RED

Sistemas para CIBERDEFENSA

El ciberespacio es un nuevo ámbito de las operaciones militares que exige armas específicas

LOS seres humanos han combatido en cada momento de la historia con las armas y en los ámbitos en los que la tecnología disponible se lo ha permitido. Y, desde hace unos años, el ciberespacio se ha convertido en un nuevo entorno de las operaciones militares que requiere sistemas de armas específicos, tanto para proteger objetivos propios de la potencial acción del enemigo como para atacar los del adversario.

El Ministerio de Defensa cuenta con estructuras para dotar a las Fuerzas Armadas tanto de sistemas TIC como de sistemas de armas enfocados a los ámbitos terrestre, naval, aéreo y espacial. Pero quedaba pendiente un paso más, al que no ha sido ajena la Dirección General de Armamento y Material (DGAM), que a principios del año 2020 sintió la necesidad de contar con un departamento que aportara una visión unificada para la obtención de sistemas de ciberdefensa. El resultado ha sido incluir en el seno de la Subdirección General de Programas un dominio de competencias en este ámbito.

El nuevo órgano es la Jefatura de Sistemas Satelitales y de Ciberdefensa

(JSSAT-CIBER) que dirige el almirante Alfonso Pérez de Nanclares y engloba dos áreas. Una agrupa a las iniciativas vinculadas con el desarrollo del segmento de vuelo de los programas espaciales de navegación, vigilancia y comunicaciones. La otra acoge los proyectos relacionados con el componente del dominio de la ciberdefensa.

Aunque ambas esferas poseen distintas señas de identidad, las dos cuentan con un muy alto componente tecnológico, a la vez que gozan de transversalidad sobre el conjunto de los equipamientos que en los próximos años entrarán en servicio en las Fuerzas Armadas españolas.

GUÍA DE CIBERDEFENSA

Las actuaciones del equipo humano del Área de Ciberdefensa están enfocadas de manera fundamental a la obtención de sistemas para las «fuerzas de ciberdefensa». Su principal exponente es el Mando Conjunto del Ciberespacio (MCCE) y, más concretamente, la Fuerza de Operaciones del Ciberespacio (FOCE), que asume capacidades que abarcan la defensa, explotación y respuesta, las dos últimas, competencia exclusiva del citado Mando Conjunto.

También cumple la función de asesorar y orientar a las diferentes Oficinas de Programa y a sus órganos de coordinación en la Armada, los Ejércitos y los Mandos Conjuntos para la obtención, modernización o sostenimiento de los productos finales que requieren un alto grado de protección frente a ciberataques.

A su frente se encuentra el capitán de navío Enrique Cubeiro, quien formó parte del núcleo humano que dio vida al Mando Conjunto de Ciberdefensa (MCCD), donde ejercería la responsabilidad de jefe de Operaciones y, después, la de jefe de Estado Mayor, por lo que es un buen conocedor del sector de la ciberdefensa en sus vertientes nacional e internacional. Una de las primeras tareas que con carácter prioritario ha acometido es la redacción de una guía para concienciar y orientar en materia de ciberdefensa a los técnicos inmersos en hacer realidad fragatas, submarinos, vehículos de combate o aviones.

El documento se encuentra en la fase final de revisión previa a su publicación y en sus páginas explica la realidad de los riesgos asociados con el mundo ciber y el grado de exposición a las ciberamenazas. Contiene un compendio de reflexiones, recomendaciones y buenas prácticas que abarca desde los aspectos técnicos referidos a la arquitectura y las configuraciones hasta consideraciones contractuales, procedimentales y de concienciación.

Uno de los aspectos a los que más atención presta la guía es la seguridad

Peligros que exigen una sólida protección ciber

DELINCUENTES muy especializados y equipos multidisciplinares que suelen trabajar para el mejor postor o servicios de inteligencia de determinados países son capaces de encontrar vulnerabilidades, crear ciberarmas, sortear las protecciones de seguridad y penetrar en las entrañas de las redes de instituciones, empresas y ordenadores individuales para sustraer aquello que les interesa.

