INCIDENCIA DE LA CIBERGUERRA EN LAS OPERACIONES NAVALES

Julio ALBERT FERRERO
Vicealmirante (2ª RE)

Introducción

La extraordinaria evolución tecnológica en los últimos años ha dado lugar a la aparición del ciberespacio como campo de batalla equivalente a la tierra, la mar, el aire, y el espacio aéreo, que estará presente a nivel global en todos los conflictos armados del futuro, de hecho ya lo está. El campo de la seguridad ha quedado notablemente ampliado. Este ciberespacio está sometido a constantes ataques cuya frecuencia, intensidad y complejidad crece continuamente y es motivo de preocupación en el ámbito internacional. La OTAN, la UE, los Estados Unidos y las naciones más importantes han tomado conciencia de esta amenaza y están analizando los procedimientos y estableciendo doctrinas para hacer frente a estos ataques, además de estar creando mandos dedicados específicamente a este campo.

Los ataques cibernéticos o ciberataques pueden llegar a bloquear y a paralizar la vida nacional, constituyendo la guerra cibernética o ciberguerra que transcurrirá paralelamente, o de forma independiente, con todo conflicto armado y por consiguiente tendrá una influencia sobre su desarrollo. En este artículo se describen las distintas operaciones que conforman la guerra naval y se analiza la incidencia de estos ciberataques en las operaciones navales.

La mayor parte de las operaciones en las que se puede ver envuelta una fuerza naval requieren una conducción estratégica y operacional, con un planeamiento y ejecución en ambiente conjunto y combinado. La naturaleza de estas operaciones exige un planeamiento complejo, que puede implicar a gran variedad de mandos de diferentes estados u organismos internacionales así como de diferentes ejércitos. Esto último tiene como consecuencia la necesidad de disponer de sistemas de mando robustos y potentes que permitan compartir la información y que esta sea accesible de manera puntual, precisa, y completa, para ello cobra especial relevancia la gestión de la información (*information management)* con el fin de facilitar el ejercicio del mando y la ejecución de las operaciones. Además el ambiente conjunto y combinado requiere una profunda coordinación y sincronización de las operaciones.

Por otra parte los avances de la tecnología en el ámbito del mando y control, están propiciando cada vez más la inmersión de los niveles de mando

estratégicos y operacionales en el nivel táctico. Esta inmersión es consecuencia, entre otras, de la necesidad de seleccionar los objetivos militares con la seguridad de no asumir riesgos que generen daños colaterales (ciclo de *targeting)* o efectos no deseados.

Los sistemas de mando y control empleados para el planeamiento y conducción de las operaciones en los niveles superiores antes mencionados consisten en potentes redes de comunicaciones que emplean fundamentalmente los satélites para asegurar la conectividad entre los diferentes niveles de mando. Estas redes están formadas por servidores informáticos que permiten planear, conducir e incluso ejecutar acciones militares. El ejercicio del mando se consigue mediante el empleo de servicios de intercambio de información, tanto de correo electrónico y empleo de *chat* (comunicaciones informales en claro), como de navegación por las páginas *web*.

Por todo lo anterior la ciberguerra supone una amenaza para las operaciones militares, principalmente en los niveles superiores de mando (estratégico y operacional) y en menor medida, en el nivel táctico.

Generalidades

Las operaciones navales se inician con la fase estratégica que comienza con el despliegue de la Fuerza Naval, seguida por las Misiones de Seguridad. El concepto de seguridad dentro de la estrategia y táctica naval es completamente distinto al de la seguridad referida a la defensa, puesto que las Misiones de Seguridad comprenden la Cobertura, la Exploración, la Vigilancia y la Búsqueda, que tienen por objeto conseguir la Seguridad del Mando y la Seguridad de la Fuerza, a su vez el mando consigue su seguridad cuando logra sorprender al enemigo. Inversamente la Fuerza consigue su seguridad cuando evita que el enemigo la sorprenda. En la guerra naval la frontera entre la estrategia y la táctica está precisamente en la fase de las Misiones de Seguridad que ocurre entre la fase de Despliegue y la fase de Contacto en la que actúan las armas. Las operaciones en esta fase dependen de las telecomunicaciones en las redes de mando y control y redes tácticas que enlazan a las fuerzas exploradoras con sus mandos naturales. Las redes de mando y control enlazan el Cuartel General del jefe del Estado Mayor de Defensa (JEMAD) con los Cuarteles Generales de los tres Ejércitos y a su vez el de estos con sus mandos operativos. En la Armada, hasta ahora el Cuartel General comunica con el Almirante de la Flota y sus mandos subordinados. Bajo el mando directo del JEMAD está el Mando de Operaciones que ejerce la dirección de todas las operaciones militares.

