El Pentágono se asocia con la OTAN para crear un sistema de guerra ciberespacial global

RICK ROZOFF :: 15/10/2010

Los rumores sobre el virus informático Stuxnet para atacar una central nuclear civil de Irán son un ejemplo del desarrollo del CYBERCOM para funciones ofensivas

Un comunicado de la agencia Reuters afirma que USA tiene prevista este mes la activación de su Cibermando con capacidad operativa total y "preparado para enfrentarse a cualquier confrontación en el ciberespacio".

Con vistas a la implantación de un sistema planetario de guerra ciberespacial, el lanzamiento del primer mando militar múltiple del mundo -que incluye a las principales divisiones de las fuerzas del ejército estadounidense, es decir, la aviación, la infantería, los marines y la armada- está coordinado con una iniciativa complementaria de la Organización del Tratado del Atlántico Norte (OTAN) en Europa.

El pasado mes de septiembre, tras una década de existencia, el mando del Equipo Operativo Conjunto de la Red Global de Operaciones del Departamento de Defensa de USA fue disuelto oficialmente para pasar a integrarse en el nuevo Cibermando de USA (en inglés, CYBERCOM).

Al anunciar dicha transición, el servicio de prensa del Pentágono señaló que el equipo operativo había estado perfeccionando "la mejor manera de operar en el campo de batalla del ciberespacio" con "la doble misión de dirigir ciberoperaciones ofensivas y defensivas" que en 2003 se le habían asignado al Mando Estratégico Estadounidense (en inglés, STRATCOM), bajo cuyo control estará ahora también el CYBERCOM. Un año después, en 2004, el Equipo Operativo Conjunto de la Red Global de Operaciones fue reconfigurado para que "asumiese el cometido ofensivo" de las actividades de defensa y ataque aquí arriba mencionadas.

El general de las fuerzas aéreas Kevin Chilton, comandante del Mando Estratégico, presidió el 7 de septiembre la ceremonia de transición. El teniente general de infantería Carroll Pollett, director del Equipo Operativo de la Red Global de Operaciones desde 2008, pasará a ocuparse ahora únicamente de la Agencia de Sistemas de Información de la Defensa, en cuyas dependencias de Arlington (Virginia) tuvo lugar la ceremonia, si bien la Agencia de Sistemas de Información de la Defensa del Pentágono tiene previsto el traslado del CYBERCOM a Fort Meade (Maryland).

Éstas son algunas de las declaraciones del general Pollett durante la celebración:

"[La información] es un imperativo fundamental a la hora de proporcionar a nuestros soldados y a nuestros dirigentes nacionales los medios necesarios para la guerra.

"El ciberespacio se ha convertido en un nuevo campo de batalla.

“El ciberespacio ha adquirido una importancia similar a la que tienen tierra, mar y aire. Está claro que debemos defenderlo y volverlo operativo.” [1]

Su definición del ciberespacio como el “quinto espacio militar” forma parte de la retórica habitual de los funcionarios del Pentágono, quienes también lo denominan “quinto campo de batalla espacial”. [2] Cuando los jefes de los ejércitos más poderosos de la historia hablan de añadir una nueva dimensión a las tradicionales -infantería, aviación, marina de guerra, marines y operaciones con satélites y misiles-, no sólo pretenden ampliar los preparativos de la guerra a un nuevo ámbito, sino que éste en buena parte domina a los demás.

El 21 de mayo, dos semanas después de haberse convertido en el primer comandante del CYBERCOM y del lanzamiento de éste, el general Keith Alexander dijo que el Pentágono “depende de sus redes para el mando y el control, las comunicaciones, la inteligencia, las operaciones y la logística” y que la misión de su mando consiste en “impedir, detectar y defender a nuestra nación de las amenazas que surjan en el ciberespacio”.

El general, que asimismo es director de la Agencia de la Seguridad Nacional del Departamento de Defensa, añadió que es necesario definir “reglas claras de confrontación” para la ciberguerra, que “sirvan tanto para tiempos de paz como de guerra”. [3]

En sus primeras declaraciones públicas desde que asumió el mando, Alexander se refirió a sus funciones en un contexto de guerra.