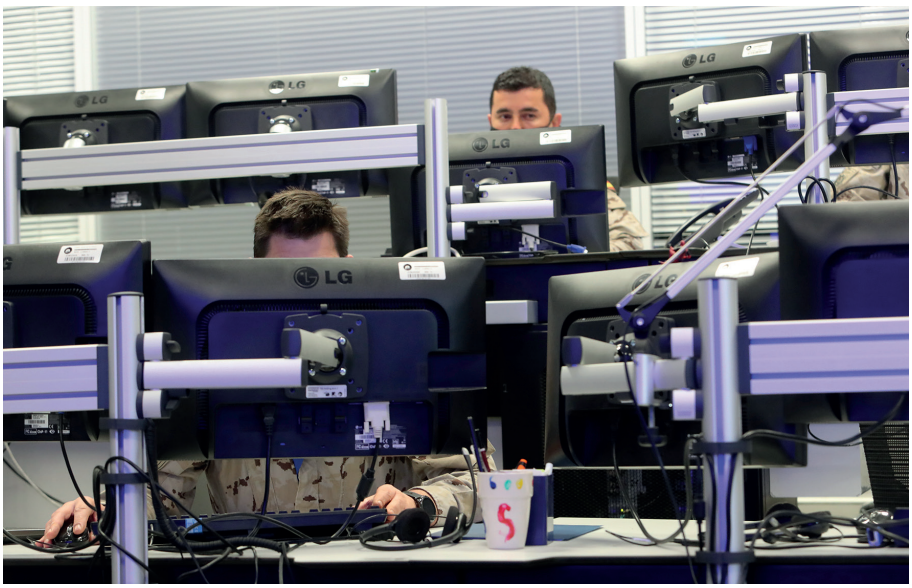
Mediante capturadores de pantalla, de teclado, recolectores de documentos PDF y otras muchas herramientas maliciosas, los intrusos bloquean, secuestran o recolectan información, la empaquetan, la trocean y la extraen sin que, en muchos casos, los propietarios o vigilantes lleguen a detectar la incursión.

Uno de los vectores de ataque más empleados es el correo electrónico a través del uso de una técnica que se conoce como *phishing*. Mediante la suplantación de una identidad conocida por el destinatario u otras técnicas de engaño, se incita a la víctima a ejecutar una determinada acción, a partir de la cual se inicia la secuencia de acciones maliciosas: robo de credenciales, ejecución de *malware*, cifrado de archivos, etcétera.

El jefe del Área de Ciberdefensa de la DGAM, capitán de navío Enrique Cubeiro, pone el acento en que las vulnerabilidades que en mayor medida son explotadas en los ciberataques son la falta de actualización o de mantenimiento de la red y el *software*, la inadecuada configuración de los elementos de seguridad de los sistemas, la existencia de interconexiones inapropiadas, las emanaciones electromagnéticas no deseadas y, por supuesto, los procedimientos incompletos o mal definidos.

MCCE

La Dirección General de Armamento y Material ya dispone de un área dedicada a programas de ciberdefensa



Pepe Díaz

La Fuerza de Operaciones del Ciberespacio (FOCE) asume capacidades que abarcan la defensa, explotación y respuesta a incidentes en este ámbito.

de la cadena de suministro, que está siendo cada vez más empleada como vector de ataque por las ciberamenazas. Entre las muchas modalidades se encuentra el *tampering*, que consiste en la manipulación malintencionada de un elemento *hardware* o *software* en algún escalón de la cadena logística, desde la fabricación a la instalación en el sistema. Para mitigar el riesgo asociado y evitarlo, es necesario implantar diferentes medidas a lo largo del proceso de aprovisionamiento.

CUATRO LÍNEAS DE ACCIÓN

En opinión del capitán de navío Cubeiro «la ciberdefensa debe contemplarse en todas las etapas de un programa. Eso abarca la fase conceptual y de definición, por supuesto la de desarrollo e incluso la de baja para el servicio». No hay que olvidar que las amenazas a las

De la espada al ordenador

DESDE el principio de los tiempos, la especie humana ha combatido sobre el terreno. Y a lo largo de los siglos se han ido perfeccionando las técnicas de combate y el armamento para adaptarse a ese entorno. Primero se incorporó la caballería, después las armas de fuego y la artillería, aparecieron las armas químicas, los vehículos blindados y armamento cada vez más preciso y sofisticado.

El mar fue el segundo ámbito de la guerra. Al principio se empleaban naves a remo, que combatían al abordaje. Con posterioridad llegó la propulsión a vela y la artillería en la edad media. La propulsión a vapor nacida en el siglo XIX supuso una tremenda revolución. Y, en el siglo XX, el submarino se convirtió en arma decisiva, al tiempo que la táctica y la estrategia naval evolucionaban continuamente con la aparición sucesiva de la aviación embarcada, los misiles, las comunicaciones vía satélite o las tecnologías *stealth*.