Recientemente (12 diciembre del 2012) se ha creado bajo el Mando del JEMAD, el Mando de Vigilancia y Seguridad Marítima y el Mando de Defensa y Operaciones Aéreas. El Almirante de la Flota será también el Comandan-

te del Mando de Vigilancia y de Seguridad Marítima apoyado por su Estado Mayor orgánico y mantendrá una doble dependencia, operativa del JEMAD y orgánica del almirante jefe del Estado Mayor de la Armada (AJEMA). Actualmente el AJEMA es quien ejerce el Mando de la Vigilancia Marítima y quien lo ejecuta es el Almirante de Acción Marítima (ALMART) desde Cartagena en el Centro de Operaciones y Vigilancia de Acción Marítima (COVAM). Igualmente el general jefe del Mando Aéreo de Combate del Ejército del Aire, será el comandante del Mando de Defensa y Operaciones Aéreas apoyado por su Estado Mayor orgánico y mantendrá una doble dependencia, operativa del JEMAD y orgánica del jefe del Estado Mayor del Aire (JEMA).

Con independencia de lo establecido anteriormente cuando las operaciones navales requieran conducción estratégica o empleen medios conjuntos las fuerzas orgánicas se integrarán en la estructura operativa de las Fuerzas Armadas (FAS) bajo el Mando del JEMAD.

El enlace entre las unidades que proporcionan las Misiones de Seguridad son normalmente helicópteros, aviones de Patrulla Marítima, se efectuará por redes tácticas que emplean el espectro electromagnético y no el ciberespacio por lo que su eliminación está cargo de las Contramedidas Electrónicas Activas (ECM) que son las que normalmente se emplearan en el nivel táctico, sin embargo siempre que se eleve el nivel operacional o el nivel estratégico se emplearán las redes de mando y control vía ciberespacio. Estas redes son cifradas y seguras, protegidas en las que todos sus elementos están sometidos a requisitos de seguridad física, por ejemplo accesos controlados etc.

En enero del 2013 se ha creado el Mando Conjunto de Ciberdefensa, ostentado por un general bajo la dependencia directa del JEMAD que tendrá la responsabilidad de ser el único mando que emprenderá acciones de Ciberdefensa para lograr los objetivos nacionales de Ciberdefensa.

Características de la ciberguerra

La ciberguerra puede ser una confrontación entre dos o más naciones en el ciberespacio en el que se emplean los ciberataques, por lo menos por parte de uno de ellos. Es un tipo de guerra asimétrica como el terrorismo internacional, en la que el enemigo es desconocido y no identificado (un único hacker puede poner en jaque a un estamento).

La ciberguerra no tiene fronteras puede atacar y ser atacada desde cualquier lugar del mundo, por lo tanto su campo de operaciones es enorme y tiene asegurado su anonimato. Sus características se derivan de las del Ciberespacio.

La ciberguerra se diferencia de los simples ataques, ciberataques, por la importancia de los daños que produce. La frontera entre ambos, en un principio podría ser, que los ciberataques serán considerados como el principio de

una ciberguerra, cuando produzcan la eliminación de una Infraestructura Crítica. Las armas de la ciberguerra, los virus, no producen destrucción sino interrupción de funciones por ello pasan a considerarse como armas de interrupción masiva y precisamente al no destruir tampoco disuaden, que es otra característica fundamental de la ciberguerra. Los virus no son las únicas armas de ciberguerra en la puede haber ataques de todo tipo más o menos sofisticados.

Los ciberataques serán rentables dada la desproporción entre las acciones de Ciberdefensa que normalmente requerirán tiempo y esfuerzo considerable y el propio ciberataque.

En la ciberguerra, el ciberespacio no se puede dominar sino que se comparte, al igual que ocurre con la situación estratégica de la guerra naval conocida como Dominio Compartido del Mar. Por lo tanto no puede existir Dominio del Ciberespacio al igual que el Dominio del Mar que solo existe como Dominio Relativo del Mar, situación que lo limita en el espacio y en el tiempo, y que se produce cuando ambos contendientes disponen de submarinos y de aviación naval. Otra característica de la ciberguerra es su similitud con la guerra electrónica, que tiene por objeto el dominio del Espectro Electromagnético, que afecta a las telecomunicaciones y a los sensores electrónicos, como el radar, mediante las operaciones de Contramedidas Electrónicas Activas (ECM) y Contramedidas Electrónicas Pasivas (ESM) y Contra Contramedidas Electrónicas (CCME) que actúan en el espacio aéreo. Las primeras tienen por objeto eliminar las telecomunicaciones y los equipos electrónicos radiantes de mando y control. Son medidas indiscretas. Las segundas tienen por objeto detectar la presencia y las características del enemigo mediante el análisis de las radiaciones de sus sensores y son medidas discretas. Las últimas son las medidas que anulan o tienden a anular las acciones ECM.

