CAPÍTULO QUINTO

LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR

LA CIBERSEGURIDAD EN EL ÁMBITO MILITAR

JUAN JOSÉ DÍAZ DEL RÍO DURÁN

RESUMEN

Este capítulo estudia la ciberseguridad en el ámbito militar. Para ello, se comienza dando un enfoque general de estrategia, referido a los nuevos retos y amenazas del comienzo del siglo XXI, para pasar a continuación a analizar los riesgos en el ciberespacio y el estado del arte de la defensa, explotación y ataque en esta nueva dimensión, considerada un nuevo «global common». Se repasa asimismo, la necesidad de introducir nuevas perspectivas en el concepto estratégico de la OTAN ante el papel cada vez más relevante de esta dimensión y se describen las actuaciones y medidas tomadas, tanto por otros países de nuestro entorno como por nuestro Ministerio de Defensa para afrontar este desafío y la estructura y organización adoptada. Se finaliza examinando el importante esfuerzo de colaboración internacional en este campo del Ministerio de Defensa, así como las numerosas actividades de formación, concienciación y adiestramiento desarrolladas en el ámbito del EMAD, concluyendo con un análisis de la cifra y su industria en España.

Palabras clave: Estrategia, amenazas, riesgos, políticas, seguridad, información, ciberespacio, redes, internet, comunicaciones, tecnología, ciberseguridad, ciberdelincuencia, ciberataque, ciberdefensa, ciberterrorismo, ciberguerra, Rusia, China, vulnerabilidad, inteligencia, dimensión, global, NEC, CNO, OTAN, enemigo, Ministerio de Defensa, normativa, organización, mando, control, infraestructura, cooperación, adiestramiento, formación, concienciación, cifra.

CYBER-SECURITY IN THE MILITARY FIELD

ABSTRACT

This chapter examines the cyber-security in the military field. To this end, it starts giving a general approach of strategy, referred to the new challenges and threats at the beginning of this century, analyzing then the risks in cyberspace and the state of the art of the defense, exploitation and attack in this new dimension, considered a new «global common». It looks in addition, the need to introduce new prospects in the strategic concept of NATO facing the role increasingly relevant to this dimension and describes the actions and measures taken, both by other countries in our environment and our Ministry of Defense to cope with this challenge and the structure and organization adopted to do it. It finishes taking consideration on the important international collaborative effort in this area of the Ministry of Defense, as well as the numerous training activities, awareness and training efforts developed in the field by the Defense Staff, concluding with an analysis of the encryption methods and technologies and its industry in Spain.

Key words: Strategy, threats, risks, policies, security, information, cyberspace, networks, Internet, communications, technology, cyber-security, cyber crime, cyberattack, cyberdefence, cyberterrorism, ciberwarfare, enemy, Russia, China, vulnerability, intelligence, dimension, global, NEC, CNO, NATO, Ministry of Defense, regulations, organization, command, control, infrastructure, cooperation, training, education, awareness, encryption.

INTRODUCCIÓN

Miércoles 2 de mayo de 2007; Redmond (Estado de Washington, Estados Unidos); Sede de Microsoft; reunión organizada por la NATO Office of Security y el Departamento de Defensa de EEUU con la colaboración del gigante de la informática; es la séptima edición del «NATO Cyber Defense Workshop». Están presentes la mayor parte de los representantes de las naciones OTAN en asuntos de seguridad en el ciberespacio. Todo transcurre según lo previsto. Es el momento de que el representante del Centro de Excelencia de Ciberdefensa de la OTAN en Tallin (Estonia), el Profesor Peeter Lorents, presente los progresos en la constitución del Centro.

La información con la que comienza su intervención nos deja perplejos y se abre un gran debate. Acaba de decirnos que su país está siendo objeto de ataques cibernéticos desde el día 27 de abril, al principio sencillos, mal coordinados y fácilmente mitigables, pero que desde el día 30 eran más sofisticados y mejor coordinados y se centraron en ciertos routers y DNS (Domain Name Servers) causando interrupciones temporales del servicio al mayor proveedor de comunicaciones fijas de Estonia.

Una novela de ficción podría empezar así, pero desafortunadamente los hechos que se describen arriba son reales y ocurrieron tal y como se ha descrito. Sin embargo y a pesar de que posiblemente esa línea atraería con mayor fuerza la atención del lector, creo que este capítulo debe redactarse de una forma convencional y estructurada. Para ello intentaré hacer en primer lugar un enfoque estratégico general, pasando a continuación a particularizar en la ciberseguridad.

Escenario estratégico general

El escenario estratégico del comienzo de este siglo XXI, se caracteriza porque, junto a los tradicionales riesgos y amenazas para la paz, el equilibrio, la estabilidad y la seguridad internacionales, han emergido otros de nuevo cuño, como el del terrorismo de carácter transnacional y alcance global, con gran capacidad de ocasionar daño indiscriminadamente, así como las diferentes modalidades de ataques que se pueden producir a través del ciberespacio.

Los atentados de Nueva York, Madrid o Beslán, en cuanto al terrorismo y los ciberataques sobre Estonia, Georgia y un largo etcétera de países, en cuanto al ciberespacio, han evidenciado que, frente a los nuevos riesgos y amenazas, la superioridad militar tradicional no constituye un factor de disuasión eficaz ni garantiza más seguridad automáticamente. Tampoco asegura una prevención efectiva contra ataques terroristas o ciberataques, ni evita el riesgo de proliferación de armas de destrucción masiva, cuya posibilidad de caer en manos de tales grupos es hoy la amenaza más grave para la seguridad global.

La lucha contra estas nuevas amenazas es clave en la estrategia de las organizaciones internacionales de seguridad y defensa. También Europa debe afrontarlas decididamente si no quiere convertirse en un objetivo fácil.

Por vez primera en la historia, la Unión Europea se ha dotado de una estrategia de seguridad propia. Pero ésta reclama una mayor determinación, recursos suficientes y un uso más eficaz y coherente de cuantos instrumentos dispone para la gestión de crisis y la prevención de conflictos; unos requerimientos realmente exigentes a los que ningún país europeo, e incluso EEUU como gran potencia, es capaz de hacer frente en solitario.

A su vez, la Alianza Atlántica, que fue la primera en percibir la necesidad de acomodar las respuestas tradicionales al nuevo escenario estratégico, está inmersa en un proceso de transformación profunda de sus estructuras, procedimientos y capacidades, con el fin de conseguir unas fuerzas aliadas mejor dotadas, interoperables y capaces de actuar con la máxima eficacia.

Nos encontramos, pues, dentro de un nuevo escenario estratégico en el que la política de seguridad demanda planteamientos novedosos y cambios de mentalidad, de un modo especial en lo que se refiere a la gestión de crisis y resolución de conflictos y a la necesidad de adaptación de las Fuerzas Armadas a las circunstancias de cada momento.

El ciberespacio y la ciberseguridad

La alta dependencia tecnológica de nuestra sociedad es una realidad constatable, siendo imprescindible para el buen funcionamiento de los Estados, sus Fuerzas y Cuerpos de Seguridad y sus infraestructuras. Esta dependencia seguirá aumentando en el futuro. Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera. Todas estas funciones dependen de sus redes de comunicaciones e informáticas, que en el caso de EEUU, por ejemplo, consisten en más de 15.000 redes(1) y siete millones de terminales informáticos distribuidos en cientos de instalaciones en docenas de países, para cuyo funcionamiento mantienen más de 90.000 especialistas. En menos de una generación, las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico.

(1) www.afcea.org/signal/signalscape/index.php/2010/08/cyberdefense-issues-dod-culture/;
www.reuters.com/article/idUSTRE69C5ED20101013

Paralelamente, la dependencia tecnológica, la globalización y la facilidad de acceso a las tecnologías hace que a día de hoy la probabilidad de sufrir ataques informáticos o ciberataques sea muy elevada, permitiendo potencialmente a nuestros adversarios obtener inteligencia valiosa de nuestras capacidades y operaciones y desestabilizar nuestra economía. Como es lógico, a mayor dependencia, mayor es el impacto que podría tener un ataque a los sistemas sobre los que se sostiene un país o una organización.

Los usuarios de Internet se han acostumbrado a pensar que la información de cualquier lugar o suceso de actualidad en el mundo está disponible prácticamente de inmediato, ven el mundo como un gigantesco PC en el que ellos, mediante su «ratón», intervienen de forma interactiva a través del ciberespacio en todas sus actividades (viajes, trabajo, banca, compras, etc). A este respecto, es conocido el pasaje de un relato de Clay Shirky (2), en que un padre le pregunta a su hija mientras están viendo una película en la TV, por qué está buscando algo en la parte trasera de ésta y ella le contesta que «el ratón, porque quiero cambiar el final de la película».

Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar, aire y espacio, a través del ciberespacio. Citemos a continuación algunos datos que nos pueden dar una dimensión del problema:

- Si en diciembre de 1.995 el número de usuarios de Internet era de 16 millones, en 2.001 pasó a ser de 458 millones y en enero de 2010 alcanzó la cifra de 1.700 millones (3). Se espera que en 2.015, el número de terminales con acceso a Internet supere el número de habitantes de nuestro planeta (4).
- Durante 2008, Symantec creó 1,6 millones de nuevas firmas de amenaza, o lo que es lo mismo, una nueva firma cada 20 segundos (5).

---

(2) Clay Shirky (nacido en 1964) es un escritor americano, consultor y profesor sobre los efectos sociales y económicos de las tecnologías de Internet. Enseña Nuevos Medios de Comunicación en la Universidad de Nueva York (NYU).

(3) www.internetworldstats.com/stats.htm

(4) W.D. Sincoskie, Telecordia Technologies.

(5) Enlace: www.symantec.com/business/resources/articles/article.jsp?aid=20090511_symc_malicious_code_activity_spiked_in_2008.

- La Base de Datos Nacional de Vulnerabilidades de EEUU (The National Vulnerability Database, NVD) (6), integra todas las vulnerabilidades disponibles públicamente y contiene aproximadamente 43.800 de ellas a fecha de finales del mes de septiembre de 2.010, así como las alertas del US_CERT (Computer Emergency Response Team), catalogando aproximadamente 13 al día.