Unos días antes, Kevin Chilton -director del Mando Estratégico- y William J. Lynn -secretario adjunto de Defensa- también habían declarado que la siguiente prioridad del CYBERCOM sería “desarrollar las reglas de confrontación de la ciberguerra”. [4]

En las raras ocasiones en que los medios de comunicación aluden a la creación por parte del Pentágono de un mando militar para ciberoperaciones sin precedente alguno, la palabra preferida con la que definen sus objetivos es “defensa”. En cambio, cuando los militares y el personal del Departamento de Defensa hablan entre sí, utilizan términos más directos: guerra, combate, tiempos de guerra, reglas de confrontación, campo de batalla, cibercampo de batalla.

En cuanto al uso que suele darle Washington a la palabra defensa, vale la pena recordar que cuando en 1949 USA cambió el nombre del Departamento de la Guerra por el de Departamento de Defensa fue sólo una cuestión de semántica, ya que un año después el Departamento de Defensa se enzarzó en la guerra de Corea.

El ejércitos estadounidense no ha defendido su territorio continental desde 1812, cuando USA provocó una guerra contra Gran Bretaña al invadir Canadá. Tampoco ha defendido territorios estadounidenses desde su mediocre actuación en Pearl Harbour en 1941 (Hawai pasó a ser un estado 18 años después) y en los combates posteriores en posesiones incluso más remotas: las Filipinas, Guam, la Isla de Wake y el atolón de Midway.

Durante la Primera Guerra Mundial en Europa, inicialmente en Francia y después en la Rusia soviética desde 1917 a 1919, Washington llamó a sus fuerzas armadas lo que eran en realidad: tropas expedicionarias.

En la guerra lanzada por USA y la OTAN contra Yugoslavia en 1999 y en la invasión de Iraq cuatro años después, el objetivo prioritario fue la destrucción de las redes eléctricas y las telecomunicaciones de ambos países. En el caso de Yugoslavia se utilizaron bombas de grafito para inutilizar el suministro eléctrico en la nación.

Los recientes rumores sobre el uso del virus informático Stuxnet para atacar la central nuclear civil de Irán en Bushehr son un ejemplo de cómo están desarrollando el CYBERCOM para funciones ofensivas en tiempos de guerra. En un mundo que depende cada vez más de la tecnología de la información, los ciberataques han sustituido a los misiles de crucero y a las bombas de grafito.

Además, con el proyecto Ataque Global Inmediato (*Prompt Global Strike*) del Pentágono [5] para lanzar misiles balísticos e hipersónicos intercontinentales de crucero a cualquier lugar del mundo en un intervalo de respuesta de 60 minutos -que en el futuro se reducirá hasta ser prácticamente instantáneo- y con el desarrollo de bombarderos supersilenciosos a gran distancia, capaces de evitar los radares y las defensas antiaéreas y de penetrar en el interior del país al que se dirigen, la ostentación del poder global para declarar una ciberguerra dejaría al mundo indefenso ante el chantaje económico y los ataques de los yanquis. Los equivalentes extranjeros del Mando del Pentágono, el control, las comunicaciones, los ordenadores, los servicios de inteligencia, la vigilancia y el sistema de reconocimiento (C4ISR) quedarían neutralizados.

No sólo Irán sería vulnerable, también Rusia y China

La edición de octubre-septiembre de *Foreign Affairs*, la revista del Consejo de Relaciones Exteriores, incluye un artículo de William Lynn, secretario adjunto de Defensa, titulado "Defending a New Domain: The Pentagon's Cyberstrategy" [Cómo defender un nuevo dominio: la ciberestrategia del Pentágono], en el que se afirma que "El Pentágono ha construido poderosas defensas por capas en torno a redes militares y ha inaugurado el nuevo Cibermando para integrar las operaciones de ciberdefensa en todos los ejércitos". [6] En dicho artículo se enumeran los cinco componentes de la estrategia del Pentágono para la ciberguerra:

> * El ciberespacio debe equipararse a la tierra, el mar y el aire en lo que respecta a la guerra;
>
> * Cualquier posición defensiva debe ir más allá del mero mantenimiento del ciberespacio "limpio de enemigos" para incluir operaciones sofisticadas y precisas que permitan una reacción inmediata;
>
> * Las ciberdefensas no deben limitarse al mundo informático, sino extenderse a las redes comerciales, controladas por el departamento de Seguridad Territorial [*Homeland Security*];
>
> * Con vistas a implantar un sistema eficaz de "alerta compartida" ante las amenazas se ha de posibilitar el establecimiento de ciberdefensas con aliados internacionales y

