¡*MALWARE* A BABOR! LA CIBERDEFENSA EXPLICADA CON SÍMILES NAVALES

Enrique CUBEIRO CABELLO

Introducción

EN mis ya casi cinco años como profesional de la ciberdefensa en un puesto relevante, como es el de jefe de Operaciones del MCCD (Mando Conjunto de Ciberdefensa), he podido constatar, con bastante frustración, el escaso conocimiento y entendimiento que existe sobre este campo y aplicable a todas sus dimensiones: desconocimiento sobre su naturaleza (¿esto de la ciberdefensa tiene que ver con las operaciones, con las infraestructuras o con los servicios?), entidad, cualidad y calidad de los recursos que han de dedicarse (¿es una prolongación de lo CIS o requiere recursos propios?, ¿qué es lo que van a hacer?, ¿cuántos hacen falta?), capacidades, tiempos y medios requeridos para el proceso de planeamiento de las acciones operacionales, asignación de cometidos y delimitación de responsabilidades, encuadramiento orgánico y relaciones de mando… Y podría seguir, pero solamente dispongo de unas pocas páginas.

Y cuando algo no se conoce o no se entiende, los que han de tomar decisiones se ven ante la disyuntiva de retrasar la decisión o correr un alto riesgo de equivocarse.

La ausencia de unos conceptos claramente definidos y universalmente aceptados nos lleva a carecer de un lenguaje común, lo cual, a su vez, dificulta la generación de la doctrina que, por otra parte, está muy mediatizada por la escasez de recursos (especialmente humanos) y por una aún nada clara asignación de cometidos y delimitación de responsabilidades, que además cada día parece más confusa y que está a su vez propiciada por la ausencia de una terminología común y de doctrina. Es como una pescadilla que se muerde la cola.

El que nadie nos entienda bien y el que esa falta de entendimiento redunde de forma muy evidente en nuestro perjuicio nos ha llevado a comprender la importancia de llevar a cabo un esfuerzo pedagógico.

Este artículo, cuya modestia viene ya dada por su propia extensión, nace con esa pretensión: explicar qué es eso tan raro de la ciberdefensa a personas sin muchos conocimientos en la materia. Para ello, basándome en mi experiencia y como ya anuncia el título, voy a apoyarme en una forma de explicación que he descubierto que es la más efectiva: la de utilizar el símil. Así, dado que el público al que primariamente va dirigida esta REVISTA es la Armada, recurriré una y otra vez a analogías que resulten bien conocidas para la mayoría de los lectores.

El hecho de que en el ciberespacio se navegue y que los dispositivos tengan unas cosas llamadas puertos puede ser un buen comienzo.

Ciberespacio, quinto ámbito de las operaciones

El hecho, avalado por la Historia, de que el ser humano ha combatido con las armas y en los entornos en los que la tecnología disponible en cada momento se lo ha permitido es lo que explica la reciente aparición del ciberespacio como quinto ámbito de las operaciones (1).

Este reconocimiento, todavía muy discutido, no es un asunto baladí. Como tampoco lo es el hecho de que prácticamente todas las naciones con algún peso en el tablero se están dotando de capacidades para negar el acceso del adversario al ciberespacio y asegurar el propio.

Pero, antes de continuar, es necesario analizar, aunque sea muy someramente, algunas peculiaridades del ciberespacio que explican el porqué de su complicado encaje con lo que hasta ahora existía.

Quizás lo primero a destacar es la intensa actividad hostil que en todo momento se desarrolla en él. En el resto de entornos no hay actores que de forma permanente y persistente traten de vulnerar nuestros espacios aéreo, marítimo o terrestre de soberanía. En el ciberespacio, sí. Y ello se explica por lo muy complicado que resulta no ya la simple detección, sino también la trazabilidad y atribución de casi cualquier ciberataque, lo que se traduce en la incapacidad de ejercer la disuasión al fallar uno de sus principales pilares: la disuasión por represalia (si no sé quién me ha atacado, difícilmente podré responder). De ahí que los ciberataques sean una de las modalidades de actuación que mejor se adapta a las características de la guerra híbrida.

