STIC. Para llevar a cabo esta difícil tarea es preciso contar con personal convenientemente preparado, lo que conlleva la necesidad de adquirir las herramientas que permitan la formación y especialización del personal militar, ya sea a través de centros de formación militar o de las universidades, en cuyo caso será preciso disponer de los convenientes acuerdos.

Conceptos y nuevos factores emergentes

Conviene hacer referencia a algunos de los factores más relevantes que afectan de lleno al mundo de la ciberdefensa. Entre otros, destacar los siguientes: ciberterrorismo organizado, iniciativas internacionales en materia de ciberdefensa, espionaje industrial a instituciones o Estados (conocido como ciberespionaje), ciberataques a sistemas de información de alto interés, ciberataques a sistemas SCADA (1) (especialmente sensibles), necesidad de integración en mandos internacionales de ciberdefensa, necesidad de mando nacional y organización del mismo, adaptación de las FF. AA. en materia de ciberdefensa, necesidad de adiestramiento y carencia de cursos de perfeccio-

(1) Acrónimo de *Supervisory Control And Data Acquisition* (Supervisión, Control y Adquisición de Datos), es un *software* para ordenadores que permite controlar y supervisar procesos industriales a distancia.

namiento sobre seguridad tecnológica. Estos son algunos de los factores más importantes en el entorno de la ciberdefensa, convertidos actualmente muchos de ellos en retos para nuestras FF. AA. Por ello vamos a definir y a situar al lector en estos nuevos conceptos y factores en los cuales la ciberdefensa militar trabaja día a día.

El primero sería el *ciberterrorismo*. Bajo mi punto de vista, esta palabra hoy en día parece más ciencia ficción que realidad, pero los datos revelan que hay que comenzar a considerarla con la amplitud que le corresponde. La definición de ciberterrorismo se basa en el uso de medios de tecnologías de la información, ya sean informáticos de telecomunicaciones o electrónicos, para generar extorsión, miedo o terror a un sector de la población, persona física o incluso a un Estado con la finalidad de obtener beneficio de ello. Este puede ser económico, político, cultural o religioso. La realidad es que las estadísticas hablan por sí solas y nos revelan que los incidentes informáticos críticos se han incrementado en un 150 por 100. Analizando los datos actuales procedentes del centro criptológico nacional, organismo encargado de establecer el nivel nacional de alerta, llegamos a la conclusión de que este factor está tomando una gran importancia; de hecho, el estado de alerta se ha elevado sustancialmente en los últimos tiempos.

Por otro lado, parece que esta actividad delictiva va a tener un crecimiento exponencial en los próximos años, según la evolución de los datos registrados. De hecho, se pueden ver los primeros casos de extorsión real a usuarios mediante técnicas como el *ransomware* (2) con el objetivo de financiar actividades delictivas y mafias en la red. Tampoco hay que olvidar que durante el año 2012 el cibercrimen ocasionó 87.000 millones de euros de pérdidas, cantidad que se considera irá en aumento. Gran parte de ella fue recogida y administrada por ciberterroristas, que consiguen de esta forma incrementar la capacidad de financiación de sus actividades delictivas. Todo ello obliga a los gobiernos a considerar que muchas organizaciones terroristas pueden estar preparando acciones específicas para generar terror entre la sociedad, lo que les obliga a vigilar de cerca a este tipo de organizaciones.

Finalmente, estos grupos organizados tienen muy claras las ventajas de este tipo de actuación frente al terrorismo tradicional, ya que, entre otras, no comporta riesgo físico al terrorista y puede actuar desde cualquier punto del planeta sin limitación geográfica. Esto añade una dificultad adicional para los Cuerpos y Fuerzas de Seguridad del Estado y FF. AA., que no siempre pueden localizar al enemigo en un área o región determinada.