La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias.

Sun Tzu (600 años a.C.) decía en su obra «El arte de la guerra»: «Cien victorias en cien batallas no es lo ideal. Lo ideal es someter al enemigo sin luchar». Este pensamiento ha ganado valor con el paso del tiempo, especialmente con el nacimiento del ciberespacio y la ciberguerra. Puede ser la primera ocasión en que su pensamiento podría imaginarse realizado en toda su extensión gracias a la existencia del ciberespacio. El ciberespacio es una nueva dimensión en la que se pueden materializar conflictos y guerras, que no tiene límites ni fronteras y que, sorpresivamente, parece no tener restricciones ni leyes, al menos efectivas. Por otra parte, Clausewitz pensaba que «La Guerra es un acto de fuerza para doblegar la voluntad del enemigo». Podría deducirse que la ciberguerra aúna los dos pensamientos de estos grandes estrategas, ya que produciendo una parálisis estratégica, se puede doblegar la voluntad del enemigo sin aplicación de la fuerza física.(7)

Ejemplo reciente del lugar preeminente que está ocupando el ciberespacio y su seguridad en nuestro mundo han sido las consecuencias de los ciberataques sufridos por Estonia en el año 2007, del que se hablará con posterioridad. En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes. Este fue el caso de los ciberataques sufridos por Georgia

(6) http://nvd.nist.gov/

(7) «Cyber Wars: A Paradigm Shift from Means to Ends». Autor: Amit Sharma, del Institute for System Studies and Analysis» del Ministerio de Defensa de la India.

durante el conflicto con Rusia en Ossetia del Sur y Abkhazia. Por primera vez en la historia una operación militar fue acompañada de una serie de ciberataques a los sitios Web del gobierno Georgiano y otras páginas comerciales, dejándolos fuera de servicio en algunos casos y modificando el aspecto de las páginas en otros («Defacement»(8)). Expertos de Estados Unidos han concluido que países como China, Rusia o Corea del Norte disponen de unidades especializadas y personal capacitados para llevar a cabo ciberataques y prevén que en los próximos diez años se sufrirán graves consecuencias derivadas de sus acciones, dado que en la actualidad la mayor parte de los sistemas disponen de una protección insuficiente, de procedimientos inadecuados y de un adiestramiento deficiente en seguridad. En este sentido, también se ha pronunciado en febrero de 2010 el antiguo Director de Inteligencia Nacional de EEUU, Mike McConnell (9); afirmó ante el Comité de Ciencia, Transporte y Comercio del Senado, que «el país no se está tomando con seriedad la ciberseguridad y caerá víctima de un ciberataque demoledor en los próximos años. Si la nación entrara en una ciberguerra, perderíamos… no mitigaremos este riesgo. Hablaremos de ello, agitaremos los brazos, tendremos una ley, pero no vamos a mitigar este riesgo». McConnell dijo también declararse fuerte partidario de que el gobierno asuma un papel principal en la ciberseguridad, ya que un ciberataque importante podría paralizar el comercio y hacer temblar la confianza de los consumidores en los mercados financieros y el gobierno federal, «compitiendo con los daños de un ataque nuclear al país».

Las posibles consecuencias de este tipo de ataques pone de relevancia la necesidad de dotarse de una capacidad de seguridad en el ciberespacio, que garantice una adecuada protección frente a éstos y que a su vez permita conocer y bloquear los sistemas del adversario en caso necesario. En países aliados y de nuestro entorno ya se han iniciado los trabajos para obtener esta capacidad. La situación podría agravarse con la actual crisis económica, ya que ésta está originando una restricción en

(8) ***Defacement*** es un término usado en *informática* para hacer referencia a la deformación o cambio producido de manera intencionada en una *página web* por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún *bug* en el propio *servidor* o por una mala administración de éste. Ataques de defacement conocidos se han hecho sobre los portales de Twitter por el «ciberejército iraní», en el de nuestra última presidencia de la UE y en los de los gobiernos de Georgia y Venezuela, este último «colgando» un recordatorio de la «*boda*» entre los señores Castro y Chávez.

(9) www.federaltimes.com/article/20100224/IT01/2240307/-1/RSS

inversiones de seguridad tanto en empresas como en las administraciones públicas y las FAS.

En Estados Unidos la seguridad en el ciberespacio está al mismo nivel que el «Homeland Security», habiendo nombrado el actual gobierno de Obama, un coordinador de ciberseguridad en la Casa Blanca, que será responsable de supervisar una estrategia nacional para garantizar los intereses de los americanos en el ciberespacio. En el ámbito militar americano, ya desde hace unos años, se han llevado a cabo trabajos para la obtención de una capacidad de Operaciones en el Ciberespacio en cada uno de los ejércitos. Posteriormente, explicaré los objetivos de estas Operaciones.

En Alemania, se ha formado la «Unidad de Reconocimiento Estratégico del Bundeswehr», compuesta por un numeroso grupo (10), en su mayoría expertos en seguridad y en el Reino Unido se ha creado una Oficina de Ciber Seguridad (OCS, Office of Cyber Security) encargada de coordinar las capacidades defensivas y de respuesta a intrusiones en redes del Reino Unido (11). El ex-Primer Ministro Gordon Brown, declaró que «de la misma forma que en el siglo diecinueve tuvieron que asegurar los mares por su seguridad nacional y prosperidad y en el veinte fue el espacio aéreo, en este siglo toca hacerlo con el ciberespacio para que los negocios y las personas puedan operar de modo seguro en él».

Hace un año, el Presidente Obama declaraba; «Dado el enorme daño que puede causar incluso un único ataque cibernético, no bastará con respuestas a medida. No es suficiente el reforzar nuestras defensas tras los incidentes o ataques. De igual forma a cómo hacemos frente a los desastres naturales, hemos de tener planes y recursos de antemano, compartiendo información, emitiendo avisos y asegurando una respuesta coordinada». (Presidente Barack Obama, 29 mayo 2009).

A nivel nacional, el Ministerio de Defensa ha publicado la Política de Seguridad de la Información, sus normas de aplicación y ha tomado numerosas iniciativas para incrementar la seguridad de su información, tanto en el ámbito de la red de Propósito General (de orientación administrativa) como en el de Mando y Control (dependiente del JEMAD y orientado a las operaciones). Como es lógico, también la Directiva de

(10) www.spiegel.de/international/germany/0,1518,606987,00.html

(11) www.securecomputing.net.au/News/148634,uk-government-to-create-office-of-cyber-security.aspx.

Planeamiento Militar estudia las capacidades relacionadas con el ciberespacio con las que las Fuerzas Armadas deben contar y el Concepto de Estrategia Militar, describe el nuevo escenario estratégico, en el que la ciberseguridad es tenida en cuenta y se analizan las tendencias y previsiones en este campo.

El JEMAD también ha expresado públicamente la importancia del desarrollo de capacidades relacionadas con las nuevas tecnologías, resaltando la necesidad de desarrollar medidas para mejorar la seguridad de los aliados ante la posibilidad de un ciberataque y definiendo esta amenaza como una de las más complejas a la que cualquier sistema defensivo puede enfrentarse, tanto por sus potenciales efectos sobre la sociedad como por su dificultad de identificar al agresor (12).

La ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares. Unos cuantos programadores pueden, si encuentran una vulnerabilidad a explotar, amenazar nuestros sistemas logísticos, robar nuestro planeamiento operacional o cegar nuestros sistemas de inteligencia y de mando y control. Por este motivo, muchos ejércitos están desarrollando capacidades ofensivas en el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades (13). Para tratar de impedirlo y estar por delante de nuestros adversarios, necesitamos ajustar y mejorar continuamente nuestras defensas. Por otra parte, el análisis forense necesario para identificar a un atacante puede llevar meses, si es que la identificación es posible finalmente, e incluso, si el atacante es identificado y no es un estado sino por ejemplo, un grupo terrorista, puede suceder que no tengamos medios para responder. Para más complicación, los ciberataques a menudo se originan en servidores situados en países neutrales y las respuestas pueden conllevar consecuencias imprevistas a sus intereses, razón por el que el uso de este tipo de reacciones debe estar siempre bajo un mando estratégico que tenga una visión integral y global de la situación.

Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados; tanto su software como su hardware pue-

(12) www.uimp.es/blogs/prensa/2009/07/17/el-jemad-afirma-que-no-hay-alternativas-claras-a-la-otan-porque-hoy-por-hoy-es-una-alianza-insustituible/
(13) www.reuters.com/article/idUSTRE69C5ED20101013

den ser saboteados antes de ser unidos en un sistema en explotación. El código dañino, incluyendo las «bombas lógicas (14)», puede insertarse en el software cuando se está desarrollando. En cuanto al hardware, tanto las «puertas traseras», como los «kill switches (15)», se pueden «grabar» en el «firmware» de los «chips» de los ordenadores, permitiendo su manipulación remota: el riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar. Este tipo de amenaza ya se ha materializado en hardware adquirido por el DoD de EEUU y con seguridad en el de muchos otros países que no han sido capaces de detectarlo.

Ejércitos de diversos países han reconocido formalmente al ciberespacio como un nuevo dominio de enfrentamiento («Global Commons (16)»). Aunque el ciberespacio es un dominio hecho por el hombre, se ha hecho tan crítico para las operaciones militares como la tierra, el mar, el aire y el espacio.

Tanto la OTAN, como la UE están llevando a cabo acciones para dotarse de una capacidad que les permita defenderse y reaccionar adecuadamente frente a estas amenazas. En la Declaración de la Cumbre de Riga (29 de noviembre de 2006), los Jefes de Estado y de Gobierno de la OTAN demandaron la mejora de la protección de los sistemas de información claves respecto de posibles ciberataques. En la Declaración de la Cumbre de Estrasburgo (4 de abril de 2009), afirmaron la vigencia

(14) Es una parte de código insertada intencionadamente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre-programadas, en cuyo momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos, «trigger», que se dispare al cambiar la condición de trabajador activo del programador).