---

(1) La OTAN, en la Cumbre de Varsovia de julio de 2016, reconoce el ciberespacio como quinto ámbito de las operaciones, junto con los espacios terrestre, naval, aéreo y espacial.

Relacionado con ello está la variedad de actores (agencias gubernamentales, organizaciones criminales, grupos *hackivistas* (2), grupos terroristas, individuos aislados) y motivaciones que hay detrás de esos ataques (obtención de información, beneficio económico, activismo, terrorismo, afán de notoriedad…).

Otra de las características del ciberespacio es su transversalidad con el resto de ámbitos de las operaciones: lo que ocurre en el ciberespacio tiene siempre un fuerte impacto sobre el resto. Y viceversa, aunque no de forma tan acusada.

Una peculiaridad que hay que entender es la diferencia que existe en lo relativo al tiempo y al espacio con relación al resto de ámbitos. En el combate naval, la distancia, rumbo, velocidad y alcance de las armas del enemigo son datos esenciales. En el ciberespacio, no. El adversario no está sujeto a ninguno de esos condicionantes. Puede atacar en cualquier momento y desde cualquier ubicación, lo que también impide utilizar los sistemas tradicionales de representación de la *operational picture* y dificulta su integración en la visión del campo de batalla global.

Tampoco son visibles en el ciberespacio los movimientos de tropas, ni apreciables los cambios de alistamiento. Consecuencia: no existe una alerta temprana efectiva que nos permita anticiparnos a la acción del adversario.

Y, cómo no, hay que referirse a las armas y a su control. También en esto el ciberespacio es muy diferente. No existe un *Jane's Fighting Ships* del ciberespacio. Ningún estado conoce a ciencia cierta qué tienen los otros. Con el agravante de que mientras en el ámbito naval el adversario va a ser por lo general otra fuerza naval de armamento conocido, en el ciberespacio puede ser cualquier cosa: desde una agencia de inteligencia de un gobierno extranjero a un adolescente con acné. Las ciberarmas tienen, a su vez, sus peculiaridades. Una de ellas es que su propio uso pone en riesgo su efectividad futura. Dado que las más sofisticadas se diseñan aprovechando alguna vulnerabilidad de objetivo, generalmente *software* y desconocida, el ataque puede alertar de su existencia y propiciar su corrección, anulando a partir de ese momento la efectividad de la ciberarma. Imaginemos lo que supondría si cada vez que lanzásemos un torpedo, el enemigo neutralizara su efectividad y tuviéramos que construir otro modelo para el siguiente ataque.

Hoy en día, en el proceso de planeamiento de un ataque se presta enorme atención a los efectos colaterales. Por mor de las interconexiones, esto es especialmente complicado en el ciberespacio. Nunca será posible una estimación tan precisa de sus efectos indeseados como la que aplica para

(2) Vocablo resultante de unir *hacker* y «activista».

el armamento convencional. Incluso el sistema más aislado y protegido habrá de contar con algún punto de entrada y salida de información; y usuarios, lo que impide confinar la propagación de sus efectos, que pueden aparecer, incluso años después, en sistemas muy remotos con relación al objetivo.

Para terminar este apartado, también es importante desmontar esa falacia, construida a partir de cientos de películas, de que los ciberataques se planean y ejecutan en cuestión de segundos. Por lo general, un ciberataque dirigido puede requerir semanas y hasta meses de planificación. En cuanto a su ejecución, los tiempos son muy variables, de segundos a años, en función del efecto que se persiga.