El segundo factor sería el *ciberespionaje*. Nuestras empresas y nuestros Estados no están a salvo de ataques provinientes de otros países, e incluso de

(2) *Ransomware*: virus que bloquea o cifra tu ordenador y solicita el pago de un «rescate» para recuperar los datos.

ataques de origen interno. Se necesitan medios de contención y ciberseguridad para poder hacer frente a estos ataques. Asimismo, se ha de prevenir el uso de información por terceros mediante técnicas de criptografía para la información sensible. El problema resulta fácil de exponer: si la información de especial interés de empresas relevantes a nivel de Defensa, como por ejemplo Indra o Navantia, llegase a manos ajenas, podría ser empleada, incluso en caso de enfrentamiento, por un país enemigo, que conocería previamente todas las debilidades en sistemas de defensa e información. En lo que se refiere al sector civil, existen numerosos indicios de que la industria china utiliza claramente técnicas de ciberespionaje para poder tener acceso a tecnología equivalente, e incluso en muchos casos ha mejorado los proyectos occidentales. También tenemos ejemplos aparecidos en los medios extraídos de las revelaciones de Edward Snowden sobre espionaje y vigilancia realizada por Estados Unidos. El ciberespionaje es una realidad.

En tercer lugar, está el factor de mayor actualidad, los *ciberataques*. Como su propio nombre indica, son ataques realizados sobre un objetivo de manera electrónica, que son en gran medida difícilmente detectables y tienen una importancia tremenda. Actualmente nos encontramos con una media aproximada de unos 3.500 ataques diarios desde diferentes partes del mundo. Es cierto que la mayoría de ellos van dirigidos contra páginas *web* o empresas civiles en general, pero no hay que olvidar que una gran parte tiene que ser repelida por organismos especializados, que actualmente no dan abasto. Este hecho obliga a las empresas y numerosas corporaciones a prepararse para hacer frente a este número considerable de ataques.

Si bien, las empresas civiles no tienen una coordinación tan eficiente como la que puede tener un Estado a nivel de defensa para repeler estos ataques, ya han dado sus primeros pasos en materia de coordinación y asociación para estar altamente protegidas. Existen numerosas compañías que ya colaboran entre sí para aprender de estos ataques y saber protegerse. En concreto, Indra es un referente internacional, al disponer de un centro de mando de ciberseguridad desde el que es capaz de defenderse con garantías en el ciberespacio mediante las últimas tecnologías de análisis y protección en tiempo real. No obstante, los sistemas con más riesgos tangibles son los SCADA, ya que controlan hidroeléctricas, centrales nucleares, iluminación, etc. Con la aparición de Stuxnet (3) estos comienzan a estar en jaque, lo que implica que sus administradores deben estar a la vanguardia de este tipo de guerra para poder hacer frente a la amenza que suponen estos nuevos ataques. Hay que recordar que Stuxnet puede ser considerado como el primer acto real de ciberguerra

(3) Stuxnet es un gusano informático que afecta a equipos con sistema operativo Windows, descubierto en junio de 2010. Este conocido gusano espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos.

entre dos Estados, ya que se demostró que Israel lo utilizó contra sistemas SCADA de centrales nucleares de Irán. Declaraciones recientes, en julio de 2013, de Edward Snowden revelan que Estados Unidos colaboró con Israel en la creación de este *malware* (4).

Las evidencias son una muestra de que ya no nos enfrentamos a guerras convencionales. Las nuevas armas se pueden preparar en una oficina con equipos informáticos y ser desplegadas a miles de kilómetros a una velocidad cercana a la de la luz. Con estos factores juega el concepto básico de una ciberarma.

Actualmente España se encuentra en el *top 10* mundial de los países en los que se producen más ciberataques hacia la banca *online*. Consultando los datos de la empresa S21sec, se corrobora que el *malware* bancario es el principal riesgo de seguridad y de fraude al que se enfrenta el sector financiero, el comercio electrónico, las aseguradoras y los servicios *online*. Durante los primeros seis meses del año 2013, S21sec detectó y analizó más de dos millones de troyanos y clasificó 135.000 muestras de *malware* bancario. Las compañías intentan poner remedio mediante consultoras de seguridad, pero la labor de las Fuerzas y Cuerpos de Seguridad del Estado es fundamental para poder contener estos tipos de ataques y funcionar a la par que las empresas civiles. Queda bastante claro que los ciberataques a nivel nacional, preocupan y bastante.