La ciberguerra en las redes de mando y control y en las telecomunicaciones

Las redes de mando y control son redes informáticas encriptadas es decir son redes seguras de comunicaciones en tiempo real con acceso a varias bases de datos, no suelen estar conectados a Internet, si lo están que no es lo normal, lo hacen a través de sofisticados dispositivos de seguridad, al correo electrónico, sistema cartográfico, y no suelen presentar la situación táctica, normalmente presentan la situación operacional o estratégica. Son cada vez más dependientes del Ciberespacio y del Espectro Electromagnético, a su vez es el área en la que se centra fundamentalmente la Ciberguerra. En Defensa se suele denominar redes de mando y control a las que manejan información clasificada. Las redes no clasificadas como la Red de Propósito General de Defensa (WAN PG), conectada a Internet, que es la que general-

mente se emplea entre los miembros de las Fuerzas Armadas diariamente, también son objeto de la Ciberguerra, incluso más que las redes de mando y control.

En Estados Unidos y en la OTAN, se ha desarrollado el concepto de Operaciones Cibernéticas en Redes; *Computer Network Operations* (CNO), cuyo objeto es el de conseguir la superioridad en la información negándosela al adversario.

Aunque la superioridad total es prácticamente imposible de lograr, habrá que obtener y mantener por lo menos una superioridad local durante las operaciones. Es difícil, casi imposible, ceñir la ciberguerra al ámbito local. Las CNO, se utilizan principalmente para degradar o engañar los sistemas de mando y control del enemigo, anulando su capacidad para tomar decisiones con eficacia, protegiendo al propio tiempo los sistemas de mando y control propios y amigos. Se subdividen a la vez en tres: *Computer Network Defence* (CND), *Computer Network Explotation* (CNE) y *Computer Netwok Attack* (CNA). Las CND tratan de analizar las características de los virus enemigos y de los demás tipos de posibles ataques para tratar de eliminarlos y por lo tanto tienen cierta relación con el cometido de las ESM, corresponden a una estrategia defensiva.

Las *Computer Network Explotation* (CNE) incluyen las acciones de recolección de información para inteligencia sobre sistemas de información enemigos, así como su explotación; y las *Computer Network Attack* (CNA) tienen por objeto interferir o bloquear los sistemas de telecomunicaciones y de mando y control y por lo tanto se corresponde con las ECM, que incluyen las acciones tomadas para perturbar, denegar, degradar o destruir información que circula por los sistemas enemigos y también a los propios sistemas, acciones que corresponden a una estrategia ofensiva.

La OTAN emplea entre otros sistemas el de mando y control *Maritime Command and Control System* (MCCIS), que la Armada ha adoptado como sistema propio de mando y control. La US Navy emplea el sistema de mando y control SIPRNET, así como el CENTRIX solo para las unidades que operan en el Índico. El Sistema de Mando Naval Nacional (SMN) se ha compatibilizado con el Sistema MCCIS a la vez que recibe información de otras fuentes. Se ha desarrollado el Sistema *Broadcast Maritime Readiness and Ships to Share System* (BRASS), para automatizar la radiodifusión en la transmisión de datos y del tráfico buque tierra entre los mandos en la mar y en tierra. Este sistema forma parte de la Red Marítima de Comunicaciones de la OTAN, opera en HF, LF, y en SATCOM.

El control y la gestión de la Información y su empleo en apoyo de las actividades propias han pasado a ser una de las prioridades principales y ocupaciones de un comandante en la mar y en tierra. Comprende aspectos tales como:

— Guerra Electrónica.
— Seguridad en las operaciones (MILSEC).
— Operaciones psicológicas (PSYOP).
— *Computer Network Defense* (CND).
— *Computer Network Attack* (CNA).
— Apoyo al seguimiento y destrucción física.

Los sistemas y redes de comunicaciones en la Armada son entre otros:

— Sistema de Mando Naval (SMN).
— SACOMAR Sistema automático de conmutación de mensajes.
— SIMENDEF. Sistema de comunicación conjunta.
— SMSC. Sistema de Mando y Control Militar.

Las nuevas tecnologías se aplican en cualquier unidad de la Armada tanto en las redes convencionales, que tratan de gestión, mensajes, intercambio de información entre los mandos como en otras redes menos convencionales, como los *data-link*, Manejo y Apoyo a los Sistemas de Combate, Control de Plataformas, que comprende la propulsión, la electricidad y otros servicios. La US Navy puede tener una información completa de la situación táctica en tiempo real vía satélite a través del *Link 16* vía satélite completada con la información que fluye por las redes de mando y control de sus sistemas *Command, Control, Comunications, Computer, Intelligence* (C4I).