(15) Es una medida de seguridad utilizada para apagar un dispositivo en una situación de emergencia en la que no se puede hacer de la forma habitual. Al contrario que en un apagado normal, que cierra todos los sistemas de forma ordenada y sin dañar la máquina, un «kill switch» está diseñado para abortar completamente la operación a cualquier coste.

(16) Se conocen como «Global Commons», aquellos entornos en los que ninguna persona o estado puede tener su propiedad o control y que son básicos para la vida. Un «Global Common» contiene un potencial infinito en lo referente al conocimiento y avance de la biología y la sociedad. Incluye los mares, el aire, el espacio y el ciberespacio. www.twq.com/10july/docs/10jul_Denmark.pdf («Managing the global Commons», por Abraham M. Denmark).

de su compromiso en el fortalecimiento de los sistemas de información y comunicaciones de importancia crítica para la Alianza frente a ciberataques, que tanto agentes estatales o no, pueden tratar de explotar, pues cada vez es mayor la dependencia de estos sistemas. A modo de ejemplo, la OTAN, aparte de adquirir la correspondiente capacidad, NCIRC (NATO Computer Incident Response Capability), para cuyos objetivos se basa principalmente en su Centro Técnico y definir el Concepto y Política de Ciberdefensa, ha creado la Autoridad de Gestión de la Ciberdefensa (CDMA, Cyber Defense Management Authority) y su correspondiente estructura y organización de apoyo; La ciberseguridad es uno de los desafíos más importantes a la seguridad, siendo un asunto estratégico del mismo nivel que las Armas de Destrucción Masiva y la Yihad Global(17). Por otra parte, la UE ha elaborado el Concepto de Operaciones en Red (CNO; Computer Network Operations) y la EDA (European Defence Agency) ha publicado el correspondiente contrato para su implementación(18). EE.UU ha creado un Mando para el Ciberespacio (Cyber Command).

Las operaciones cibernéticas en redes (CNO; Computer Network Operations)

El término «CNO» tiene una amplia acepción, tanto en el campo civil como militar. En su sentido militar, se podría definir como las acciones tomadas de forma deliberada para obtener la superioridad en la información y denegarle ésta al enemigo. La superioridad en la información es un elemento clave en el concepto NEC (Network Enabled Capability), que trataremos en el siguiente apartado. Dentro del dominio militar, se considera una de las cinco capacidades principales de las Operaciones de Información (IO), junto con las conocidas en el mundo anglosajón como: Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC) y Electronic Warfare (EW).

Las CNOs, en combinación con las de Guerra Electrónica (EW), se utilizan principalmente para interrumpir, perturbar, inutilizar, degradar o engañar los sistemas de mando y control del enemigo, anulando su capacidad para tomar decisiones con eficacia y oportunidad, preservando

(17) www.betanews.com/article/Mr-Obama-Dont-forget-the-cyberwar-threat/1228782845

(18) B-Brussels: 'computer network operations for EU-led military operations (EU milops CNO capability)' — 10-CAP-OP-37 2010/S 157-242011 Contract notice. www.eda.europa.eu/genericitem.aspx?area=Reference&id=665)

a la vez los sistemas de mando y control propios y amigos. Las CNOs, de acuerdo con la publicación Joint Doctrine for Information Operations de EEUU (19), se subdividen a la vez en tres:

- Computer Network Defence (CND), que incluye las acciones tomadas para proteger, monitorizar, analizar, detectar, reaccionar y recuperarse frente a los ataques, intrusiones, perturbaciones u otras acciones no autorizadas que podrían comprometer la información y los sistemas que la manejan.
- Computer Network Exploitation (CNE), que incluye las acciones e inteligencia de recolección de información sobre sistemas de información enemigos, así como su explotación.
- Computer Network Attack (CNA): que incluye las acciones tomadas para perturbar, denegar, degradar o destruir información que circula por los sistemas enemigos.

NNEC (NATO Network Enabled Capability)

La era de la información está alterando la distribución de poder, aumentando la complejidad de los sistemas CIS, restando importancia a las distancias geográficas y reduciendo drásticamente los tiempos de reacción.

Estos cambios, así como las recientes operaciones en curso, están llevando a todos los Aliados a transformar las Capacidades de sus FAS (Fuerzas Armadas), donde una red de redes dentro del concepto NEC (Network Enabled Capability), que definiremos en breve, jugará un factor decisivo en las operaciones y se potenciará como motor y guía de nuestro esfuerzo, alcanzándose la Superioridad en la Información.

Para que el Mando pueda decidir y la decisión a tomar sea la correcta y adecuada para la conducción de las operaciones, esa información habrá de ser precisa, fiable, pertinente y oportuna. En una primera aproximación y de forma general (sin particularizar en el caso OTAN), se podría decir que NEC es «la capacidad de integrar todos los componentes del medio operativo (sensores, elementos de decisión y plataformas de armas) desde el nivel político-estratégico hasta el nivel táctico, a través de una infraestructura de información y redes».

(19) www.c4i.org/jp3_13.pdf, http://www.au.af.mil/info-ops/netops.htm, www.iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm

Formalmente, se conoce como NNEC «la capacidad cognitiva y técnica de la Alianza para federar los diferentes componentes del entorno operativo, desde el nivel estratégico hasta el táctico, mediante una infraestructura de redes y sistemas de información». Trataremos de ver lo que este concepto significa desde la óptica de la seguridad de la información, que es uno de los mayores retos a los que nos enfrentaremos en la convergencia hacia esta nueva capacidad de operación en red.

Los principios(20) de NNEC son los siguientes: una Fuerza robustamente conectada mejora el conocimiento compartido de la información. Compartir la información mejora la calidad de ésta y la percepción de la situación. La percepción compartida de la situación permite la colaboración y sincronización y mejora la velocidad de decisión del Mando, lo que a su vez, incrementará enormemente la eficiencia de las misiones por la agilidad y velocidad de la acción. NNEC busca la mejora de la eficiencia de la toma de decisiones, mediante la integración de las personas y la información en una red.

La gestión de la información en NNEC será una responsabilidad fundamental, que requiere liderazgo, involucración de máximo nivel y la creación y mantenimiento de una estructura organizativa eficaz. La información se gestionará haciendo hincapié en la «responsabilidad de compartir» («responsibility-to-share») convenientemente equilibrada con el principio de seguridad de la «necesidad de conocer» («need-to-know»). La información se protegerá de acuerdo con los principios de «Seguridad de la Información» («Information Assurance»), es decir, de su confidencialidad, integridad, disponibilidad, autenticidad y no repudio.

Todo usuario tendrá un perfil de derechos de acceso a la información, dondequiera que se conecte a la federación de redes. Aunque habrá ocasiones en que las naciones no querrán compartir ciertas informaciones, esto será la excepción, no la regla.

La convergencia a NEC exigirá una prácticamente total interconexión con otros sistemas (Federación de Redes), incluso con ONGs. Este puede ser el caso de la AMN (Afghanistan Mission Network) (21), que constituye una federación de redes entre la red clasificada de ISAF (Internatio-

---

(20) www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf, *nnec.act.nato.int/, www.afcea.org/.../060525-AFCEA2006DraftV1.2.pptMajGenvanDam_000.ppt* y *www.bdcol.ee/.../7_%20Arturas%20Litvaitis-Challenges%20of%20Implementing%20NCW%20Tenets%20in%20Coaliti...*

(21) www.isaf.nato.int/

nal Security Assistant Force) y las extensiones nacionales de las redes de los países de la Coalición(22), con todas las medidas de seguridad que esto conlleva a fin de minimizar los riesgos. Como podemos fácilmente deducir de todo lo anteriormente citado, el esfuerzo (sobre todo en el aspecto de seguridad) para poder alcanzar todos los objetivos citados será muy considerable y requerirá no solamente importantes recursos técnicos, humanos y económicos, sino también un cambio de mentalidad imprescindible. Los principales retos serán:

- Todos los usuarios precisarán recibir la formación y adiestramiento adecuados para utilizar adecuadamente la cada vez mayor información disponible. Necesitarán emplear todas las herramientas disponibles del sistema para extraer la información y necesitarán tiempo para adaptarse a un tipo de cultura más abierta, que requiere compartir la información en mucho mayor grado y establecer la confianza entre los colegas y socios de las coaliciones que se determinen.
- Los desafíos técnicos y procedimentales no deben tampoco ser subestimados. La capacidad de desarrollo será a menudo compleja y requerirá la integración de sistemas legados y sistemas nuevos, a la vez que será necesario asegurar las actualizaciones futuras a todo el sistema en su conjunto. Todo esto conllevará unos procesos de adquisición más flexibles y la búsqueda de socios adecuados en la industria.
- Mientras que la mayoría de nuestros aliados pondrán su capacidad militar en NEC, habrá algunos socios de coalición y organizaciones que no estarán en sintonía, lo que requerirá una consideración profunda de este problema para poder trabajar con ellos.
- Todos estos desafíos vendrán acompañados por la necesidad de evitar una sobrecarga de información y garantizar la robustez de la red. La cada día más creciente amenaza de los ataques cibernéticos, a la que seremos más vulnerables a medida que crezca nuestra dependencia de la red, hará que debamos paliarla mediante nuevas medidas de seguridad. Habrá que tener previsto el poder continuar las actividades en modo degradado y evitar el colapso de la red, contando con medios alternativos de comunicación para mantener activos los elementos clave de la red de redes.
- Por último y no por ser lo último tendrá menos importancia, las restricciones presupuestarias obligarán a una cuidadosa priorización en las decisiones de inversión.

(22) www.defensesystems.com/articles/2010/09/02/c4isr-2-afghan-mission-network-connects-allies.aspx

Revisión del concepto estratégico de la OTAN. Ciberespacio y el artículo V

El actual Concepto Estratégico de la OTAN data de 1.999. La Alianza opera en un ambiente de cambio continuo, con desafíos globales, que obligan a su revisión. Se espera que antes de que finalice el año 2010 se establezca el nuevo Concepto (23). Los adversarios pueden intentar explotar la creciente dependencia de la Alianza de los sistemas de información mediante operaciones de información diseñadas para interrumpir, modificar, o interceptar la información manejada en ellos, en una estrategia para contrarrestar la tradicional superioridad de armamento de la OTAN.