El MCCD

El MCCD se concibió en febrero del año 2013, mediante la Orden Ministerial 10/2013, de 19 de febrero, por la que se creó. Sin embargo, los primeros que alimentamos su plantilla no llegamos a sus entonces muy humildes instalaciones en la Base de Retamares hasta septiembre de ese año. Sin apenas recursos, puede decirse que los componentes pioneros del MCCD fuimos como una dotación de quilla que tuvo que construirse su propio barco y a la que se le obligó a navegar y hasta a disparar sus cañones antes de que este existiera.

En estos ya casi cinco años de vida, el MCCD se ha ganado un (creo) merecido prestigio. Es ya una unidad madura, que sabe a lo que se dedica, hacia dónde debe ir, que cuenta con personal formado y cualificado y unas capacidades reales y en continuo crecimiento. Somos como una fragata camino de su primera calificación operativa, paralelismo que puede extenderse incluso al tamaño de su dotación.

Aún así, hay cosas que no han variado, en particular, esa sensación de ser un ente todavía bastante desconocido y, por tanto, no del todo bien utilizado. Toca aquí, pues, explicar quiénes somos y a qué nos dedicamos, aunque sea de forma muy sucinta.

Lo primero que hay que entender es que el MCCD se dedica, fundamentalmente, al planeamiento y ejecución de operaciones en el ciberespacio. En ese sentido, su orgánica es semejante a la de la Armada: cuenta con un Estado Mayor, que hace las veces de Cuartel General; una Jefatura de Operaciones, que es la fuerza que ejecuta, y una Jefatura de Administración y servicios, que sostiene y apoya a la fuerza.

La Jefatura de Operaciones, como tal fuerza, utiliza sus sistemas de armas; sistemas que están enfocados a tres diferentes campos de actividad, pero muy interrelacionados: la defensa, la inteligencia y el ataque, que explicaré más adelante.

Al igual que la Armada, el MCCD dirige y coordina, por delegación del CMOPS (3), una de las operaciones permanentes que desarrollan las Fuerzas Armadas y que están contempladas en el OPLAN Marco. En el caso del MCCD, es responsable de la vigilancia y defensa permanente (24/7/365) del ciberespacio de interés. Asimismo, el comandante del MCCD tiene consideración de Mando Componente del Ciberespacio. Veamos cómo desarrolla su misión.

Las tres capacidades operativas: defensa, explotación y respuesta

La defensa, como su nombre indica, está enfocada a la protección. Puede decirse que el modelo adoptado es muy similar al de la defensa contra la amenaza aérea: descentralización y control por veto. El MCCD es a esa defensa lo que el AAWC (4) a la defensa aérea de una fuerza naval.

En este sentido, en la distribución de responsabilidades, el MCCD se hace cargo de la ciberdefensa de los sistemas conjuntos y corporativos, en tanto que los Ejércitos y la Armada lo hacen de los que son propios de sus ámbitos. Ello incluye unidades y sistemas de armas.

Los centros neurálgicos de esa defensa son los Centros de Operaciones de Seguridad (COS). El MCCD, que cuenta con sus propios COS, dirige y coordina la actividad del resto de estos centros. Además, en el desarrollo de la misión permanente ya mencionada, el MCCD ejerce sobre ellos el control táctico.

La dirección de las operaciones de ciberdefensa se desarrolla desde el Centro de Coordinación y Control de Ciberdefensa (C4D) del MCCD. Este viene a ser el CIC (5) de la ciberdefensa (tiene, incluso, un aspecto parecido): es el puesto de mando del comandante en jefe del MCCD en su calidad de Mando Componente, y desde donde se lleva a cabo la dirección, coordinación y control de las operaciones, mediante el procesamiento de la información sobre ciberdefensa procedente de las diversas fuentes y la disponibilidad de los medios de mando y control (C2) necesarios para la conducción de operaciones y diseminación de información a los diferentes mandos.