> * El Departamento de Defensa debe prestar su ayuda para mantener e incrementar el dominio tecnológico estadounidense y mejorar el proceso de adquisiciones para no quedarse rezagados ante la celeridad y la agilidad con que evoluciona la industria de la tecnología de la información (IT). [7]

Antes de la cumbre de la OTAN, que tendrá lugar en Portugal los días 19 y 20 de noviembre, el Departamento de Defensa tiene previsto publicar este otoño un documento de ciberestrategia, cuya aparición estará sincronizada con la puesta en funciones del CYBERCOM a pleno rendimiento.

El 28 de agosto, el Washington Post publicó un artículo titulado "El Pentágono considera los ataques preventivos como parte de la estrategia de ciberdefensa", que detallaba lo siguiente:

El Departamento de Defensa está utilizando un "enfoque agresivo" de las ciberoperaciones, en el que "se incluyen acciones preventivas tales como la destrucción de la red de ordenadores de un adversario en ultramar".

Según se deduce de los documentos del presupuesto destinado al Pentágono, éste está desarrollando toda una serie de potenciales armamentísticos que le permitirán "atacar y explotar los sistemas de información del enemigo mediante el engaño, la negación, la afectación, la perturbación y la destrucción de tales sistemas".

El despliegue del software y del hardware para tales planes es "el siguiente paso lógico de la ciberestrategia general que William J. Lynn III, secretario adjunto de Defensa, presentó la semana pasada", a saber, una "defensa activa". [8]

En agosto, el general Keith Alexander, director del CYBERCOM, intervino en la conferencia LandWarNet 2010 en Tampa (Florida), cuyo tema era "Cómo alcanzar el ciberdominio mundial de los mandos conjuntos". Reiteró en ella el argumento de que "el ciberespacio es ahora un escenario a considerar junto a los de tierra, mar y aire". [9] Con un tono mucho más inquietante, añadió: "Hemos de poseer potencialidad ofensiva para destruir en tiempo real a quien trate de atacarnos". [10]

Por "defensa activa" debe entenderse la capacidad de iniciar los ataques preventivos no sólo contra piratas informáticos individuales, sino también contra redes enteras de ordenadores nacionales.

El *Washington Post* citó las palabras de un alto funcionario no identificado del Pentágono, el cual sostuvo la misma posición: "Creo que tenemos claro que para asegurar la integridad de nuestras redes militares hemos de llegar hasta donde sea posible -una vez que sepamos de dónde viene la amenaza- para tratar de eliminar dicha amenaza allá donde podamos", incluso si "al atacar el ordenador de un atacante en otro país infringimos su soberanía". [11]

Un periodista del mismo diario advirtió que "el Pentágono tiene reglas vigentes de confrontación para la defensa de la red, tales como el derecho de defensa propia, pero puede que no sea tarea fácil establecer la línea que separa la defensa propia de la acción

ofensiva". [12]

Las reacciones a tales declaraciones y a otras parecidas no se han hecho esperar desde Rusia y China, aunque no de fuentes oficiales. El mes pasado, un sitio web ruso publicó un análisis bajo el título de "USA está preparado para tumbar la red de Internet en todo el mundo", en el que se decía que "a partir del 1 de octubre [la fecha original en que se iba a poner en marcha el CYBERCOM como mando independiente], miles de piratas informáticos militares y de espías estadounidenses iniciarán sus actividades de ciberguerra". [13]

El autor recordó a sus lectores que en abril de este año Leon Panetta, director de la CIA, dio a conocer el proyecto de esta agencia para los próximos cinco años, CIA 2015, cuyo "segundo pilar" incluye "la inversión en tecnología para que la agencia incremente su alcance analítico y operacional y sea más eficiente. El personal de la agencia debe poder operar con eficacia y seguridad en un entorno de información mundial que cambia con suma celeridad. El plan incrementa el potencial de la CIA para la recopilación técnica por parte de su personal y proporciona herramientas avanzadas de software…" [14]

En mayo, el mismo mes en el que el CYBERCOM inició sus actividades, la Casa Blanca aprobó la Evaluación de la política ciberespacial [*Cyberspace Policy Review*] de este año.