Mientras que el Concepto de 1.999 entiende la defensa colectiva bajo el artículo V como la detención del avance del agresor asegurando la independencia política e integridad territorial de sus estados miembros, el nuevo Concepto debería reconocer la necesidad de modificación de la definición de «ataque armado». Parece necesario que la OTAN entienda que un ataque armado puede incluir un acto agresivo en su territorio o fuera de él, tanto en el entorno real como el virtual, si afecta a los intereses vitales de la Alianza.

Al ser la tecnología cada vez más accesible y de menor coste, los adversarios podrían atacar a los miembros de la Alianza, sus centros de comercio y la economía global, incluyendo las redes sociales mediante el necesario pero vulnerable «global common» que las sociedades modernas utilizan para conectarse y prosperar: el ciberespacio. La OTAN debería desarrollar estrategias, políticas y capacidades que le permitan defenderse y responder a las amenazas emergentes en estas áreas.

La Amenaza

En un principio, la mayoría de los llamados hackers no tenían otro tipo de motivos más que los intelectuales para la penetración en las redes. Buscaban popularidad y notoriedad por haberse saltado las medidas defensivas de sistemas importantes. No obstante, hubo un cambio radical cuando surgió la ciberdelincuencia, ya que las motivaciones pasaron a tener como objetivo principal el beneficio económico de forma ilegal; hoy en día se ha desarrollado de forma alarmante. El robo de identidad,

(23) www.nato.int/strategic-concept/what-is-strategic-concept.html

el fraude financiero (en particular la banca online y tarjetas de crédito/débito), el robo de información y ataques diversos para la extorsión son diferentes formas de ciberdelincuencia que se han convertido en un problema muy importante en todo el mundo.

El ciberterrorismo es otra de las amenazas que han cobrado fuerza durante los últimos años, gracias a su evolución y aumento de actividad. Se considera que la capacidad técnica se ha incrementado considerablemente y que la posibilidad de que se puedan lanzar ataques que logren dañar seriamente elementos de las infraestructuras críticas nacionales se ha de tener en cuenta.

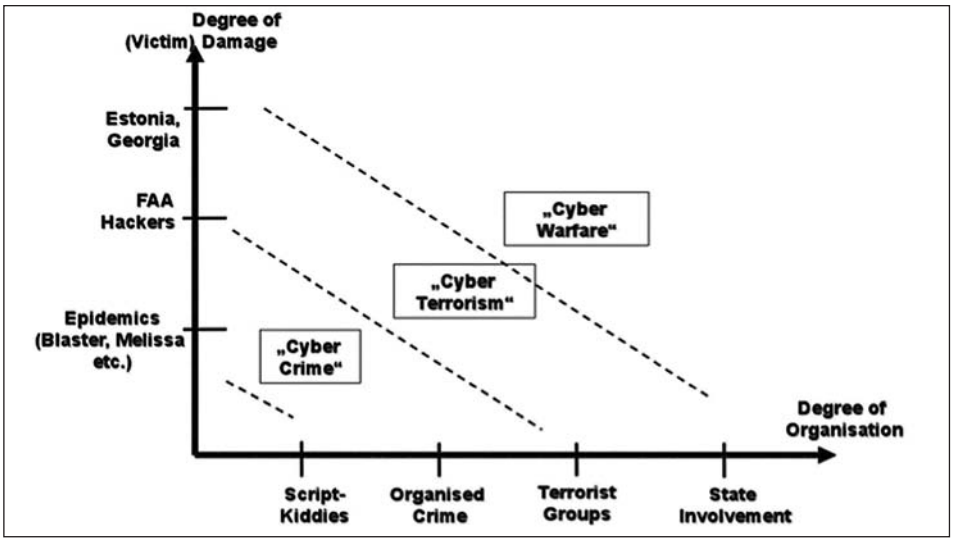
La Yihad Global se apoya en dos pilares: en el plano operativo en los ataques suicidas y en el de gestión, en Internet y en el ciberespacio. Las tres componentes necesarias para el éxito de una operación, incluidas las terroristas (mando, control y comunicaciones), las llevan a cabo a través de Internet. El ciberespacio es también la principal herramienta de propaganda, distribución de ideas, reclutamiento de voluntarios y recaudación de fondos de los terroristas islámicos.

Otra de las amenazas más importantes que se está materializando en este momento es el ciberespionaje. Algunos países, como China (24) y Rusia (25), han hecho de él una extensión de sus metodologías de espionaje clásicas. A partir de estas técnicas pueden adquirir información confidencial de todo tipo, ya sea proveniente de Estados, sus Ejércitos o información industrial que ofrecerá ventajas competitivas al mejor postor. Un ejemplo es la operación «Titan Rain», que implicaba el intento de obtención de información gubernamental de Estados Unidos y Gran Bretaña desde China y que ocasionó una gran fuga de información. En los últimos años, ha habido diferentes ciberataques a países por motivaciones políticas, como pueden ser los realizados contra Estonia, Georgia, Estados Unidos y Corea del Sur. Esto demuestra la capacidad de ciberataques que han obtenido países como Rusia y China, ganando una superioridad estratégica sobre el resto.

Por último, se cierne sobre nosotros el problema de la ciberguerra o ciberconflicto, ya que en teoría para que se pudiese denominar guerra

(24) Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Autor principal; Byan Krekel (Northrop Gruman Corporation).

(25) www.govsecinfo.com/events/govsec-2010/sessions/wednesday/joyals-general-session.aspx y www.nsci-va.org/WhitePapers/2010-02-Cyber%20Espionage%20-%20Is%20the%20US%20Getting%20More%20Than%20It's%20Giving-final%20v1.pdf



debería haber una declaración previa, que normalmente y en los tiempos actuales, no se suele producir. En la figura anterior, se recoge un interesante diagrama en el que se interpretan los posibles ingredientes que se necesitarían o que servirían para diferenciar la frontera entre los conceptos de ciberdelito, ciberterrorismo y ciberguerra, básicamente determinados por el grado de daño infligido y el grado de organización del atacante. Dentro del grado de daños, vemos la progresión desde un simple «gusano», pasando por los ataques sufridos por la Administración Federal de Aviación de EEUU, hasta llegar a los sufridos por Estonia o Georgia, que no dejan de ser el umbral previo a la ciberguerra; todavía nos queda mucho por ver. En cuanto al grado de organización, la ciberguerra requiere el respaldo de un estado.

Algunos estados han comenzado ya su carrera para la obtención de una capacidad de explotación y ataque, pues se atisban futuros ciberconflictos entre países, siendo el ciberespacio una dimensión más donde combatir, como pueden serlo tierra, mar, aire y espacio. Una gran cantidad de medios informativos(26) recogían a principios de octubre las «discusiones y especulaciones generadas a raíz de la aparición del gusano informático Stuxnet, en especial sobre quién está detrás del ataque y cuáles son sus objetivos».

(26) www.boletindintel.es/BoletinesAyS/Publico/PresentaContenido.php?Fase=1%20&%20Referencia=1343 y www.dintel.org/ También: www.economist.com/realarticleid.cfm?redirect_id=17147862

Según Eugene Karpersky, «este programa dañino no ha sido diseñado para robar dinero, bombardear con spam o acceder a datos personales; ha sido diseñado para sabotear y causar daños en entornos industriales. Mucho me temo que estamos asistiendo al nacimiento de un nuevo mundo. Los 90 fueron la década de los cibervándalos, la década del 2000 fue la de los cibercriminales, y tengo la sensación de que estamos entrando en la nueva era de las ciberguerras y el ciberterrorismo,» concluyó Kaspersky.

Según el Boletín DINTEL, la intención final de este gusano era acceder a sistemas de control industrial Simatic WinCC SCADA, que controlan procesos industriales, infraestructuras e instalaciones. Oleoductos, centrales eléctricas, grandes sistemas de comunicación, navegación aérea y marítima, e incluso instalaciones militares, utilizan sistemas similares. Tanto el blanco del ataque como la geografía donde se han detectado los primeros brotes (principalmente Irán), inducen a pensar que no se trata de un grupo cibercriminal normal. Es más, los expertos en seguridad de Kaspersky Lab, que han analizado el código del gusano, insisten en que el objetivo principal de Stuxnet no ha sido sólo el de espiar sistemas infectados, sino también el de llevar a cabo acciones de sabotaje. Todos estos hechos apuntan al hecho de que es muy probable que algún estado-nación, con acceso a grandes volúmenes de información de inteligencia, haya dado cobertura al desarrollo de Stuxnet.

Las redes de Mando y Control que manejan información clasificada poseen un alto nivel de protección y no están conectadas a Internet: sin embargo, esto no garantiza su seguridad «per se». Todos los SSOO (Sistemas Operativos) y gran número de aplicaciones empleadas en redes clasificadas son COTS (Commercial Off The Shelf), que requieren su actualización continua (especialmente para contrarrestar vulnerabilidades de seguridad), lo que se realiza a través de Internet en servidores separados, pero es prácticamente imposible analizar el código de dichas actualizaciones (a veces suponen millones de líneas de código y el fabricante no publica su contenido), por lo que solamente se suele probar en maqueta su repercusión en los sistemas antes de pasar a explotación.

Por otro lado, todos los «chips» son de manufactura no nacional y éstos pueden incluir en su «firmware» código dañino no detectable o de muy difícil detección. A día de hoy prácticamente la totalidad de los sistemas clasificados disponen de interconexiones a otros sistemas, ya sean OTAN, UE o de países aliados, lo que complica enormemente el

mantenimiento de la seguridad. Por último, tanto la OTAN y EE.UU, por ejemplo, han reconocido e informado de numerosos incidentes de seguridad en sus sistemas clasificados durante los últimos años.