Evolución de la ciberdefensa en Oriente

Una vez enfocados los factores, analizemos el marco internacional. La primera pregunta sería ¿qué países de gran interés trabajan en ciberdefensa militar? Un ejemplo claro es China. El People's Liberation Army ha desarrollado políticas de ciberguerra muy interesantes, ha implementado entrenamientos para oficiales y ha llevado a cabo ejercicios en esta materia desde los años 90. Los expertos opinan que China está financiando en gran medida a la comunidad *hacker*, tiene acuerdos de cooperación en Rusia y se sospecha también que posee su propio modelo de ciberataque. El entrenamiento chino se realiza en la Academia de Mando y Comunicaciones en Wuhan y en distintas universidades nacionales, y todos estos centros cuentan con profesores expertos en ciberguerra para formar a los nuevos alumnos. La formación abarca desde el conocimiento en informática y redes de computadores hasta la utilización de ciberarmas, lo que aporta al alumno una formación en un amplio espectro del campo de la informática y de las telecomunicaciones. Ello

(4) *Malware* (del inglés, *malicious software*), también llamado *badware,* código maligno, *software* malicioso o *software* malintencionado, es un tipo de *software* que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

permite que nos podamos hacer una idea de lo que el Ejército chino puede controlar en el ciberespacio.

El otro candidato a analizar es Rusia. Los rusos llevan años desarrollando doctrinas y programas de ciberdefensa. El *armamento* informático que poseen, o lo que es lo mismo, armas basadas en código fuente de programación, es prioritario en la política de defensa rusa. Se cree que el Federal Security Service lleva empleando a *hackers* para ciberespionaje desde hace años. En Rusia se ha dado prioridad a la carrera armamentística informática ante el miedo a que sus máximos rivales adopten ventaja en materia cibernética. Actualmente existe la evidencia de que Rusia cuenta con capacidad ofensiva en materia de ciberguerra; acontecimientos como los famosos ciberataques sobre Estonia en 2007, Georgia en 2008 y Kirguistán en 2009 lo dejan bastante claro. Según los analistas internacionales, la carrera armamentística en materia tecnológica seguirá con una evolución clara y concisa en los próximos años.

España y nuestras Fuerzas Armadas

Como bien sabemos, la ciberseguridad es esencial y las organizaciones internacionales tienen que hacer frente a las amenazas existentes. En España se lleva trabajando en este concepto de la ciberdefensa militar unos cuantos años. El Estado Mayor de la Defensa desarrolló en 2011 el concepto de ciberdefensa militar. Este término se define como «el conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control propios, además de la información que manejan». La visión nacional de ciberseguridad se aprobó el 31 de mayo de 2013; esta versión actualiza la de 2011 y da las directrices para la utilización eficiente de los recursos para la preservación de la seguridad nacional.

En el proyecto de Estrategia de Seguridad Nacional de 2013 ya aparecen entre otros los riesgos y amenazas para la seguridad nacional, conocidos como las ciberamenazas, que se relacionan directamente con los conflictos armados, el terrorismo, el crimen organizado, el espionaje, las vulnerabilidades de las infraestructuras críticas y, finalmente, los servicios esenciales de un país.

Asimismo, se expresa abiertamente la explotación y la respuesta sobre los sistemas adversarios para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos.

Además, se fijan como objetivos los siguientes: garantizar el acceso libre al ciberespacio y al funcionamiento de los sistemas CIS militares; establecer un ámbito de operación más seguro; obtener y mantener la superioridad global en el ciberespacio durante las operaciones; garantizar la operación de las redes

y servicios críticos en un ambiente degradado, así como, por otro lado, obtener, analizar y explotar la información de adversarios en el ciberespacio y, finalmente, poder ejercer la respuesta necesaria, legítima y proporcionada a acciones no autorizadas.