Operaciones antisatélite

Los satélites artificiales tienen cometidos vitales. En la Guerra Naval. La dependencia global de las comunicaciones vía satélite, aumenta la vulnerabilidad de los sistemas frente a ataques físicos y cibernéticos. Su empleo es fundamental para el ejercicio del mando de las redes de mando y control, y al propio tiempo, enlace continuo entre los buques de la fuerza naval, permitiendo el conocimiento de la situación en la mar mediante los conocidos *Tactical Data Link* (TDL) que permiten el lanzamiento de armas de una unidad sobre un adversario cuya situación y datos operativos se han obtenido por otro buque de la fuerza Naval. Los TDL son susceptibles de ser atacados, aunque no es sencillo hacerlo. Los canales de radiocomunicaciones por los que puede discurrir información digital son también susceptibles de ciberataques. Otros cometidos importantes de los satélites son el de los satélites de reconocimiento de órbita terrestre a baja altura, que proporcionan fotografías de alta resolución muy importantes en las operaciones navales. La destrucción de estos satélites forma parte de la táctica antisatélite.

En las operaciones antisatélite hay que distinguir las que afectan a la destrucción del satélite que puede hacerse con armas tripuladas o con armas no tripuladas como son los misiles o con armas cinéticas, ambas de trayectoria balística orbital, o bien la perturbación de las señales que proporcionan la posición del satélite y de sus objetivos, y las que afectan a la información de sus enlaces, en este caso, correspondientes a las redes de mando y control y a las redes tácticas, en ambos casos son acciones electromagnéticas objeto de la guerra electrónica y acciones cibernéticas objeto de la ciberguerra.

En cuanto a las primeras, las ECM producirán la correspondiente perturbación. De igual modo en cuanto a las segundas, la perturbación entra dentro del campo de acción de las operaciones CNA, que se fundamentan en la inteligencia sobre las redes de mando y control del adversario. En cuanto a la destrucción física del satélite, su parte más vulnerable es la antena y los componentes terrestres más vulnerables de un sistema satélite son los segmentos de la estación terrestre.

Entre las armas cinéticas está el cañón electromagnético fundado en la energía cinética que transporta un móvil (1/2 MV2) impulsado inicialmente por la reacción que se produce entre dos campos magnéticos de la misma polaridad, en este caso entre el cañón y el proyectil, reacción que imprime al proyectil una trayectoria balística a gran distancia. No emplea pólvora ni explosivo alguno simplemente el tremendo choque físico contra el blanco. Otro tipo de armas cinéticas antisatélite es el de los vehículos cinéticos de destrucción que se separan de sus sistemas propulsores y corrigen su trayectoria hasta colisionar con el satélite.

Generalmente los satélites son un objetivo real de los Estados, que emplean tácticas antisatélite, ataques *hacking* y ataques de pulso electromagnético (EMP). Este pulso electromagnético se puede crear mediante la explosión a gran altura de un misil balístico que genera una fuerte perturbación electromagnética, el EMP; con suficiente fuerza para producir corte de comunicaciones y para dañar infraestructuras críticas. La mayor amenaza para las comunicaciones vía satélite son los ciberataques patrocinados por gobiernos extranjeros. Otra clase de perturbación es la producida por interferencia de la radiofrecuencia, perturbación difícil de lograr toda vez que el enlace es dirigido y el perturbador tiene que situarse entre el satélite y la unidad receptora.

Recientemente el grupo Anonymous interfirió con éxito un satélite de la NASA, consiguiendo información sobre sus proyectos.

La ciberguerra en la lucha contra el tráfico marítimo

La lucha contra las comunicaciones marítimas en su doble vertiente, la de ataque al tráfico mercante enemigo y la protección del tráfico marítimo propio es el cometido más importante de las marinas de guerra de los países de

condición marítima, porque afecta a la supervivencia nacional. El ataque al tráfico enemigo estará a cargo de la fuerza submarina propia principalmente, que no requiere el empleo del ciberespacio y por consiguiente no parece que tenga aplicación la ciberguerra, dada la independencia de actuación que caracteriza al arma submarina. Cuando el ataque al tráfico se efectúa por las fuerzas aeronavales de superficie, como los Grupos de Ataque Antisubmarinos *(Hunter Killers)*, que requiere coordinación las operaciones de ciberguerra tiene su aplicación.

En cuanto a la defensa del tráfico propio, según la doctrina naval actual, es preceptiva la formación de convoyes y la protección de unidades valiosas, lo que requiere el uso de las telecomunicaciones y de las redes de mando y control que a pesar de ser redes seguras estarán expuestas a los ciberataques, que exigirán las respuestas cibernéticas de los equipos de respuesta rápida (RRT), de los cuarteles generales afectados

La ciberguerra en el dominio del mar

El Dominio del Mar es una situación estratégica en la que se ha obtenido la libertad de acción en la mar y se le ha negado al enemigo. Con la aparición del submarino y del avión esta situación ha quedado eliminada ya que una fuerza naval por poderosa que sea no puede evitar la presencia de submarinos y aviones en el espacio aeronaval, por lo que su libertad de acción queda mermada. Sin embargo existe la posibilidad de que de un modo coyuntural limitado en el espacio y en el tiempo, en la que no estén presentes ni submarinos ni aviones, por la que queda establecida la situación estratégica de dominio relativo del mar como ocurrió en el Desembarco Alemán en Noruega durante la Segunda Guerra Mundial. *Esta situación estratégica se consigue por la destrucción del enemigo por el combate aeronaval o por el bloqueo de la fuerza aeronaval*.