Para explicar mejor los cometidos de estos elementos, recurramos nuevamente a un símil. Como ocurre con una avería en un barco, un ciberincidente tiene una doble naturaleza: la técnica y la operativa. Un incendio a bordo de un buque pone en marcha esas dos vías. A la primera le preocupa contener y mitigar el fuego, coordina la labor de los trozos, se asegura de la estanquei-

(3) Comandante del Mando de Operaciones.
(4) AAWC: *Anti Air Warfare Commander*.
(5) CIC: Centro de Información y Combate.

dad; su información siempre queda en el ámbito del buque. A la vía operativa le interesa conocer lo que el incendio implica en términos de operatividad: pérdida de autonomía, velocidad o maniobrabilidad, limitaciones en el empleo de las armas y sensores… y es la responsable de comunicar con el exterior del buque, especialmente con la cadena de Mando. En un barco, la primera actividad se dirige desde la Central de Seguridad Interior; la segunda, desde el CIC. Ambas siguen una línea paralela, tienen que estar en continua comunicación, pero cada una entiende de cosas diferentes. La acción de un ciberataque sobre un sistema activa igualmente esas dos vías. La técnica (que atañe al COS) trata de contener y mitigar los efectos del *malware*; entiende de protocolos, firmas de *malware*, *back-ups*, segmentación de redes (el equivalente a la estanqueidad de un barco)… La operativa (C4D) es la que evalúa e informa del impacto operativo (limitaciones en el uso del sistema, sistemas alternativos, efecto sobre las operaciones en curso…) e informa a la cadena de Mando.

El MCCD se constituye como el CERT (6) del Ministerio de Defensa. En su origen, los CERT estaban muy enfocados a la gestión de incidentes. Hoy en día su abanico de servicios se ha ampliado enormemente, abarcando otros muchos: concienciación, auditorías, comunicación pública, formación, entrenamiento…

En estos años se han desarrollado también capacidades de defensa desplegables, que no son sino pequeños COS modulares y transportables, diseñados para la protección de redes en zona de operaciones.

Al ser, en muchos casos, la amenaza compartida, se dedica un importante esfuerzo a la cooperación. Nuestra relación con otros organismos, tanto nacionales como internacionales, es muy intensa, en especial con los otros dos CERT de la Administración: el CCN-CERT y el INCIBE-CERT. Por lo general, mediante la compartición de información técnica que contribuya a prevenir ataques.

La segunda capacidad operativa de ciberdefensa es la explotación, término adaptado del inglés *exploitation*, que es el utilizado en la doctrina de los Estados Unidos. Podría traducirse por «ciberinteligencia», aunque este vocablo también origina confusión. Necesitamos ese glosario de términos que no ofrezca lugar a dudas.

Es muy importante distinguir entre «ciberinteligencia» e «inteligencia en el ciberespacio». Hoy en día, debido a la escasez de recurso HUMINT (7), gran parte de la inteligencia se obtiene de fuentes abiertas, la mayor parte de ellas en el ciberespacio y, más concretamente, en Internet. La ciberinteligencia, si bien en parte se obtiene en el ciberespacio, es aquella que específicamente apoya la realización de operaciones en él. Es decir, está enfocada al cumpli-

(6) CERT: *Computer Emergency Response Team*.
(7) HUMIT: Inteligencia obtenida por fuentes humanas.

miento de la misión de las fuerzas de ciberdefensa, por lo que ha de ser un recurso orgánico. El objetivo primero de la capacidad de explotación es conocer las capacidades, intenciones, tácticas, técnicas y procedimientos de potenciales adversarios en el ciberespacio. Es, por motivos obvios, elemento esencial en el proceso de *targeting* (8).

Para ello, se cuenta con herramientas y técnicas específicas, numerosas fuentes de ciberinteligencia y personal altamente cualificado. La necesidad de concentrar los escasos recursos ha llevado a la decisión de que esta sea una capacidad que desarrolle en exclusiva el MCCD.