La fuente rusa señala también que "numerosas publicaciones en los medios estadounidenses dan a entender que la reforma de las Ciberfuerzas de Defensa Nacional, así como la introducción de la doctrina y de la estrategia de la ciberguerra están a punto de completarse. En cuanto a la ciberestrategia, podemos suponer que sigue la línea habitual del concepto de liderazgo mundial que tiene USA" [15]

Hace unas semanas, el Global Times publicó un artículo de un investigador del Centro de Investigación y Desarrollo del Consejo de Estado de China en el que se leía lo siguiente: "Controlar el mundo mediante el control de Internet ha sido la estrategia dominante de USA" y "la estrategia de seguridad de información nacional de ese país ha evolucionado desde la prevención hasta la del ataque preventivo".

"El objetivo final de USA consiste en [ser capaz de] abrir y cerrar partes de Internet a voluntad".

El artículo afirma que en 2004 USA eliminó el nombre del dominio "ly" e inhabilitó todos los servicios de Internet en Libia y que "en mayo de 2009 Microsoft anunció en su sitio web que cancelaría el servicio de *Windows Live Messenger* para Cuba, Siria, Irán, Sudán y Corea del Norte, de conformidad con la legislación de USA". [16]

El artículo del *Washington Post* citado más arriba añadía que el cierre de una página web saudí en 2006 "afectó colateral e involuntariamente a más de 300 servidores de Internet en Arabia Saudí, Alemania y Texas". [17]

El autor chino afirmó, además, que "USA monopoliza las cinco áreas esenciales de la infraestructura de Internet":

* Las grandes empresas de tecnología de la información (IT), que fabrican ordenadores de alto rendimiento, sistemas operativos, tecnologías de bases de datos, tecnologías de redes de la conmutación y bibliotecas de recursos de la información.

* En todo el mundo, alrededor del 92,3% de los ordenadores personales y el 80,4% de los superordenadores utilizan chips de Intel, mientras que el 91,8% de los ordenadores personales utilizan sistemas operativos de Microsoft y el 98% de la tecnología básica de los servidores está en manos de IBM y Hewlett-Packard.

* Por otro lado, el 89,7% del software de bases de datos lo controla Oracle y Microsoft y el 93,5% de la tecnología patentada esencial de las redes de conmutación está en manos de compañías estadounidenses.

* Una vez que ha controlado la infraestructura de Internet y los sistemas de hardware y software, USA pasa ahora a controlar el contenido de Internet.

El gobierno estadounidense ha adoptado el macrocontrol y se ha centrado en la financiación para utilizar de forma activa a las grandes empresas de tecnología de la información con la finalidad de crear una infraestructura global de Internet que pueda manipular. [18]

Además, mencionó que el senador Joseph Lieberman, presidente del comité senatorial de Seguridad Interna y Asuntos Gubernamentales, presentó recientemente a sus colegas del Senado una propuesta de ley de Protección del Ciberespacio como un valor nacional que permitiría que el presidente "pudiese ordenar a Google, Yahoo y a otros motores de búsqueda que suspendiesen los servicios de Internet.

"Y, además, otros proveedores de Internet en USA podrían pasar bajo el control del presidente cuando se produzca 'una situación de urgencia' en Internet.

"Si esto ocurre, el presidente de USA tendría oficialmente el poder de abrir o cerrar Internet." [19]

Los temores de los expertos chinos se confirmaron tras las declaraciones del general de la fuerza aérea Michael Hayden -director de la Agencia de Seguridad Nacional desde 1999 a 2005, subdirector de la Inteligencia Nacional desde 2005 a 2006 y director de la CIA de 2006 a 2009-, quien el mes pasado afirmó, con palabras que luego difundió Reuters, que "el ciberterrorismo supone una amenaza de tal calibre que el presidente de USA debería tener autoridad para cerrar Internet en caso de ataque". Exactamente dijo lo que sigue: "Mi opinión es que probablemente haya que legislar algún tipo de potestad para que el presidente tome medidas urgentes… cuando considere que deba tomarlas". [20]

El Pentágono y la Casa Blanca no pretenden actuar solos en la puesta a punto de una estructura internacional de guerra cibernética.