El combate aeronaval va precedido del correspondiente despliegue estratégico de las fuerzas combatientes, seguido por una fase de aproximación en las que se desarrollan las Misiones de Seguridad referidas anteriormente, que normalmente finalizarán con la fase de búsqueda que dará lugar al despliegue táctico antes de iniciar la fase de contacto que desembocará en el combate. En la Exploración y la Búsqueda cuando se empleen aviones no tripulados serán controlados principalmente por canales cibernéticos. En el caso de que las fuerzas navales cuenten con aviación embarcada el combate se iniciará por el bombardeo aéreo seguido por el *combate naval de superficie*, en sus distintas modalidades de Combate, en Alta Mar, Combate en el Litoral, Combate en el Origen o Combate en una Ofensiva de Base Geográfica.

Dada la entidad de todo combate naval de superficie, estarán presentes desde el principio, tanto la guerra electrónica como la ciberguerra. Las

operaciones de guerra electrónica comenzarán con las acciones de ESM con el fin de obtener los parámetros de los radares enemigos, seguidas por la activación de las ECM para perturbar los radares y las telecomunicaciones del adversario. En cuanto aparezcan los primeros síntomas de un ciberataque, se iniciaran acciones defensivas de Ciberdefensa (CND), pasando al propio tiempo a utilizar canales alternativos que deberán estar previstos en el planeamiento militar. La fuerza aeronaval establecerá un ciberplan de silencio cibernético compatible con las operaciones en curso, con idéntico espíritu restrictivo al de los planes de silencio de comunicaciones y de guerra electrónica.

Cuando uno de los contendientes cuenta con una importante fuerza submarina y su fuerza naval de superficie es manifiestamente inferior a la de un adversario de condición marítima, que necesita del transporte marítimo para el desarrollo normal de su existencia queda establecida la situación estratégica conocida como Dominio Negativo del Mar, como sucedió durante la Segunda Guerra Mundial en la que la poderosa fuerza submarina germana consiguió en auténtico dominio negativo del mar. En este caso puede no tener aplicación la ciberguerra dada la característica de sigilo e independencia que tienen los modernos submarinos. La situación más normal será la de un Dominio Compartido del Mar cuando sea un conflicto simétrico en la que cada uno de los contendientes conserva cierta libertad de acción en la mar. Las operaciones ofensivas en red (CNA) por su complejidad quedan limitadas a los Centros de Respuesta Rápida (RRT) existentes en los Cuarteles Generales instalados en tierra.

En cuanto *al bloqueo naval* solo existe el bloqueo a distancia y ha quedado eliminado el bloqueo cerrado debido a la aparición de la aviación y de la guerra de minas. Durante la guerra civil española la Flota Nacional ejerció el bloqueo naval desde Palma de Mallorca sobre la Flota Republicana basada en Cartagena. Las operaciones de ciberguera serán semejantes a las indicadas anteriormente.

La explotación del dominio del mar

Una vez logrado el Dominio del Mar o mejor dicho el Dominio relativo del Mar aparece la situación estratégica de Explotación del Dominio del Mar, que consiste en las Operaciones de Proyección del Poder Naval sobre Tierra, que se subdividen en: *operaciones anfibias, el bombardeo naval y el bombardeo aeronaval*.

La ciberguerra en la explotación del Dominio de Mar será analizada a continuación desde cada una de las operaciones correspondientes indicadas.

La ciberguerra en las operaciones anfibias

En las operaciones anfibias intervienen la fuerza naval, la fuerza aérea y la fuerza de desembarco de Infantería de Marina. Aunque doctrinalmente sean operaciones navales de apoyo (es decir que las operaciones anfibias no son operaciones conjuntas), el planeamiento es conjunto entre las tres fuerzas.

Las operaciones constan de las fases de ensayo, embarque, movimiento a la zona objetivo y asalto anfibio bajo el mando naval de la Fuerza Anfibia Operativa (FAO), seguida por la fase de consolidación de la cabeza de playa bajo el mando del jefe de la Fuerza de Desembarco de Infantería de Marina (FD) a continuación tiene lugar el desembarco administrativo de las fuerzas del Ejército de Tierra que llevarán acabo el paso de escalón y finalmente la fase de reembarque de la fuerza de desembarco bajo el mando del Jefe de la FAO.