La parte más importante, bajo mi punto de vista, son los retos que se fijan: concienciación, formación, adiestramiento, evaluación de la amenaza y gestión de riesgos; rapidez de reacción; control, inteligencia especializada y coordinada; establecimiento de las autorías y recursos dedicados, tanto humanos y materiales como financieros, para poder llevar a cabo esta tarea. También existe una complejidad del marco legal, ya que ante tanta insuficiencia de legislación es difícil ajustarlo a día de hoy. Por otro lado, también se establecen tres capacidades básicas: defensa, explotación y respuesta. Está claro que estas tendrán en cuenta aspectos como el material a utilizar, la infraestructura donde desarrollar las actividades, el equipo humano, el adiestramiento del mismo y respetar y seguir las doctrinas OTAN y UE.

Estas capacidades tienen que permitir responder ante incidentes, supervisar los sitemas de mando y control militares, así como respetar integramente los objetivos que se establecen en la defensa nacional. Tampoco hay que olvidar que será necesario fomentar acuerdos con el sector privado y público para intercambio de información y coordinación de medios y recursos.

Hay que recordar que en España tenemos los siguientes organismos directamente relacionados con el tema que nos ocupa: Instituto Nacional de Tecnologías de la Comunicación (INTECO), Centro Criptológico Nacional (CCN-CNI), Capacidad de Respueta ante Incidentes de Seguridad (CCN-CERT), Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), Grupo de Delitos Telemáticos de la Guardia Civil (GDT-GC), Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional (UID-TIC) y la Agencia Española de Protección de Datos (AEPD).

MCCD y Armada

En el ámbito de nuestras FF. AA., por Orden Ministerial 10/2013, de 19 de febrero se creó el Mando Conjunto de Ciberdefensa (MCCD) de las FF. AA. Este órgano pertenece al Estado Mayor de la Defensa y depende directamente del jefe de Estado Mayor de la Defensa.

La misión del MCCD es el planeamiento y la ejecución de acciones en torno a la ciberdefensa militar, en los sistemas de información y telecomunicaciones de las FF. AA. u otros previamente establecidos, así como la respuesta adecuada en el ciberespacio ante agresiones que afecten a la defensa nacional española.

La Armada tampoco se queda atrás y, como viene siendo habitual, es pionera en estos ámbitos, y también ha adoptado los cometidos establecidos en materia de ciberdefensa por el Estado Mayor de la Defensa. Se ha creado un Grupo de Ciberdefensa, que ha absorbido las funciones del anterior Grupo de Seguridad de las Tecnologías de la Información y Comunicaciones de la Armada y ha potenciado todo el ámbito de la ciberseguridad para acometer la vigilancia, la defensa y la protección de las redes clasificadas que son propiedad de la Armada.

Para poder asumir todos los cometidos del Plan de Acción para la obtención de la Capacidad de Ciberdefensa, en la Armada se hace necesaria la creación y establecimiento de un Equipo de Respuesta ante Emergencias Informáticas CERT-AR (5) con la misión de actuar como centro de respuesta frente a incidentes de seguridad en tecnologías de la información. Recordar que un CERT estudia el estado de seguridad global de redes y ordenadores, y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y además ofrece información que ayuda a mejorar la seguridad de estos sistemas. Sus misiones incluirán las capacidades de monitorización constante de redes y sistemas que manejan información clasificada en el ámbito de Armada, con énfasis en SMN y SACOMAR; inspección y análisis de vulnerabilidades de redes específicas; detección, resistencia y recuperación ante incidentes de seguridad, e integración/coordinación con el CERT-FAS.

Medidas, acciones y compromisos en la ciberdefensa nacional

Actualmente existen carencias en los cursos de perfeccionamiento sobre seguridad tecnológica, tan específica como la necesaria para afrontar la ciberdefensa. El Ministerio de Defensa ya ha firmado un convenio con la Universidad Politécnica de Madrid para poder fomentar las relaciones en materia de formación de los futuros especialistas. En el convenio se recogen los siguientes aspectos: cursos de formación que acrediten la especialización en ciberdefensa, se fija el currículo y contenidos de dicha formación conjuntamente y, además, se realizarán proyectos de investigación en materia de ciberdefensa.