En mayo, poco después de la inauguración del CYBERCOM, los expertos estadounidenses en seguridad de la ciberguerra se reunieron durante un simposio de dos días sobre control

estratégico del ciberespacio celebrado en Omaha (Nebraska); entre ellos había "cibercomandantes de varios mandos estadounidenses de combate, de la OTAN, de Japón y de Reino Unido". [21]

En el mismo mes de mayo, el grupo de expertos de la OTAN, dirigido por la ex secretaria de Estado Madeleine Albright, publicó su informe OTAN 2010, en el cual se afirma que "la OTAN debería planificar la organización de un paquete de medidas de ciberdefensa que incluya elementos pasivos y activos". [22]

Tres semanas después, un artículo del *Sunday Times* de Londres reveló que "en un informe del grupo de Albright se afirma que un ciberataque contra la infraestructura esencial de un país de la OTAN podría equivaler a un ataque armado, lo cual justificaría una respuesta.

"'Un ataque a gran escala contra los sistemas de mando y control de la OTAN o contra las redes de suministro de energía podría posiblemente llevar a medidas de defensa colectiva, según especifica el artículo 5', afirmaron los expertos."

El artículo citaba además a un experto jurídico del Centro Cooperativo de Calidad de la Ciberdefensa de la OTAN, establecido en Estonia en 2008, el cual afirma que "debido a que el efecto de un ciberataque podría equivaler al de un ataque armado, no hay por qué volver a redactar los tratados que están en vigor". Se estaba refiriendo a los artículos 4 y 5 de la Alianza: el 4 sirvió para justificar el transporte de misiles antibalísticos Patriot a Turquía durante los preparativos de la guerra contra Iraq en 2004 y el 5 para justificar la participación de la OTAN en la guerra de Afganistán; ambos podrían invocarse y activarse en caso de ciberataque.

El artículo del *Sunday Times* añade:

"La OTAN se toma muy en serio las advertencias de los servicios de inteligencia de toda Europa de que los ciberataques lanzados desde Rusia y China son una amenaza cada vez mayor.

"La OTAN está sopesando el uso de la fuerza militar contra enemigos que lancen ciberataques contra los Estados miembros.

"Este cambio se debe a una serie de ataques rusos de piratería informática contra miembros de la OTAN y a las advertencias de los servicios de inteligencia sobre la creciente amenaza en proveniencia de China." [23]

El mes pasado se celebró en Tallín, la capital de Estonia, el 13º Taller de Ciberdefensa. En el discurso que pronunció ante los asistentes, el ministro de Defensa, Jaak Aaviksoo, afirmó: "Los potentes sistemas de ciberseguridad nacional de los aliados construirán bloques de ciberdefensa de la OTAN de una estructura contundente". [24]

En junio, en el centro de la OTAN en Estonia, país fronterizo con Rusia, se celebró una conferencia de cuatro días de duración bajo el título de "Cómo abordar los conflictos cibernéticos". Melissa Hathaway, directora de ciberseguridad del Consejo Nacional de Seguridad de USA, pronunció un discurso que estableció la tónica de la conferencia.

Gloria Craig, directora de Política Internacional de Seguridad del Ministerio de Defensa de Reino Unido, insistió en la urgencia de ampliar la capacidad de defensa frente a los ciberataques al afirmar que "en estos momentos, la OTAN no está preparada para un ciberataque global". [25]

También en junio, unos "cien participantes de las principales empresas globales de tecnología de la información, del sector bancario, de la comunidad de la inteligencia, de la OTAN, la UE y otras instituciones" asistieron en Rumania a la conferencia "La ciberdefensa en el contexto de la nueva estrategia de la OTAN", de la cual se hizo pública una declaración en la que se manifiesta que "la OTAN debe incrementar sus esfuerzos para responder al peligro de los ciberataques mediante la protección de sus propias comunicaciones y sistemas de mando, ayudando a los aliados a mejorar su capacidad para evitar ataques y recuperarse de ellos y a desarrollar un paquete de medidas de ciberdefensa…". [26]

En agosto, la OTAN reveló que ha creado una División de Amenazas Emergentes contra la Seguridad "con el fin de ocuparse del creciente espectro de amenazas y riesgos inhabituales", lo cual incluye las ciberoperaciones. "La División de Amenazas Emergentes contra la Seguridad unifica varias ramas del conocimiento ya existentes, pero hasta ahora separadas, en los cuarteles generales de la OTAN. La unificación de esta labor en una única División nos aportará mayor concentración y visibilidad." [27]