Las operaciones anfibias son las operaciones mas complicadas y completas de la guerra naval, dado que a lo largo de ellas tienen lugar todas las operaciones de dicha guerra, tales como guerra de minas, combate aeronaval, lucha antisubmarina, fuego naval de apoyo bombardeo aéreo, y guerra naval especial., por ello el planeamiento es complejo especialmente el planeamiento logístico y el de la organización de la cabeza de playa

La ciberguerra afectará a las tres fuerzas participantes, la FAO, la FD y la Fuerza Aérea, dada la importancia de este tipo de operaciones será preceptivo el empleo de las redes de mando y control y por lo tanto pueden ser objeto de ataques cibernéticos y de contramedidas electrónicas tanto en el nivel táctico como operacional y estratégico, que tenderá principalmente a interferir especialmente en los aspectos logísticos de las operaciones.

La ciberguerra en el bombardeo naval

El bombardeo naval por la fuerza naval de superficie puede ser sobre objetivos terrestres o sobre los blancos de la cabeza de playa, en las operaciones anfibias (esto exige artillería de calibre superior a las tres pulgadas). El empleo de las redes de mando y control quedará limitado acciones de nivel táctico, por lo tanto no se producirá normalmente interferencias de la ciberguerra. Sin embargo en situaciones de crisis un pequeño acaecimiento táctico se puede convertir en estratégico.

La ciberguerra en el bombardeo aeronaval

El bombardeo puede estar a cargo de la aviación embarcada sobre objetivos en tierra o sobre la cabeza de playa en las operaciones anfibias, en ambos

casos, al igual que en el bombardeo naval, el empleo de redes de mando y control se limitará para las acciones de nivel táctico y por consiguiente no se producirán ciberataques. Por el contrario, en el ámbito de una operación conjunta, y el bombardeo lo hace la aviación basada en tierra, es decir perteneciente al Ejército del Aire tanto sobre blancos en tierra o sobre blancos en la cabeza de playa se emplearán redes de mando y control, por tratarse operaciones que requieren niveles de mando de cierta entidad dentro del ámbito operacional o estratégico por lo que habrá gran probabilidad de ciberataques.

La ciberguerra en las operaciones antiaéreas

Cuando la amenaza sea exclusivamente aérea el cometido de la fuerza naval no es el de lograr el dominio del mar sino el de garantizar la seguridad de la fuerza o sea que tiene un carácter defensivo dando lugar a la guerra antiaérea. Estas operaciones se desarrollan dentro de un nivel táctico que no requiere el empleo de las redes de mando y control por lo tanto no se verán afectadas por la ciberguerra. Puede utilizarse el nivel operacional por necesidades de coordinación con el consiguiente empleo de comunicaciones los sistemas *Data Link* vía satélite susceptibles de ser interferidos por la guerra electrónica como por los ataques cibernéticos. Estas operaciones no existen en el nivel estratégico.

La ciberguerra en la lucha antisubmarina

Cuando el cometido de la fuerza submarina enemiga implique el ataque a la fuerza naval propia se establece una lucha antisubmarina de carácter defensivo que se desarrolla dentro de un nivel táctico que normalmente no requiere el empleo de las redes de mando y control, si por el contrario nuestra fuerza naval despliega en demanda de los submarinos enemigos, la lucha antisubmarina tiene un cometido marcadamente ofensivo, que probablemente exigirá una coordinación con otras fuerzas navales propias. En este caso las operaciones tendrán lugar dentro de los niveles operacional y táctico. Por consiguiente podrán harán uso de las comunicaciones y de los sistemas *Data link* vía satélite, que pueden ser interferidas santo por la guerra electrónica como por los ataques cibernéticos.

La ciberguerra en la guerra de minas

La guerra de minas comprende el minado ofensivo contra el tráfico marítimo del enemigo en el acceso a sus puertos o en sus zonas fértiles, y el minado

defensivo en los accesos a nuestros puertos, bases navales o zonas fértiles de nuestra navegación mercante y en las operaciones de contraminado. Aunque estas operaciones tienen un contenido estratégico corresponden acciones que se desarrollan en un nivel táctico que normalmente no requiere el empleo de redes de mando y control, sino simplemente serán de comunicaciones directas con sus mandos a flote y que por lo tanto no parece pueden ser objeto de la ciberguerra.

La ciberguerra en la guerra naval especial

La Guerra Naval Especial es el conjunto de de las operaciones navales que se realizan en la mar en apoyo a las operaciones navales expedicionarias en general y en particular en operaciones de apoyo a la proyección de fuerzas de la Infantería de Marina.