Hay que esperar hasta el siglo XX para ver convertirse el aire en campo de batalla. Hasta entonces tan solo había servido para apoyar la observación a distancia en el combate terrestre desde globos aerostáticos. Como en los casos anteriores, la evolución tecnológica obliga una y otra vez a revisar los conceptos doctrinales que rigen el combate: el motor a reacción, el radar, los misiles, las aeronaves no tripuladas…

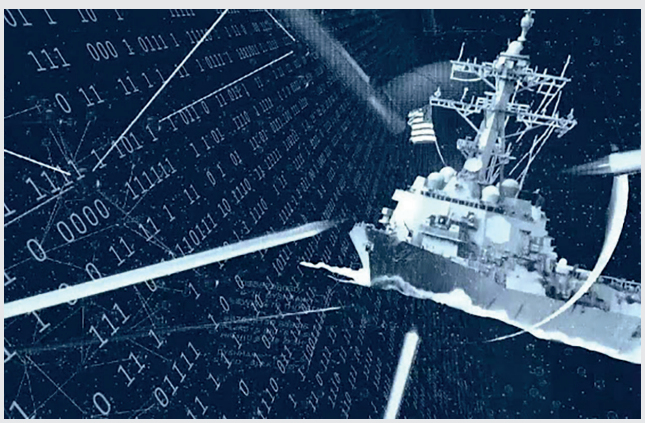
El espacio pasa a ser objeto del interés militar en la segunda mitad del siglo XX. Las operaciones militares se apoyan cada vez más en las comunicaciones vía satélite como medio vital para el ejercicio del mando y control. También en los satélites de observación para la obtención de inteligencia del adversario. Las potencias más avanzadas desarrollan capacidades para impedir el uso de estos medios al enemigo.

UN NUEVO ESCENARIO BÉLICO

En la frontera entre el siglo XX y XXI ha surgido el quinto dominio de la guerra: el ciberespacio. Un medio en el que, como en el terrestre, naval, aéreo y espacial, puede combatirse y en el que hay que defender los intereses propios de la acción del enemigo. Su objetivo es asegurar la libertad de acción a las fuerzas propias y negárselo o dificultárselo al oponente.

Se trata de un ámbito que puede llegar a tener una enorme influencia sobre los otros cuatro y que posee unas peculiaridades: requiere capacidades específicas para operar en él, no está completamente incluido en alguno de los otros cuatro dominios, existe presencia de fuerzas propias y adversarias, permite ejercitar el control sobre el oponente, y posibilita la asimetría y sinergia entre dominios.

En consecuencia, se necesita contar con capacidades específicas y fuerzas especializadas dotadas también de sistemas de armas y combate específicos para este ámbito de las operaciones.



La ciberdefensa influye sobre los otros dominios del combate: terrestre, aéreo, naval y espacial.

MCCE

La nueva área de la DGAM está elaborando una guía para concienciar y orientar en materia de ciberdefensa.

que se ve sometido un sistema de armas varían de forma sustancial a lo largo de su ciclo de vida, que puede superar los 20, 30 o incluso más años, «lo que en ciberdefensa es toda una eternidad», añade Cubeiro.

La mayor parte de la decena de proyectos de ciberdefensa que están en marcha se enmarcan todavía en el ámbito de la I+D+i y, por tanto, bajo el paraguas de la Subdirección General de Planificación, Tecnología e Innovación (PLATIN) de la DGAM.

Lo natural es que varios de esos u otros proyectos diferentes acaben transformándose en programas de obtención. De ser así, el Área de Ciberdefensa sería la que dotaría de recursos específicos a una o las varias Oficinas de Programa que se constituirían.

Entre las iniciativas que se están abordando figura, por ejemplo, el desarrollo de los sistemas necesarios para la obtención de la *Situational Awareness en el Ciberespacio*, la presentación de la *Cyber Operational Picture* y plataformas de respuesta o de adiestramiento en técnicas específicas. Se trata de proyectos que el Área de Ciberdefensa conoce y sigue muy de cerca, en estrecha coordinación con PLATIN y el Mando Conjunto del Ciberespacio.

El capitán de navío Cubeiro y su equipo de técnicos y especialistas se plantean cuatro primeras líneas de acción. Las dos de mayor trascendencia son la puesta a punto de un sistema ciber orientado al empleo de las unidades operativas y, por supuesto, la ya citada labor de asesoramiento directo a las Oficinas de Programas, cuya primera etapa es la guía.

Una tercera conlleva el establecimiento y mantenimiento de relaciones de confianza con las empresas y entidades vinculadas con el mundo de la ciberdefensa, tanto públicas como privadas. En cuarto término, efectuar el seguimiento puntual del estado del arte.

Recientemente se ha constituido un grupo de trabajo para mejorar la relación entre todos los organismos implicados en los futuros proyectos de obtención de sistemas para la ciberdefensa. Liderado por la Subdirección General de Programas de la DGAM, su cometido es coordinar, impulsar y efectuar el seguimiento y control de la gestión de dichas capacidades durante todo el proceso de obtención. Con ello se pretende conseguir el apoyo mutuo entre los diversos órganos participantes gracias a las aportaciones de las competencias de cada uno.

Juan Pons

Juan Pons

El capitán de navío Enrique Cubeiro está al frente del Área de Ciberdefensa en la DGAM.