Este mes, la Agencia de Consulta, Mando y Control (NC3Q) organizó una conferencia en la República Checa y la Agencia de Adquisición de Tecnologías Avanzadas de la Alianza anunció que "la OTAN está evaluando la inversión de hasta 930 millones de euros (1,3 mil millones de dólares) en 2011 y 2012 en proyectos de varios años para enfrentarse a los retos esenciales de la seguridad, tales como la ciberdefensa, el apoyo a la OTAN en Afganistán y a la seguridad marítima". [28]

Un informe reciente divulgó que, en una entrevista con el *Suddeutsche Zeitung*, Anders Fogh Rasmussen, secretario general de la OTAN, afirmó que quería que la Alianza "ampliara la definición de los ataques que provocan la activación de la Alianza para que incluya los ciberataques" [30] como parte del nuevo concepto estratégico al que adherirse en su cumbre del mes próximo.

A mediados de septiembre William J. Lynn, segundo en la línea de mando del Pentágono, se encontraba en Bruselas para disertar ante el Consejo del Atlántico Norte, el principal órgano de gobierno de la OTAN, y de un comité de expertos en seguridad. [29]

Para movilizar a los militares aliados de Washington con vistas a la cumbre de noviembre, afirmó: "La OTAN tiene un escudo nuclear, está construyendo un escudo de defensa [con misiles] cada vez más poderoso, necesita un ciberescudo también… Las alertas compartidas de la guerra fría deben aplicarse a la ciberseguridad en el siglo XXI. Del mismo modo que nuestras defensas aéreas y nuestros misiles defensivos están vinculados, también debe estarlo nuestra ciberdefensa." [31]

Cuando Lynn llegó a Bruselas, los mandos de USA y Europa estaban terminando los quince días de maniobras conjuntas de 2010 -"los sistemas militares de comunicaciones e

información más importantes del mundo"- en el Centro conjunto de simulaciones multinacionales del área de entrenamiento de Grafenwoehr (Alemania). En total había 1400 participantes de 40 países: Alemania, Austria, Afganistán, Armenia, Albania, Azerbayán, Bulgaria, Bosnia, Canadá, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Francia, Finlandia, Georgia, Hungría, Italia, Iraq, Irlanda, Kazajistán, Lituania, Macedonia, Moldava, Montenegro, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumania, Serbia, Suecia, Turquía, Ucrania y USA.

Un portavoz de los mandos de USA y Europa declaró lo siguiente a propósito de dicho evento: "Ahora tenemos una 'operación' en el Pacífico, la Operación Pacífico. Otra en USA, que utiliza a Sudamérica y Canadá para interconectar su red de sistemas de comunicación. Estas maniobras que estamos realizando aquí, en Grafenwoehr, tienen ramificaciones por todo el mundo y los principales mandos están poniendo a punto su propia versión." [32]

Desde 2006, USA también ha dirigido las maniobras militares de la Operación África en ese continente, las "mayores maniobras de interoperabilidad en las comunicaciones de África" [33], primero bajo el mando conjunto de USA y Europa y, en fechas recientes, bajo el nuevo mando de USA y África. Las maniobras de la Operación África 2010 se realizaron en agosto en Ghana con la participación de 36 naciones africanas.

La palabra adecuada para describir la red militar que el Pentágono ha construido en los últimos años es "global" (Worldwide), como lo evidencian las naciones participantes bajo el mando estadounidense en la Operación Combinada de 2010 y en la Operación África 2010: 75 países, incluidos Afganistán e Iraq.