La Guerra Naval Especial de la Armada está constituida por su jefe, coronel de Infantería de Marina, o capitán de navío, bajo el mando del Almirante de la Flota, las unidades de la Guerra Naval Especial, procedente de la Unidad de Operaciones Especiales de Infantería de Marina, y la Unidad de Buceadores de Combate así como de las plataformas de proyección e inserción y unidades de apoyo aptas para el empleo en Guerra Naval Especial cuando sean asignadas, sus cometidos son:

— Obtención de Inteligencia específica y concreta y perecedera de interés estratégico u operacional, por medios humanos y en territorio hostil, de acceso restringido o políticamente sensible.
— Ataque específico y concreto a blancos de interés estratégico y operacional o cuando se están llevando a cabo operaciones determinadas.
— Amplio espectro de medidas en apoyo a fuerzas a liadas o amigasen paz, crisis o conflictos.

Estos cometidos pueden llevarse a cabo para fines específicos y en forma autónoma en apoyo de las operaciones navales convencionales. Tendrán capacidad de reconocimientos hidrográficos, demoliciones submarinas y reconocimientos en profundidad en operaciones anfibias, en operaciones de interdicción (MIO), en cometidos antipirata, visita y registro no cooperativo y seguridad del tráfico energético.

Al igual que en el caso anterior todas estas acciones tácticas también de interés estratégico no requieren un flujo frecuente en las redes de mando y control sino que será suficiente con el empleo de canales de radiofrecuencia por lo que no serán objeto de la ciberguerra. La ya comentada inmersión de los niveles estratégicos y operacionales puede requerir el empleo de sistemas de mando y control susceptibles de ser atacados cibernéticamente

La ciberguerra en las operaciones antipiráticas

Actualmente la Armada participa en la Operación ATALANTA organizada por la Unión Europea en aguas de Somalia, cuyo mando reside en Northwood (Reino Unido), con mando de la fuerza naval rotatorio. La red de mando y control que se emplea está basada en internet con acceso restringido y cifrado, ante la falta de una red propia europea. Además la Armada ha participado puntualmente en la Operación ALLIED PROTECTOR de la OTAN, con prácticamente los mismos cometidos que la Operación ATALANTA.

La poca entidad de la infraestructura pirática hace poco probable el riesgo del empleo de ciberataques ni de contramedidas electrónicas, no obstante se sabe que los piratas conocen la situación de los barcos a través de los sistemas de información mundial AIS disponible en muchas páginas *web* en internet y con un buen virus pueden actuar contra la coordinación existente entre las múltiples unidades navales que operan en el pasillo de Seguridad (IRTC) del Golfo de Aden o en el Indico, ya que se realiza a través del cha entre las fuerzas navales, que incluyen a las no pertenecientes a la OTAN, *(chat Mercury)* y a los sistemas de mando y control CENTRIX o MCCIS para las fuerzas navales de la OTAN.

La ciberguerra en las operaciones navales antiterroristas

La OTAN está llevando a cabo la Operación ACTIVE ENDEVOUR (OAE) en el Mediterráneo, bajo el Control Operativo del Mando OTAN de Nápoles, en apoyo a la guerra que los Estados Unidos mantienen contra el terrorismo internacional. Las unidades que intervienen tienen por cometido «localizar, seguir y cuando se ordene, abordar buques de comportamiento sospechoso; y demostrar el compromiso de la OTAN para ayudar a la disuasión, defensa y protección contra el terrorismo, así como impedir sus acciones».

España, participa como un aliado más dentro de la OTAN en esta operación ininterrumpidamente desde octubre de 2001. Hasta enero de 2006 la Armada asignó inicialmente a esta operación fragatas de la 41.ª Escuadrilla que por razones económicas están siendo relevadas por buques BAM. Estas operaciones tienen una simplicidad táctica que no requiere las acciones de guerra electrónica y solo la de perturbación cibernética en el nivel estratégico. A pesar de esto pueden tener una presentación general *(Recognized Maritime Picture)* (RMP) completa y actualizada, cuya actualización requiere el uso de muchas redes y sistemas susceptibles de ser atacados. Durante los últimos años la Armada ha participado periódicamente en operaciones puntuales *(Surge Operations)*.

La ciberguerra en la acción del estado en la mar

La Acción del Estado en la Mar se traduce en las misiones permanentes de la Armada, bajo el mando del Almirante de la Flota y la conducción estratégica del JEMAD.

Los cometidos específicos de la Acción del Estado en la Mar son entre otros:

— Ejercer la vigilancia marítima.
— Apoyar al control de la inmigración ilegal.
— Colaborar dentro del plan nacional de la lucha contra la droga.
— Realizar campañas de vigilancia de pesca entre en los caladeros nacionales internacionales.

Aun cuando no está especificado, es obvio que esta Acción del Estado en la Mar comprende también las acciones antiterroristas y antipiratería. La naturaleza de los distintos cometidos hace poco probable la acción cibernéticas contra las redes de mando y control por parte de los oponentes potenciales. A pesar de ser operaciones de poca entidad son actualmente de prioridad para la Armada.