A pesar de la dificultad ya reseñada de contar con una alerta previa en el ciberespacio, es necesario mantener el conocimiento de la situación (*situational awareness*) en la medida de lo posible. Una de las actividades en las que esto se sustenta es la vigilancia digital, una especie de patrulla costera enfocada a las ciberamenazas, que abarca desde foros *hackivistas* a la *dark web*. Y como siempre pasa en este tipo de tareas, buscando champiñones a veces se encuentra algún Rolex (páginas de pornografía infantil, venta de credenciales robadas, planeamiento de ataques que afectan a otras organizaciones, *webs* de tráfico de armas), que inmediatamente denunciamos a los organismos responsables, con los que existe una muy estrecha colaboración.

El grupo de explotación es también el encargado de contextualizar aquellos incidentes tras los que se piense que existe un actor amenaza preocupante; por ejemplo, intentos de intrusión con fines de ciberespionaje tras los cuales se sospeche que está una agencia de inteligencia de un gobierno extranjero. Su objetivo, en este caso: dar respuesta a las cuestiones de quién, por qué y para qué.

La capacidad de respuesta puede traducirse perfectamente por capacidad ofensiva. Ello implica contar con desarrolladores de *malware*, expertos en intrusión de sistemas, ingenieros sociales… además de un arsenal de ciberarmas e infraestructura para su lanzamiento. Ha de entenderse en su conjunto como un sistema de armas, en el que el elemento humano es el más valioso por su dificultad de obtención. Al igual que la de explotación, y en parte por el mismo motivo (concentración de un recurso escaso), la capacidad de respuesta es exclusivamente desarrollada por el MCCD.

Este sistema de armas ha de ser capaz de llevar a cabo un amplio abanico de acciones, dirigidas a objetivos concretos, que abarcan la intrusión, degradación, neutralización o captura de activos adversarios, y, cuando así se requiera, de forma sigilosa y sin dejar trazas.

Un ataque dirigido es un proceso largo y complejo que comienza con un análisis profundo y metódico del objetivo, el descubrimiento de activos y vulnerabilidades, el diseño de una forma de penetración que permita la inser-

(8) Proceso de identificación, enumeración y desarrollo de objetivos.

ción del *malware*, así como el desarrollo de uno a medida del objetivo que explote alguna de las vulnerabilidades detectadas (algo así como diseñar el cañón y el proyectil correspondiente para cada acción), la estimación de los daños colaterales, la realización de ensayos en entornos de simulación, etc. Muy distinto a lo que vemos en el cine.

Transversal a las tres ya referidas, existe una cuarta capacidad de extraordinaria relevancia: la investigación digital, en la que también el elemento humano es con mucho el más valioso, permite analizar en profundidad aquellos incidentes que por su gravedad, novedad o por suponerse que son obra de un actor amenaza de primer orden así se determinen. Ello implica contar con personal muy experto y, dada la continua evolución de las ciberamenazas, en formación permanente. Asimismo, exige especialización en diversas áreas: en diferentes tipos de dispositivos (ordenadores, dispositivos móviles, sistemas de control industrial, IoT) (9), distintos sistemas operativos (*Windows, Android, IOS*), ingeniería inversa de *malware*, recuperación de datos y medidas antiforense.

Producto fundamental de esta capacidad son los indicadores de compromiso obtenidos del análisis de los ataques y del *malware* empleado —TTP (10) del adversario, firmas, vectores y patrones de ataque, elementos de mando y control, dominios y direcciones IP que forman parte de la infraestructura atacante—, que permiten la adopción de medidas en los sistemas de Defensa para detectar y rechazar ataques similares futuros.

El hecho de que las capacidades de defensa y ataque, además de las de ciberinteligencia e investigación digital, convivan en la misma unidad da lugar a una valiosa sinergia.