Ataques e incidentes reseñables

Solo comentaré algunos de los incidentes más conocidos para poder situar el alcance de esta amenaza:

EEUU

Tal y como recientemente declaró el Vicesecretario de Defensa de EEUU, el señor William J. Lynn III (27), en la primavera de 2008, una variante de un gusano relativamente «benigno» de tres años de edad, comenzó su sinuoso camino a través de las redes militares clasificadas de EEUU, diseminado por medio de un dispositivo de almacenamiento removible («flash drive USB») introducido en un portátil en una base de Oriente Medio y se autocargó en una red del Mando Central de EEUU. El Pentágono ha afirmado hace unos meses que la penetración, fue un ataque deliberado lanzado por un servicio de información extranjero. El código se diseminó sin ser detectado tanto en redes clasificadas como no clasificadas, estableciendo lo que se puede considerar una «cabeza de playa» digital, desde la que los datos podían transferirse a servidores bajo control extranjero. Este gusano fue una auténtica pesadilla para los administradores de las redes, que necesitaron cerca de 14 meses de trabajo para su limpieza, bajo la operación denominada «Operation Buckshot Yankee» y constituyó el mayor compromiso de la seguridad de las redes militares de EEUU, marcando un punto de inflexión en su estrategia de ciberdefensa, lo que originó que se llevase a cabo una gran reorganización de las fuerzas de defensa de la información, incluyendo la creación del nuevo Mando del ciberespacio (Cyber Command) (28).

El 4 de julio de 2009, día en que se celebra la fiesta de la independencia en Estados Unidos, se sucedieron una serie de ataques de Denegación de Servicio contra diferentes instancias en ese país (la Casa Blanca, el Departamento de Seguridad, el Servicio Secreto, la Agencia

(27) www.cfr.org/publication/22849/defending_a_new_domain.html
(28) www.wired.com/dangerroom/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/#ixzz0zDYjk9kk

de Seguridad Nacional…), llevados a cabo por una red de «botnets» (29) de más de 50.000 ordenadores. Dos días más tarde, esta misma red atacó a otros once objetivos en el gobierno de Corea del Sur. Se concluyó que el autor primario de ambas operaciones era Corea del Norte, siendo los motivos políticos los más probables. Se sabe, además, que la inteligencia militar de este país ha entrenado a un conjunto de hackers para fortalecer su capacidad de ciberataque.

Estonia

Aunque este capítulo comenzaba con una mención a los ataques sufridos por este país, creo necesario dar alguna información complementaria, ya que se puede considerar como el primer ataque serio contra las infraestructuras cibernéticas de una nación. Estonia sufrió un fuerte ciberataque en los meses de abril y mayo de 2007. Fueron una continuación en el ciberespacio de los problemas relacionados con motivo de la retirada del monumento soviético conmemorativo de los soldados caídos durante la Segunda Guerra Mundial. Junto a las manifestaciones y protestas en las calles de Tallin, Estonia sufrió una serie de ataques informáticos que dejaron fuera de servicio los sitios Web del gobierno, bancos, escuelas, etc. durante unos días, requiriéndose el apoyo experto de la OTAN y países aliados para contener los daños. La agitación fue proporcionada por la propaganda rusa, difundida por medios de comunicación y foros de debate de Internet.

Los ataques iniciales del 27 y 28 de abril fueron simples, mal coordinados y fácilmente atenuados; hubo un par de páginas web que sufrieron «defacement» y muchos ataques de denegación de servicio (DDoS) (30) contra servidores web del gobierno. Algunos blancos civiles

(29) **Botnet** es un término que hace referencia a un conjunto de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del *IRC*: Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante *HTTP*, con lo que el control de estas máquinas será mucho más simple.

(30) Un **ataque de denegación de servicio**, también llamado ataque **DoS** (de las siglas en *inglés **D**enial **of** **S**ervice*), es un ataque a un sistema de *computadoras* o *red* que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del *ancho de banda* de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le

fueron también atacados, especialmente los portales de noticias. Las descripciones detalladas de ataque, información de objetivos y los datos de tiempo de ejecución fueron albergados en muchos foros de hackers rusos y foros de discusión. La información fue también diseminada vía Chats (charla interactiva) de Internet, MSN y correo electrónico. Algunos sitios también suministraron herramientas de software para atacar los objetivos designados.

El 30 de abril se produjo un cambio en el perfil atacante, cuando empezaron a aparecer programas de ejecución automática (bots) más grandes y ataques bien coordinados. Estos nuevos ataques también se dirigieron a la infraestructura de la red, a los Internet Service Providers (ISPs). Se atacaron también servidores DNS (31) en el ISP, con éxito en algunos casos, afectando a servicios de DNS temporalmente en gran parte de Estonia. Los robots de spam (publicidad/información no deseada) se usaron para atacar servicios de correo electrónico del gobierno con resultados diversos, si bien la mayoría de los sistemas pudieron resistir los ataques.

Ya el cuatro de mayo se produjo el mayor de los ataques. La mayoría de las agresiones eran relativamente «sencillas» y pudieron ser bloqueadas en los ISPs, aunque no obstante, algunos sistemas quedaron tem-

---

dice «denegación», pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

La forma más común de realizar un DDoS a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz.

(31) Domain Name System / Service (o DNS, en español: sistema de nombre de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

poralmente fuera de servicio. Después de los ataques del 4 de mayo, la situación pareció calmarse.

En la mañana del día 10, el sitio web www.hanza.net (el banco más grande de Estonia) fue blanco de un fuerte ataque de DDoS; más de 97 % de todas transacciones de banco en Estonia son realizadas en Internet. La mayoría de los demás ataques tuvieron poco efecto sobre la población.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y NORMATIVA EN EL MINISTERIO DE DEFENSA

La seguridad de la información en el Ministerio de Defensa se estructura en cinco áreas: «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en poder de las empresas», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones». Obviamente, este quinto capítulo se centrará en esta última área, aunque como es lógico tiene una estrecha relación con el resto de áreas.

En el año 2005 el Ministerio de Defensa vio la necesidad de afrontar un proceso de modernización, consecuencia de la evolución de las tecnologías de la información, que recogiera su política de seguridad de la información como documento único del cual debería emanar toda norma interna en materia de seguridad de la información del Ministerio, facilitando así, la necesaria coordinación en el desarrollo normativo posterior y de este modo alcanzar un conjunto normativo equilibrado, completo y con criterios unificados.

En el año 2006, se publicó la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprobó la mencionada política de seguridad de la información, con objeto de alcanzar la protección adecuada, proporcionada y razonable de la Información del Ministerio de Defensa, mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad.

Esta OM derogó la Orden Ministerial Comunicada 1/1982, de 25 de enero, por la que se aprobaban las normas para la protección de la documentación y material clasificado, y la Orden Ministerial 76/2002, de 18 de abril, por la que se aprobaba la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o

transmitida por sistemas de información y telecomunicaciones, si bien esta última estará transitoriamente en vigor en tanto no se publiquen las normas de «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», y «Seguridad de la Información en las Instalaciones», correspondientes al desarrollo normativo de segundo nivel de la política de seguridad de información del Ministerio. Su finalidad era establecer la estructura y responsabilidades en materia INFOSEC en el Ministerio de Defensa.

En la OM 76/2002, continúa estando por tanto en vigor lo siguiente:

- Que el Ministro de Defensa es la «Autoridad de Acreditación de la Seguridad de los Sistemas», si bien estará asistido por las siguientes «Autoridades Delegadas de Acreditación» (ADA):
  a) El Jefe del Estado Mayor de la Defensa, que es la ADA en los Sistemas conjuntos de Mando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica. El JEMAD cuenta con un Organismo de Acreditación para apoyo a sus funciones, que se ha articulado a través de la DIVICS (División CIS) y su Sección de Seguridad de la Información CIS.
  b) El Subsecretario de Defensa (SUBDEF), que es la ADA en el ámbito de los Sistemas responsabilidad del Órgano Central y periféricos del Ministerio de Defensa.
  c) El Jefe de Estado Mayor del Ejército de Tierra, el de la Armada y el del Ejército del Aire, que son las ADA,s en los Sistemas específicos de sus respectivos Ejércitos.
  d) El Director del CNI, que es la ADA en los Sistemas responsabilidad de su Organismo y en el ámbito internacional (OTAN, UEO y otras organizaciones internacionales). Asimismo es responsable de asesorar al resto de las ADA,s en materia INFOSEC (32) y coordinar en materia Criptográfica y TEMPEST(33). Designará un Organismo de Acreditación para apoyo a sus funciones.

También recoge esta OM la definición de acreditación de sistemas CIS, que creo pertinente traer a colación. En el ámbito de la seguridad de la in-

(32) Protección de la información almacenada procesada o transmitida, por Sistemas de Información y Telecomunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas.

(33) Transient Electro Magnetic Pulse Emanation Standard.

formación CIS, se entiende por «acreditación», la autorización otorgada a un Sistema por la Autoridad de Acreditación, para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación. La acreditación siempre estará basada en la Declaración de Requisitos Específicos de Seguridad del Sistema (DRES) y en los Procedimientos Operativos de Seguridad (POS), aparte de ser necesario un análisis de riesgos y un concepto de operación para la obtención de la citada autorización.

Volviendo de nuevo a la OM 76/2006, se establecen en dicha política las definiciones, los conceptos y los principios básicos comunes a todos los ámbitos del Departamento. Se designa como Director de Seguridad de la Información del Ministerio al Secretario de Estado de Defensa, y se le encomienda, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas.

Se establece, asimismo, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa, como órgano de coordinación de la seguridad de la información del Ministerio, que preside el Secretario de Estado de Defensa.

En el año 2010 se ha publicado la Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa. Estas normas tienen por finalidad establecer la estructura funcional de la Seguridad de la Información del Ministerio de Defensa, sus responsables y cometidos.

En ella, se designa al Director General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones. En el ejercicio de los citados cometidos será el interlocutor, a nivel corporativo, del Ministerio de Defensa con el Centro Nacional de Inteligencia y organismos externos al Departamento, con facultad de representar al Director de Seguridad de la Información del Ministerio de Defensa (DSIDEF) en el ámbito de sus competencias.

Asimismo, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de De-

fensa (Inspección General CIS) como órgano de apoyo técnico para la realización de las tareas encomendadas al Director General de Infraestructura en las áreas de su respectiva competencia. No obstante, parece estarse preparando una reorganización de esta Inspección que podría afectar a su dependencia orgánica y funciones.