Correlación entre la guerra electrónica y la ciberguerra

De lo expuesto anteriormente se deduce claramente que en la guerra naval, la guerra electrónica cuyo ámbito de actuación es el espectro electromagnético y la guerra ciberespacial cuyo ámbito es el ciberespacio se complementan en cierto modo, tienen normalmente un mando común y puede establecerse que en el nivel estratégico y el nivel operacional predominan casi exclusivamente las acciones de ciberguerra mientras que en el nivel táctico predominan las acciones de guerra electrónica.

En el cuadro del Anexo I se exponen las posibilidades de acciones cibernéticas y de guerra electrónica electrónica.en las distintas operaciones navales en los niveles táctico, operacional y estratégico.

Conclusiones

En los conflictos armados del futuro siempre estará presenta la ciberguerra.

La dependencia global de las comunicaciones vía satélite en las operaciones navales aumenta la vulnerabilidad de estos sistemas frente a ataques físicos o cibernéticos.

Los ciberataques en una situación de guerra consistirán principalmente en ataques a las redes de mando y control, así como a la logística de la Fuerza Naval.

ANEXO I

POSIBILIDADES DE ACCIONES DE GUERRA ELECTRÓNICA (GE) Y DE CIBERGUERRA (CB) EN LOS NIVELES TÁCTICO, OPERACIONAL Y ESTRATÉGICO EN LAS OPERACIONES NAVALES

	Nivel Táctico		**Nivel Operacional**		**Nivel Estratégico**	
	GE	**CB**	**GE**	**CB**	**GE**	**CB**
Ataques a las redes de Mando y Control	SI	SI	SI	SI	SI	SI
Operaciones antisatélite	SI	SI	NO	SI	NO	SI
Ataques al tráfico marítimo	NO	NO	SI	SI	NO	SI
Defensa del tráfico marítimo	SI	SI	SI	SI	NO	SI
Dominio negativo del mar	NO	NO	SI	NO	NO	SI
Combate aeronaval	SI	NO	SI	SI	NO	SI
Operaciones anfibias	SI	SI	SI	SI	SI	SI
Bombardeo naval	NO	NO	NO	NO	NO	NO
Bombardeo aeronaval	SI	NO	SI	SI	NO	SI
Guerra naval especial	NO	NO	NO	NO	NO	NO
Guerra antiaérea	SI	NO	SI	SI	SI	NO
Lucha antisubmarina	SI	NO	SI	SI	SI	NO
Operaciones antipiréticas	NO	NO	NO	NO	NO	NO
Operaciones antiterroristas	NO	NO	NO	NO	NO	SI
Operaciones antidroga	NO	SI	NO	SI	NO	SI

ANEXO I (continuación)

POSIBILIDADES DE ACCIONES DE GUERRA ELECTRÓNICA (GE) Y DE CIBERGUERRA (CB) EN LOS NIVELES TÁCTICO, OPERACIONAL Y ESTRATÉGICO EN LAS OPERACIONES NAVALES

	Nivel Táctico		Nivel Operacional		Nivel Estratégico	
	GE	**CB**	**GE**	**CB**	**GE**	**CB**
Operaciones interdicción naval	NO	SI	NO	SI	NO	NO
Acción del Estado en la mar	NO	SI	NO	SI	NO	SI
Operaciones de apoyo conjuntas y combinadas	SI	SI	SI	SI	NO	SI

En general en las operaciones que se desarrollan dentro de un nivel táctico bajo un mando en la mar como puede ser un ataque antisubmarino en el que interviene aeronaves y escoltas, o una acción de guerra naval especial o de guerra de minas en la que no se emplean las redes de mando y control sino únicamente redes tácticas, serán objeto menor de la ciberguerra.

Por el contrario en el combate aeronaval, operaciones anfibias, y así como en operaciones de apoyo, conjuntas y combinadas de cierta entidad, estará presente la ciberguerra fundamentalmente en los ciberataques a las redes de mando y control y redes logísticas. En los últimos años se ha implantado el uso del chat, para intercambio de información táctica, por lo que su interferencia retrasaría la toma de decisiones.

Conclusión final

Las operaciones navales se verán afectadas por ataques cibernéticos a los sistemas de mando y control y de comunicaciones en los niveles estratégicos y operacionales, que requieren coordinación y planeamiento, por el contrario en el nivel táctico que se desarrolla en la mar y por consiguiente exterior a los Cuarteles Generales la incidencia será menor por supuesto más fácil de eliminar mediante el pase a los canales de radiocomunicaciones, a pesar de que por ellos pueden discurrir informaciones digitales susceptible de ataques cibernéticos.

BIBLIOGRAFÍA

Publicación número 149 del IEEE titulada Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio.
Distintas informaciones publicadas en internet, prensa y revistas.
Publicaciones no clasificadas del Ministerio de Defensa.
Información verbal directa de expertos de la Armada.