Formación y adiestramiento

La formación en ciberdefensa, que se desarrolla en el marco del Plan FORCIBE elaborado por el MCCD, contempla tres niveles: básico, avanzado y orientado al puesto. Hay que asimilar que la ciberdefensa actúa en el que, sin ningún género de dudas, es el entorno operativo más demandante y cambiante en el que operan nuestras Fuerzas Armadas. Ello origina, por una parte, la necesidad de un tremendo esfuerzo en formación; por otra, la imposibilidad de que un individuo abarque todo el campo de conocimiento. Por tal motivo, la especialización en ciberdefensa requiere el posterior desarrollo de perfiles muy dispares, orientados a los diferentes puestos de trabajo: operadores de monitorización, analistas forenses, expertos en intrusión en sistemas,

(9) IoT: *Internet of Things* (Internet de las Cosas).
(10) Técnicas, Tácticas y Procedimientos.

analistas de vulnerabilidades, ingenieros sociales, auditores, analistas de ciberinteligencia, programadores… que requieren una formación muy específica, en muchos casos difícil de obtener y, por lo general, muy cara.

El no contar con estos perfiles especializados sería como si el personal de la Armada tuviera una formación común única con la que hubiera que enfrentarse a cualquier puesto de trabajo: artillero, radarista, electricista, cocinero, escribiente, etcétera.

Y al igual que la Armada desarrolla sus ejercicios, las fuerzas de ciberdefensa también lo hacen, siguiendo la conocida máxima de «entrenamos como combatimos». Para ello, se cuenta con simuladores (*cyberranges*) en forma de entornos virtuales seguros, que reproducen con bastante fidelidad sistemas reales (*hardware, software*, usuarios) en los que pueden entrenarse distintas habilidades (por lo general, ofensivas y defensivas), tanto de forma individual como en equipo. Nuestro *cyberrange* es extraordinariamente versátil. Puede darnos desde el equivalente a una galería de tiro con pistola a un escenario muy complejo y cuasirreal, con múltiples actores y sistemas sobre los que pueden interactuar numerosos equipos.

Este año, el MCCD está liderando el potente equipo nacional que participa en uno de los ciberejercicios más avanzados del Mundo, el Locked Shields. Organizado por el Centro de Excelencia de Ciberdefensa en Estonia, reúne cada año a más de 1.000 participantes, distribuidos entre 25-30 equipos que representan a diferentes estados de la OTAN. El escenario de este año cuenta con más de 4.000 máquinas virtuales; en él, los equipos azules han de defenderse de los continuos ataques de los equipos rojos con un objetivo esencial: mantener el servicio a toda costa. El ejercicio no contempla únicamente aspectos técnicos, sino que incluye también retos legales, de información pública y valora la compartición de información y cooperación entre equipos. Viene a ser el equivalente ciberespacial al Trident Juncture.

¿Las ciberamenazas afectan a la Armada?

Llegados aquí, es posible que algunos lectores todavía no entiendan muy bien qué significan las ciberamenazas para la Armada y que aún sigan considerándolas como algo ajeno y que no afecta a la Institución. Como primera aproximación, que justificaré a continuación, me atrevo a afirmar que las ciberamenazas son, a día de hoy, uno de los principales riesgos para la Armada, si no el que más, tanto por su probabilidad de ocurrencia como por su elevado impacto potencial. Veámoslo con algunos ejemplos.

Las fragatas clase *Baleares* podríamos decir que eran «ciberinvulnerables». Lo mismo que las carabelas de Colón, simplemente por el hecho de ser básicamente analógicas y por no contar con conexiones con el exterior. En cierto modo, cuando una DEG largaba el último esprín del muelle quedaba tan aisla-

Fragata *Andalucía* de la clase *Baleares*. (Foto: *www.flickr.com/photos/armadamde*).

da del mundo exterior como si estuviera en Marte. No podemos decir lo mismo de las *F-100*. Prácticamente nada a bordo de la *Álvaro de Bazán* funciona sin algún tipo de *hardware* o *software*, los sistemas se interconectan unos con otros, el buque tiene elementos casi permanentemente conectados con el exterior (con el ciberespacio), a través de los cuales transmite y recibe información digital.