Por otra parte, se designa al Director General de Armamento y Material como responsable del área de seguridad de la información en poder de las empresas. En el ejercicio de los citados cometidos será el interlocutor, a nivel corporativo, del Ministerio de Defensa con el Centro Nacional de Inteligencia y organismos externos al Departamento, con facultad de representar al DSIDEF en el área de su competencia.

Para llevar a cabo la dirección, ejecución y supervisión de la Seguridad de la Información del Ministerio de Defensa se establecen dos niveles funcionales: el Nivel Corporativo y el Nivel Específico.

El Nivel Corporativo, bajo la autoridad del DSIDEF, es responsable, en el ámbito del Departamento, de la dirección, coordinación, evaluación y supervisión de las medidas de seguridad de la información en las cinco áreas ya citadas.

En el Nivel Específico se establecen siete ámbitos (EMAD, los tres CCGG, SEDEF, SUBDEF y UME). El jefe o autoridad de cada uno de estos ámbitos, es el máximo responsable de la dirección, coordinación, ejecución y supervisión de las medidas de seguridad de la información específicas de cada ámbito, siguiendo los criterios unificados establecidos en el Nivel Corporativo. El Jefe de Estado Mayor de la Defensa, ejerce además las que son de su competencia respecto de los sistemas conjuntos de Mando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica.

La necesaria coordinación entre los niveles funcionales y sus diferentes ámbitos se realiza a través del ya mencionado Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa que se reunió por primera vez en septiembre de 2010. El seguimiento de las directrices establecidas en la Política de Seguridad de la Información del Ministerio de Defensa es realizado por el Comité de Seguimiento de la Seguridad de la Información del Ministerio de Defensa, que todavía no se ha reunido.

Asimismo, se establece que la Dirección General de Infraestructura es el órgano directivo al que corresponde, entre otras cosas, la prepara-

ción, planeamiento y desarrollo de los sistemas, tecnologías y **políticas de seguridad de la información del departamento**, así como la supervisión y dirección de su ejecución.

De la Dirección General de Infraestructura dependen directamente, entre otros, los siguientes órganos directivos relacionados con la seguridad de la información CIS:

- El Laboratorio de Ingenieros del Ejército, que entre otras tareas es el encargado de las imprescindibles mediciones «zoning» (34) de los locales en los que se instalan sistemas TIC. Estas mediciones también son realizadas por el GRUTRA del EA y por el CCN.
- La Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones, que ejercerá las funciones de definición de las políticas y estrategias corporativas en el ámbito de la Administración Electrónica, las tecnologías de la información, telecomunicaciones y seguridad de la información del Ministerio de Defensa, así como la planificación y coordinación de las actuaciones en estas materias.

En cuanto a la organización de la ciberseguridad en el Estado Mayor de la Defensa (EMAD), esta está regulada mediante la Instrucción 40/2008, de 15 de abril, del Jefe de Estado Mayor de la Defensa. En ella, se establece que la División de Sistemas de Información y Telecomunicaciones (DIVCIS) es el órgano del EMACON responsable del planeamiento, dirección y control del Sistema de Mando y Control Militar de las Fuerzas Armadas (SMCM), y de los sistemas de información y las telecomunicaciones que lo soportan. Son funciones concretas de la DIVCIS, entre otras, el planear, dirigir y coordinar las actividades **en materia de seguridad de la información en los sistemas de información y telecomunicaciones** que sean competencia del JEMAD. Para ello, se sirve de la Sección de Seguridad de la Información CIS, que es responsable de planear, coordinar y, en su caso, ejecutar, las actividades en materia de seguridad de la información en los sistemas de información y telecomunicaciones que sean responsabilidad del JEMAD, así como de la coordinación con los Ejércitos en dicho campo.

(34) Estas mediciones se efectúan para determinar el grado de protección ante emanaciones electrónicas e inducciones indeseables de los equipos a instalar y que pueden provocar pérdida o fugas de información de forma involuntaria, o su obtención intencionada por individuos malintencionados dotados de la tecnología adecuada. Este problema es especialmente importante en instalaciones que se encuentren en el interior de ciudades y que no cuenten con un perímetro de seguridad adecuado.

Dentro de este apartado normativo referente a la seguridad de la información en los sistemas CIS, no podríamos dejar de mencionar al Centro Nacional de Inteligencia (CNI), pues aparte de que en el Real Decreto 1126/2008 (ya mencionado anteriormente) por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, dispone que está adscrito orgánicamente al Ministerio de Defensa, con dependencia directa del Ministro, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional asigna a éste una serie de funciones que inciden directamente en todas las actuaciones de seguridad de la información del Ministerio. En él, se atribuye al Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), la responsabilidad de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica. Asimismo, es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones.

INFRAESTRUCTURA. ÁMBITOS DE PROPÓSITO GENERAL Y MANDO Y CONTROL

Plan Director CIS

La seguridad de la información CIS en el Departamento tiene dos ámbitos de muy diferentes objetivos y características: la WAN (35) de Mando y Control y la de Propósito General, de acuerdo con la Orden DEF/315/2002, de 14 de febrero, que aprobó el Plan Director de Sistemas de Información y Telecomunicaciones (PDCIS). Para su dirección, gestión y seguimiento, se creó el Comisionado del Plan, que luego pasó

(35) Las **Redes de área amplia** (WAN) son redes informáticas que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host acceden a la subred de la WAN por un encaminador o router. Suelen ser por tanto redes punto a punto.

a denominarse Inspección General CIS. En el PDCIS, se establecía que la Plataforma Informática y la Arquitectura técnica del Ministerio evolucionarían hacia un escenario cuya principal característica era la existencia de dos únicas Redes de Área Extensa (WAN) para dar soporte a todos los Sistemas de Información del Ministerio:

- Una WAN para Mando y Control Militar, cuyo despliegue y extensión se correspondería con el de los Puestos de Mando y los Centros de Comunicación. Esta WAN, se debería interconectar con los entornos tácticos, con los similares de la OTAN y con las redes de sensores que fuera necesario. Desde el punto de vista de la seguridad, al ser su orientación de carácter eminentemente clasificado y de utilización para operaciones y planeamiento militar, los sistemas que la componen deben estar acreditados al nivel de clasificación adecuado, normalmente RESERVADO Y NATO/UE SECRET, lo que como se puede imaginar supone unos condicionantes de administración, establecimiento de medidas de seguridad, cifrado y arquitectura muy exigentes y complejas.
- Una WAN Corporativa de Propósito General (PG), que daría soporte a todos los sistemas de información que no fueran específicos para mando y control y se extendería a todos los emplazamientos. Este entorno incluía la conexión a Internet del Ministerio de Defensa, a través de un único punto de acceso común para todos los usuarios y sería la única que la WAN de Propósito General tendría con el exterior. La WAN PG se configura y explota con una perspectiva corporativa e integrada, para lo que se creó el CCEA. En este único Centro Corporativo de Explotación y Apoyo se concentraron los entonces existentes Centros de Proceso de Datos y Explotación, ubicados en dos emplazamientos distintos.

Respecto de las Redes de Área Local (LAN), con carácter general, los emplazamientos del Ministerio disponen de una LAN integrada en la WAN de Propósito General. Además, en aquellos emplazamientos que lo requieren, se han establecido LANs para Mando y Control, físicamente aislada de la anterior e integrada en su correspondiente WAN. Por último, en aquellos emplazamientos que incluyen un Centro de Elaboración de Inteligencia puede existir una tercera LAN conectada también a la WAN para Mando y Control. Además y mientras que no se llegue a la implantación del concepto NEC, ya citado anteriormente, es necesario mantener una serie de extensiones de redes clasificadas de diferentes organizaciones, como la NATO Secret WAN, la ESPDNET de la UE, etc.

En cuanto a la interoperabilidad, existe una única plataforma tecnológica de interoperabilidad básica (mensajería interpersonal, flujos de trabajo, herramientas de trabajo en grupo, etc.) con dos dominios diferenciados para cada una de las dos redes WAN. Los servicios de directorio están basados en un modelo de dos directorios (uno por WAN), soportados en una única herramienta, con un diseño de arquitectura tal que permite en el futuro integrar fácilmente ambas estructuras, para lograr un único directorio.

En lo referente a Instrumentos y herramientas de seguridad, se ha desarrollado una infraestructura de Clave Pública (PKI) como soporte de seguridad para el acceso a la plataforma y a los sistemas de información, para el cifrado y para la firma electrónica. Para ello, se ha constituido una única Autoridad de Certificación (CA) raíz, para la gestión de dicha infraestructura con dos CA,s delegadas, una para cada entorno WAN, y tantas Agencias de Registro (RA) como sean necesarias. Como soporte físico de los certificados se decidió utilizar tarjetas con chips individuales y personalizadas para cada usuario del Ministerio. Todavía no se ha terminado de desplegar para la WAN PG y en la WAN de Mando y Control se empezará su despliegue en breve, aunque se ha elegido un soporte USB con el correspondiente chip.

COOPERACIÓN INTERNACIONAL

España es «Sponsoring Nation» del CCD COE («Cooperative Cyberdefence Center Of Excellence») de Tallin (Estonia) desde el mes de mayo de 2008. Como tal, tiene un representante en el «Steering Committee» para la definición de los POWs («Program Of Work») y dirección y control de sus actividades. Además, tiene desde su participación dos miembros en su plantilla, un Teniente Coronel en la vacante de Jefe del Departamento de Doctrina y Adiestramiento y un civil en calidad de científico en el Departamento de Investigación y Desarrollo. Estas personas dependen funcionalmente del EMAD, a través del Jefe de la Sección de Seguridad de la Información CIS.

Este Centro está realizando una considerable actividad promoviendo cursos de alto nivel técnico, conferencias internacionales con expertos de todo el mundo, acuerdos con diferentes instituciones y organismos, que no solo abarcan los aspectos tecnológicos sino también las consideraciones legales correspondientes a las actuaciones en el ciberespacio,

para lo que cuenta con un embrión de un Departamento a este respecto, que en breve obtendrá su dotación adecuada de recursos.