Los sistemas SCADA y otros de gran interés nacional tienen que ser protegidos exahustivamente, ya que actualmente se observan vulnerabilidades que deben ser solventadas y protegidas por organismos y unidades nacionales que tengan esa capacidad. La sostenibilidad del país depende en gran medida de la resistencia a evitar agresiones a los servicios críticos.

---

(5) CERT-AR (*Computer Emergency Response Team-Armada*).

Las FF. AA. todavía están empezando a dar sus primeros pasos en materia de ciberguerra y ciberdefensa; se estima que llevamos un retraso de aproximadamente una década con respecto a la vanguardia. Actualmente, solo se han realizado unas cuantas ediciones de ciberejercicios en las FF. AA., lo que denota una teórica falta de experiencia y preparación de actividades conjuntas. Por otro lado, apenas hay evidencias de adiestramiento y acreditación técnica para el combate. La formación en esta materia por ahora es nula en los centros de formación de oficiales y suboficiales, aunque se empiezan a ver los primeros acuerdos y cursos con las universidades, como enuncié anteriormente.

La concienciación es un factor importante, y todos los miembros de las FF. AA. deben entender la ciberguerra como otra amenaza existente y no olvidarla nunca. La integración con la ciberdefensa de la OTAN se estima necesaria por ahora, aunque empezamos a trabajar en el camino correcto. España tiene claro que la materia de ciberdefensa debe ser desarrollada en un porcentaje bastante alto a nivel interno, y no delegar en organismos internacionales en la medida de lo posible.

De considerar todos los factores, se extrae la conclusión de que la amenaza existe, y que España no ha empezado a desarrollar íntegramente la solución de defensa hasta que no ha tenido una necesidad crítica en materias de seguridad de la información. Una vez establecido el riesgo y la amenaza, se crean los grupos y organismos pertinentes para abordar esta problemática, pero la inexperiencia en estos temas hace que se necesite mucha más formación y perfeccionamiento en nuestras FF. AA.

Conclusiones

Se observa un retraso aproximado de 10 años de media con respecto a las FF. AA. de países de pontencial interés, como pueden ser Rusia, China o Irán. Estos países establecieron las bases del riesgo tecnológico mucho antes que España. La ciberdefensa española, como tal, no ha dado sus primeros pasos con un órgano independiente hasta febrero de 2013, creando el Mando Conjunto de Ciberdefensa de las FF. AA. Hasta ahora solo se han desarrollado unas cuantas ediciones de unas jornadas dedicadas anualmente a la mentalización de las FF. AA., pero su personal sigue sin tener todo el conocimiento y la experiencia que deberían en esta área, aunque se esta trabajando en la buena línea.

La cobertura de la plantilla del MCCD no está al 100 por 100, y además mucho personal necesita mayor formación para poder desempeñar estas tareas. Se precisan medios materiales *(hardware & software)* y humanos adaptados a esta área, por lo que se necesita una inversión financiera bastante importante que no puede demorarse mucho más. Dada la situación económica que azota al país, este será un factor determinante en la velocidad del desarrollo de las

acciones que se necesitan. A nivel de los Ejércitos y la Armada se necesita la implantación de unidades de ciberdefensa, así como la formación de profesionales para poder ejercerla. Actualmente se están dando los primeros pasos, renombrando antiguas unidades o grupos relacionados con la seguridad informática y estableciendo en muchos casos un CERT. Se necesita obtener una acreditación que cumpla con el porcentaje de Combat Ready que se establezca como mínimo desde el Estado Mayor de la Defensa para la plena operatividad de los Ejércitos, de la Armada y del MCCD en materia de ciberdefensa.