Producto tanto de esa naturaleza «ciberdependiente» como de las interconexiones entre sistemas, las *F-100* podrían ser vulnerables a un ciberataque. Así, sería teóricamente posible para un actor hostil introducir un *malware* que afectara a la funcionalidad de alguno de los sistemas esenciales del buque (sistema integrado de control de plataforma, sistema de combate…) afectando muy seriamente a su operatividad. Y para ello no sería necesario siquiera el acceso físico a la plataforma. Podría hacerse desde cualquier lugar del mundo, incluso con el barco en la mar. Bastaría con aprovechar alguna de las interconexiones a Internet por vía satelital: por ejemplo, la descarga de una actualización de la cartografía digital. Desconozco en profundidad la forma en que están interconectados los sistemas de una *F-100*, así que lo que sigue son únicamente suposiciones. Lo normal es que haya determinados elementos del buque, en particular en el puente, que integren información de diversos sistemas: cartografía digital, AIS, datos de rumbo y velocidad propios. Ello implica interconexiones. Y por la naturaleza transitiva de estas, si *A* está interconectado con *B,* y *B* con *C, A* lo está con *C*. Y si *A* es el SICP y *C* es Internet, tenemos un serio problema: el SICP podría ser accesible desde Internet, con lo que ello implica.

En las futuras construcciones navales esto ya se contempla, y en sus especificaciones se han incorporado elementos de ciberdefensa a bordo: *firewalls*, pasarelas, diodos, sistemas para la monitorización y correlación de eventos. Pero, a día de hoy, parece mucho más probable que una *F-100* pueda ser neutralizada mediante *malware* que por la acción de un torpedo o un misil. Y sin riesgo alguno para el atacante. También es probable que agentes potencialmente hostiles cuenten ya con la capacidad de hacerlo y que hasta hayan llevado a cabo pruebas de concepto.

Otro elemento fundamental para la Armada son sus sistemas de mando y control. Creo que, entendiendo que son sistemas construidos esencialmente mediante elementos *hardware* y *software*, cualquier lector reconocerá que son, por su naturaleza, intrínsecamente vulnerables a ciberataques. Lo mismo es extensible a cualquiera de los sistemas de armas medianamente modernos con los que cuenta la Armada.

Toda la estructura de gestión se apoya también en sistemas y aplicaciones que pueden ser atacadas a través del ciberespacio.

En resumen, la Armada depende completa y absolutamente del ciberespacio, tanto para su día a día como para el mando y control, la logística o las operaciones que llevan a cabo sus unidades. Podríamos decir que la Armada depende aún más del ciberespacio que del propio entorno en el que desarrolla su actividad: el mar (y aquí sonrío recordando esa frase que he oído tantas veces: «qué bien funcionaría la Armada si no tuviéramos barcos»).

El paraguas del MCCD no es aún lo suficientemente grande como para protegerlo todo. Y aunque lo fuera, nadie va a cuidar mejor un sistema que aquel que depende de su funcionamiento, premisa sobre la que se ha construido nuestro modelo de distribución de responsabilidades. Es, por tanto, necesario que la Armada desarrolle al máximo sus propias capacidades de ciberdefensa, al menos en su vertiente defensiva.

Epílogo

Cuando uno cambia de forma drástica el campo de su actividad profesional, es imposible no trasladar las experiencias pasadas al nuevo contexto. En mi caso, los más de quince años a bordo de buques de la Armada han impreso su sello indeleble al que no me puedo sustraer.

Por eso, en alguna ocasión especialmente tensa vivida en mi actual destino, lo que me ha pedido el cuerpo ha sido gritar por la megafonía: «¡Zafarrancho de combate! ¡Ciberataque en curso!».

Tres fragatas *F-100* en Ferrol, julio de 2017.
(Foto: Miguel Ramón Cuartero Lorenzo).