En este apartado hay que destacar también los trabajos y acuerdos internacionales que en el ministerio se han llevado a cabo o se encuentran en proceso de realización, tanto para el intercambio de información de ciberdefensa como para la adquisición de diversos equipos de cifrado o de gestión y distribución electrónica de claves para los cifradores. Es necesario nombrar asimismo, los trabajos en curso para el desarrollo de redes de coalición mediante federación de las diferentes extensiones nacionales, como es el caso de la AMN con la red de misión de ISAF, que conlleva un esfuerzo considerable desde el punto de vista de la seguridad. Mención aparte merece la participación en ejercicios de carácter multinacional en el ámbito de la ciberdefensa, que serán detallados en el siguiente apartado.

No se puede olvidar que también existe un amplio número de simposios, cursos internacionales (en las escuelas de la Latina y Oberammergau), grupos de trabajo, subcomités como el SC «information assurance» de la Alianza Atlántica, «workshops» como el de ciberdefensa OTAN, etc, en los que se viene trabajando desde hace años y que contribuyen a mejorar el conocimiento de nuestro personal y la interoperabilidad y eficacia de nuestros sistemas CIS, dotándoles de la seguridad adecuada. Cabe destacar dentro de este apartado la cumbre de Directores de Seguridad de la Información CIS de países de la OTAN, de reciente andadura (lleva celebrándose dos años) y en la que se tratan a alto nivel el estado, retos y problemas de la seguridad de los sistemas CIS OTAN y en especial la problemática relacionada con los de mando y control desplegados en operaciones.

FORMACIÓN Y ADIESTRAMIENTO

Sensibilización, Concienciación y Formación

La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio. La seguridad CIS es un campo amplísimo, que requiere de una especialización muy considerable y que además exige que dentro de ella se contemplen a la vez diversos campos de especialización. Es muy difícil encontrar personas que dominen todos estos campos. Por intentar identificarlos, podríamos decir que serían: la electrónica de red y comunicaciones (switches, routers, cifradores, etc),

los sistemas operativos y aplicaciones, las bases de datos y las aplicaciones web. Evidentemente no es lo mismo el conocimiento que debe tener un administrador de seguridad de una red que las personas que componen un equipo de acreditación de sistemas o las que pertenecen a un equipo de respuesta ante incidentes o de un CERT, lo que a su vez nos da idea de diferentes escalones y diferentes requerimientos. Como podemos imaginarnos, la formación mencionada requiere, además, de una continua actualización acorde con la vertiginosa evolución de las tecnologías de la información.

A modo de ejemplo de lo mencionado en el párrafo anterior, el reconocido Instituto SANS(36), ha sido patrocinador de una compañía que ha realizado un reciente estudio sobre la necesidad de profesionales de seguridad en el Reino Unido, llevado a cabo mediante encuesta entre los profesionales del sector más destacados y experimentados. Los principales resultados han sido que el Reino Unido tiene dificultad en encontrar personal para trabajos de ciberseguridad (aproximadamente el 90% de los encuestados) y los profesionales piensan que el número de puestos de trabajo necesarios se incrementará (60 % de las respuestas) a la vez que han detectado una disminución de solicitantes de puestos de trabajo en el conjunto del sector de Tecnologías de la Información. En cuanto a las razones que llevan a los profesionales de la seguridad a disfrutar de su trabajo, se destacan el hecho de que «no hay dos días iguales», el desafío continuo y lo interesante del trabajo y la sensación de que se está realizando algo que es realmente útil.

En el ámbito militar, la política de personal no favorece esta puesta al día, ya que hay que conjugar ésta con los cambios de destino, el cumplimiento de condiciones para dar perspectivas de promoción, los cursos de capacitación para el ascenso, etc. Todo ello lleva a la necesidad de contar con personal contratado de empresas, pero a la vez teniendo en cuenta que precisamente la seguridad es la menos externalizable en el caso de nuestras FAS, del gran coste económico que esto supone y por último en nuestros días con el problema añadido de la crisis económica que está ralentizando y en algunos casos impidiendo que se puedan desarrollar conforme a las previsiones y necesidades diversos programas de seguridad CIS.

No obstante, en este campo se pueden citar un elevado número de iniciativas, que van desde charlas rutinarias de concienciación para el

(36) www.sans.org/

personal que se incorpora a nuevos destinos, a cursos online, seminarios, cursos en los programas de formación y perfeccionamiento de los tres ejércitos, cursos conjuntos, «máster» por diferentes universidades subvencionados por el Ministerio o jornadas técnicas de temas específicos. Además, todos los años se celebran unas jornadas en el CESEDEN, denominadas Jornadas de Seguridad de la Información del MINISDEF. Estas se organizan en colaboración entre el EMACON (Estado Mayor Conjunto) y la DIGENIN (Dirección General de Infraestructuras), para concienciar y sensibilizar en esta materia y en su última edición supuso un gran éxito de asistencia con más de 350 participantes.

Ejercicios de ciberdefensa

El EMACON viene participando activamente desde el año 2008 en diversos ejercicios de ciberdefensa internacionales, entre los que se pueden citar los tres últimos ejercicios organizados por EEUU («US DoD International Cyber Defense Workshop») y los dos primeros ejercicios de ciberdefensa OTAN, en noviembre de 2009 y de 2010. Los ejercicios de EEUU han sido patrocinados por la «Office of the Secretary of Defense Networks and Information Integration, International Information Assurance Program (IIAP)» y dirigido por la «University of Nebraska Omaha». Por parte del EMAD participaron miembros de la Sección de Seguridad de la Información formando equipos con miembros invitados de dos CERTs nacionales: el CCN-CERT(37) e IRIS-CERT(38). La participación se llevó a cabo de manera remota a través de Internet. En cuanto al ejercicio OTAN de 2009, se pretendía comprobar los procedimientos entre el CERT OTAN y los CERT gubernamentales de los países participantes.

Durante 2009 y 2010, se ha participado en los trabajos del EUMS (European Union Military Staff) para la definición del Concepto de CNOs («Computer Network Operations») en operaciones militares lideradas por la UE.

Ya a nivel nacional, en octubre de 2009, el EMACON, a través de la Sección de Seguridad de la Información CIS y con la colaboración de Isdefe, organizó el Primer Ejercicio de Ciberdefensa de las FAS (ECD09), con más de 80 participantes de 20 equipos pertenecientes al Ejército de Tierra, Armada, Ejército del Aire, Cuartel General del Estado Mayor de la

(37) www.ccn-cert.cni.es/
(38) www.rediris.es/servicios/iris-cert/

Defensa (EMAD), Centro de Inteligencia de las Fuerzas Armadas (CIFAS), Centro Criptológico Nacional (CCN) y Guardia Civil.

Los resultados del ejercicio permitieron conocer con más detalle las capacidades técnicas actuales existentes en el Ministerio de Defensa en este ámbito de la Ciberdefensa, así como una primera aproximación de los diferentes centros y unidades con recursos humanos y conocimiento en esta área. Se ha podido confirmar que existe una capacidad inicial y que es vital continuar potenciando estas iniciativas para adecuarnos a las amenazas actuales, que están en continuo cambio. Es de destacar que la valoración realizada por los participantes, fue muy positiva.

En este mes de octubre se va a realizar el Segundo Ejercicio de ciberdefensa de las FAS. Para esta ocasión, la demanda de participación ha crecido de manera considerable, lo que constituye una excelente noticia. En esta edición, el ejercicio se dirigirá y controlará por entero desde el EMAD y se han introducido dos importantes mejoras en los escenarios de defensa y ataque, incluyendo sistemas SCADA y herramientas de análisis y correlación de eventos.

CIFRA

Como ya se ha citado anteriormente, corresponde al CCN la responsabilidad de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de informar sobre la adquisición coordinada del material criptológico, formar al personal de la Administración especialista en este campo y certificar la seguridad de las tecnologías criptológicas. La cifra es un aspecto imprescindible de la seguridad de nuestras comunicaciones. El uso masivo de las tecnologías de la información requiere de equipamiento de cifra acorde con las necesidades de los usuarios. Toda información clasificada que haya de ser enviada fuera del nodo donde se ha creado ha de estar cifrada. La certificación del cifrador (métrica de su capacidad) y algoritmos empleados deben estar de acuerdo con el nivel de clasificación de la información, si bien, en redes como pueda ser la WAN de Mando y Control, se utilizan los de más alta protección para ahorro de medios. Disponer de criptología nacional con seguridad verificable es un principio irrenunciable, ya que poner nuestras comunicaciones en manos de cifradores y algoritmos desconocidos o no controlados en todo su proceso de fabricación es inaceptable.

Las tendencias de las nuevas generaciones de equipos de cifra apuntan a contar con las siguientes características fundamentales: interoperabilidad entre cifradores con diferentes redes de acceso, interoperabilidad a nivel nacional y con aliados (mediante la implementación de protocolos de interoperabilidad como SCIP) y certificación múltiple (Nacional, OTAN, UE, mediante el empleo de un único equipo para proteger información diversos orígenes); asimismo, la implementación de módulos reprogramables es una característica de gran utilidad, especialmente de cara a las operaciones en coalición, que demandan la cesión temporal de medios de cifra a países con los que no existen los necesarios acuerdos o marcos de confianza en este campo.

Por otra parte, el mercado de productos de cifra es reducido, limitado casi exclusivamente a la Administración General del Estado (Presidencia del Gobierno, Ministerios de Asuntos Exteriores y su principal cliente, el Ministerio de Defensa). Existen pocas empresas nacionales que desarrollan productos cripto, que además son de tamaño y facturación reducido. A la debilidad del sector fabricante hay que añadir la rápida evolución de las tecnologías de la información que obligan a que el esfuerzo de financiación del desarrollo sea sostenido en el tiempo, para poder abordar la fabricación de nuevos productos de cifra que satisfagan las necesidades del Ministerio de Defensa.