Las FF. AA., en la medida de lo posible, tienen que buscar esta referencia en el mundo civil, trabajando poco a poco en esa dirección y realizando cometidos y colaboraciones en la misma línea que lo hacen ya las empresas civiles. El Estado tiene claro que la ciberdefensa es un asunto que hay que afrontar y trabajar en ello.

Después de todos los datos expuestos, tanto a favor como en contra, sobre el estado de la eficiencia y establecimiento de la ciberdefensa en España, se puede concluir que todavía no estamos lo suficientemente preparados para afrontar con soltura una ciberguerra, con todo lo que conlleva. Pero es evidente que se han definido todas las pautas, y se está consiguiendo en mayor o menor medida un avance y una eficiencia razonable de nuestras FF. AA. en ciberdefensa.

El Ministerio de Defensa ha conseguido establecer un camino válido que permite superar de manera eficaz las deficiencias iniciales en esta área. Viendo el progreso de estos últimos tres años, se estima que en un plazo no muy lejando veremos cómo los Ejércitos, la Armada y el MCCD serán totalmente capaces en materia de ciberdefensa. No obstante, a pesar de que la ciberdefensa ha pasado a ser una de las prioridades que contempla la Directiva de Defensa Nacional, el personal militar que tiene asignada esta tarea tendrá muchas dificultades para implementar este concepto dentro de las estructuras de las FF. AA.

Por tanto, resultaría prioritario, bajo mi punto de vista, establecer cursos de aptitud de ciberdefensa para oficiales y suboficiales, o incluso llegar a crear una especialidad que permita dotar y actualizar constantemente al personal militar en esta área. Para ello, una solución son los actuales convenios de especialización con las universidades españolas y los nuevos proyectos de ciberdefensa que están consiguiendo dar los primeros pasos para afrontar esta nueva amenaza con todas las garantías posibles, tal y como España demanda y espera de su defensa. Siguiendo estas pautas de trabajo, próximamente la capacidad total de ciberdefensa será una realidad tangible con garantías para las FF. AA. españolas, y asistiremos una vez más al compromiso de profesionalidad y eficacia que siempre ha caracterizado a nuestras FF. AA.

BIBLIOGRAFÍA

Estado Mayor de la Armada: *Concepto de ciberdefensa en la Armada,* mayo 2013.
Estado Mayor de la Defensa: *Concepto de ciberdefensa militar*, julio 2011.
—*Visión del JEMAD de la ciberdefensa militar*, enero 2011.
Presidencia del Gobierno: *Directiva de defensa nacional 2012*, julio 2012.
Centro Criptológico Nacional: *Informe de Actividades*, diciembre 2012.
Monografías del CESEDEN: *El ciberespacio nuevo escenario de confrontación*, marzo 2012.
ALBERT FERRERO, Julio: «La ciberseguridad en España». *Revista Tierra, Mar y Aire*.
Indra: *Los retos tecnológicos e industriales de la ciberseguridad*, julio 2013.
ZEA PASQUÍN, Francisco: *Ciberseguridad y Empleo Militar del Ciberespacio*, noviembre 2013.
—*Mando conjunto de ciberdefensa: Prioridades en el desarrollo de las capacidades de la ciberdefensa militar*, abril 2013.
Instituto Nacional de Estudios Estratégicos: *La Directiva de Defensa Nacional 2012*, agosto 2012.
—*Nuevo concepto de ciberdefensa de la OTAN*, marzo 2011.
—*Ciberdefensa, equipos de respuesta inmediata de la OTAN*, marzo 2012.
—*La nueva política de ciberdefensa de la OTAN*, octubre 2011.
—*Administración Electrónica, CIS, TIC, TI y otras etiquetas de modernidad en el ámbito del Ministerio de Defensa*, agosto 2013.
—*Delincuencia organizada e Internet*, noviembre 2013.
—*Zona de Conflicto Asimétrico*, noviembre 2011.
—*Siete lecciones no aprendidas sobre Anonymous*, diciembre 2013.
—*Estrategia de ciberseguridad nacional*, diciembre 2013.