CONCLUSIONES

Las tecnologías de la información hacen posible casi todo lo que nuestras FAS necesitan: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real y un largo etcétera. En menos de una generación, las TIC en el entorno militar han evolucionado desde una simple herramienta para mejorar la productividad administrativa a un medio estratégico.

Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar y aire, a través del ciberespacio. La situación podría agravarse con la actual crisis económica, ya que ésta está implicando una restricción en inversiones de seguridad tanto en empresas como en las administraciones públicas y las FAS.

La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias.

En el ámbito de las operaciones militares, los ciberataques también tienen que ser considerados como una amenaza, ya que cada vez resulta más probable que éstas se combinen con ataques informáticos con objeto de dejar fuera de servicio las redes y sistemas del adversario u orientar a la opinión pública a favor de uno de los contendientes.

La ciberguerra es asimétrica. El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares. Muchos ejércitos están desarrollando capacidades ofensivas en el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades.

Los sistemas en red no son los únicos susceptibles de presentar vulnerabilidades y ser atacados; tanto su software como su hardware pueden ser saboteados antes de ser unidos en un sistema en explotación. El riesgo de manipulación en el proceso de fabricación es totalmente real y es la menos comprendida de las ciberamenazas. El sabotaje es prácticamente imposible de detectar y peor todavía de erradicar.

Ejércitos de diversos países han reconocido formalmente al ciberespacio como un nuevo dominio de enfrentamiento («Global Commons»). Aunque el ciberespacio es un dominio hecho por el hombre, se ha hecho tan crítico para las operaciones militares como la tierra, el mar, el aire y el espacio.

La convergencia a NEC exigirá una mayor interconexión con otros sistemas (Federación de Redes), incluso con ONGs, lo que exigirá un considerable esfuerzo en seguridad de la información.

A nivel nacional, el Ministerio de Defensa ha llevado a cabo numerosas iniciativas, publicando la Política de Seguridad de la Información, sus normas de aplicación y tomando un buen número de medidas para incrementar la seguridad de su información, tanto en el ámbito de la red de Propósito General como en el de Mando y Control.

La seguridad de la información en el Ministerio de Defensa se estructura en cinco áreas: «Seguridad de la Información en las Personas», «Seguridad de la Información en los Documentos», «Seguridad de la Información en poder de las empresas», «Seguridad de la Información en las Instalaciones» y «Seguridad de la Información en los Sistemas de Información y Telecomunicaciones», designándose Director de Seguridad de la Información del Ministerio al Secretario de Estado de Defensa, y asignándole, en el ámbito del departamento, las funciones de dirigir la seguridad de la información, velar por el cumplimiento de la política de seguridad de la información y definir y crear la estructura funcional de la seguridad de la información, incluyendo, en esta última, el Servicio de Protección de Materias Clasificadas. También se designa al Director General de Infraestructura como responsable de las áreas de seguridad de la información en las personas, en los documentos, en los sistemas de información y telecomunicaciones y en las instalaciones y como órgano de apoyo técnico para la realización de estas tareas, se designa a la Inspección General del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (Inspección General CIS); como órgano de coordinación de la seguridad de la información del Ministerio, se establece, el Consejo de Dirección de la Seguridad de la Información del Ministerio de Defensa.

La dirección, ejecución y supervisión de la Seguridad de la Información del Ministerio de Defensa se lleva a cabo en dos niveles funcionales: el Nivel Corporativo y el Nivel Específico. El Nivel Corporativo, bajo la autoridad del DSIDEF y el Nivel Específico en siete ámbitos (EMAD, los tres CCGG, SEDEF, SUBDEF y UME), siendo el jefe o autoridad de cada uno de estos ámbitos, el máximo responsable de la dirección, coordinación, ejecución y supervisión de las medidas de seguridad de la información específicas de cada ámbito, siguiendo los criterios unificados establecidos en el Nivel Corporativo. El Jefe de Estado Mayor de la Defensa, ejerce además las que son de su competencia respecto de los sistemas conjuntos de Mando y Control, Inteligencia, Telecomunicaciones y Guerra Electrónica.

El Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), se le asigna la responsabilidad de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, además de garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

En el ámbito de la cooperación internacional en la ciberdefensa, España es «Sponsoring Nation» del CCD COE («Cooperative Cyberdefence Center Of Excellence») de Tallin (Estonia) y ha participado en los trabajos del EUMS para la definición del Concepto de CNOs en operaciones militares lideradas por la UE; además, el EMAD participa en un amplio número de simposios, cursos internacionales, grupos de trabajo, «workshops» y subcomités OTAN, etc, sin olvidar que el EMACON viene participando activamente desde el año 2008 en diversos ejercicios de ciberdefensa internacionales y organizando uno anual para las FAS.

La formación es uno de los puntos clave para poder obtener una adecuada defensa de nuestro ciberespacio. La seguridad CIS es un campo amplísimo, que requiere de una especialización muy considerable y que además exige que dentro de ella se contemplen a la vez diversos campos de especialización. Dentro de la formación y el adiestramiento y a nivel nacional, el EMACON, ha organizado dos Ejercicios de Ciberdefensa de las FAS con alrededor de 100 participantes distribuidos en 25 equipos pertenecientes al Ejército de Tierra, Armada, Ejército del Aire, Cuartel General del Estado Mayor de la Defensa (EMAD), Centro de Inteligencia de las Fuerzas Armadas (CIFAS), Centro Criptológico Nacional (CCN) y Guardia Civil, que está contribuyendo a la creación de una comunidad de ciberdefensa en el Ministerio.

La cifra es un aspecto imprescindible de la seguridad de nuestras comunicaciones. El uso masivo de las tecnologías de la información requiere de equipamiento de cifra acorde con las necesidades de los usuarios. Disponer de criptología nacional con seguridad verificable es un principio irrenunciable, ya que poner nuestras comunicaciones en manos de cifradores y algoritmos desconocidos o no controlados en todo su proceso de fabricación es inaceptable.

Las tendencias de las nuevas generaciones de equipos de cifra son: interoperabilidad entre cifradores con diferentes redes acceso, interoperabilidad a nivel nacional y con aliados, módulos reprogramables y certificación múltiple.

El mercado de productos de cifra es reducido, limitado casi exclusivamente a la Administración General del Estado. Existen pocas empresas nacionales que desarrollen productos cripto, que además son de tamaño y facturación pequeñas. A la debilidad del sector fabricante hay que añadir la rápida evolución de las tecnologías de la información que obligan a que el esfuerzo de financiación del desarrollo sea sostenido en el tiempo.

BIBLIOGRAFÍA

1. TIKK, Eneken; KASKA, Kadri; VIHUL, Liis;. *International Cyber Incidents, Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.
2. CZOSSECK, Christian; GEERS, Kenneth;. «The Virtual Battlefield: Perspectives on Cyber Warfare.» Tallinn: IOS Press BV, 2009.
3. LYNN, William J. III (Deputy Defense Secretary), *Defending a New Domain, The Pentagon's Cyberstrategy, Council on Foreign Relations, September/October 2010.*
4. KREKEL Byan, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* Northrop Gruman Corporation.
5. *SHARMA Amit, Cyber Wars: A Paradigm Shift from Means to Ends,* Institute for System Studies and Analysis del Ministerio de Defensa de la India.
6. PASTOR ACOSTA, Oscar; PEREZ RODRÍGUEZ, José Antonio; ARNÁIZ DE LA TORRE, Daniel; TABOSO BALLESTEROS, Pedro;. *Seguridad Nacional y Ciberdefensa.* Madrid: Cátedra ISDEFE-UPM, 2009.
7. *Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación* de la Política de Seguridad de la Información del Ministerio de Defensa.
8. Real Decreto 1126/2008, de 4 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa.
9. Instrucción 40/2008, de 15 de abril, del Jefe de Estado Mayor de la Defensa, sobre organización del Estado Mayor de la Defensa.
10. Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.
11. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
12. Orden Ministerial número 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.

13. Orden DEF/315/2002, de 14 de febrero, por la que se aprueba el Plan Director de Sistemas de Información y Telecomunicaciones y se establece, para su dirección, gestión y seguimiento, el Comisionado del Plan.

14. Informe de Amenazas CCN-CERT IA-01/09. Ciberamenazas 2009 y Tendencias 2010. Centro Criptológico Nacional.

15. Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations. The Secretary of Defense, EE.UU. JUN 09.

16. Computer Network Defense Roadmap. Department of the Navy. Chief Information Officer. May 09.

17. La ciberofensiva de China (y cómo pueden responder los EE.UU). DEF/361/09. Agregaduría de Defensa. 03 NOV 09.

18. Multiple Futures Project. Final Report. April 2009.

19. Virtual Criminology Report 2009. McAfee.

20. NATO Cyberdefence concept. Feb 09.

21. Directiva de Defensa Nacional 1/2008.

22. Concepto de Estrategia Militar.

23. Resolución A/63/37 de la Asamblea General de Naciones Unidas. 09 ENE 09.

24. Serie CCN-STIC (https://www.ccn-cert.cni.es/)

25. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

26. Normativa y Orientaciones (http://www.cni.es/es/ons/documentacion/normativa/).
    - NORMA NS/01: Infraestructura Nacional de Protección de la Información Clasificada.
    - NORMA NS/02: Seguridad en el personal. Habilitación de seguridad del personal.
    - NORMA NS/03: Seguridad Física.
    - NORMA NS/04: Seguridad de la Información.
    - NORMA NS/05: Seguridad en los Sistemas de Información y Comunicaciones.

- NORMA NS/06: Seguridad Industrial.
- NORMA NS/08: Protección de la Información Clasificada OTAN manejada en Sistemas de Información y Comunicaciones (CIS).
- Orientaciones:
  - Seguridad Documental:
    * OR-ASIP-04-01.03 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.
  - Seguridad en el Personal:
    * OR-ASIP-02-01.01 – Confección Solicitud HPS.
    * OR-ASIP-02-02.02 – Instrucción de Seguridad del Personal para acceso a IC.pdf.
  - Seguridad Física:
    * OR-ASIP-01-01.02 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.
    * OR-ASIP-01-02.02 – Orientaciones para la Constitución de Zonas de Acceso Restringido.