Las maniobras de entrenamiento multinacional dirigidas por USA y las simulaciones de guerra se celebran de forma habitual y a igual escala en toda Europa. En este momento se celebra el segundo año de las maniobras Combatientes Unidos (*Joint Warriors*) -la mayor simulación de guerra de Europa- a poca distancia de la costa y bajo el cielo de Escocia, con 30 países, 10.000 soldados, 30 barcos de guerra, tres submarinos y 21 unidades aéreas y helicópteros. Maniobras militares de tamaño comparable se realizaron durante el verano en la zona de Asia-Pacífico, cuando USA dirigió las simulaciones de guerra de las 14 naciones del Pacífico, las mayores maniobras marítimas multinacionales del mundo, con la participación de 22.000 soldados, 34 barcos, cinco submarinos y más de 100 aviones. [34]

Las maniobras de la Operación Conjunta, que tuvieron lugar del 3 al 15 de septiembre en Alemania, incluyeron por primera vez un componente de ciberdefensa. Participantes de 26 países y dos organizaciones, la OTAN, y el Centro Cooperativo de Calidad de la Ciberdefensa, con sede en Estonia, participaron en la planificación de las ciberoperaciones en el Centro Conjunto de Simulaciones Multinacionales, en Grafenwoehr.

Desde el fin de la guerra fría, y especialmente en la pasada década, el Pentágono ha expandido sus actividades por todo el mundo: bombardeos, guerras, invasiones, maniobras multinacionales y simulaciones de guerra, construcción de bases y golpes militares, despliegue de misiles y escudos, programas de entrenamiento y establecimiento de redes de transporte militar.

Gracias a la expansión hacia el Este, la OTAN es hoy día el único bloque militar del mundo

y, con la implantación hace dos años del mando de USA y África, USA ha alcanzado el control militar de dos continentes enteros.

Tiene aliados en prácticamente todas las naciones de Europa, África, Oriente Próximo y Asia y ha ubicado nuevas bases y otras instalaciones militares en el este de Europa, África, Oriente Próximo, Asia, el Pacífico sur, Sudamérica: Kosovo, Bulgaria, Rumania, Hungría, Polonia, Djibouti, Seychelles, Iraq, Israel, Kuwait, Afganistán, Kirguistán, Australia y Colombia.

Washington ha incrementado su presencia militar en varios continentes para alcanzar sus objetivos geopolíticos del siglo XXI. Con el fin de controlar el acceso y el transporte de los hidrocarburos, el Pentágono ha expandido su presencia en el Golfo Pérsico, en el Golfo de Guinea, en el Mar Negro y en las naciones cercanas al Mar Caspio. Con la reactivación en 2008 de su Cuarta Flota, USA se ha posicionado para dominar el Caribe, incluidos Colombia, Venezuela y Panamá en su orilla sur.

USA está preparando un sistema global para interceptar misiles mediante el despliegue -directamente y con sus aliados- de los sistemas *Patriot Advanced Capability-3, Standard Missile-3, Terminal High Altitude Area Defense* y otros componentes de misiles-escudo en Polonia, Israel, Bahrain, Kuwait, Qatar, Emiratos Árabes Unidos, Japón, Corea del Sur y Australia, con el Mar Negro, el Mar Mediterráneo, el Mar Báltico y el Cáucaso Sur como futuros lugares previstos.

El Pentágono no va a descansar hasta que logre dominar por completo el mundo y lo que hay por encima del mundo. A su superioridad militar en los ámbitos de tierra, mar y aire ahora está añadiendo el control del quinto campo de batalla: el ciberespacio.

Notas

[1] American Forces Press Service, September 8, 2010 [2] U.S. Cyber Command: Waging War In World's Fifth Battlespace Stop NATO, 26 de mayo de 2010 http://rickrozoff.wordpress.com/2010/05/26/u-s-cyber-command-waging-war-in-worlds-fifth-battlespace

[3] Agence France-Presse, 4 de junio de 2010 [4] Stars and Stripes, 2 de junio de 2010 [5] Prompt Global Strike: World Military Superiority Without Nuclear Weapons Stop NATO, 10 de abril de 2010. http://rickrozoff.wordpress.com/2010/04/10/prompt-global-strike-world-military-superiority-without-nuclear-weapons

[6] William J. Lynn III, Defending a New Domain:The Pentagon's Cyberstrategy Foreign Affairs, Septiembre/Octubre de 2010 http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[7] U.S. Department of Defense, 25 de agosto de 2010. http://www.defense.gov/news/newsarticle.aspx?id=60600

[8] Ellen Nakashima, Pentagon considers preemptive strikes as part of cyber-defense strategy. Washington Post, 28 de agosto de 2010 http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html

[9] United States Army, 4 de agosto de 2010 [10] Army News Service, 3 de agosto de 2010 [11] Washington Post, 28 de agosto de 2010 [12] Ibid [13] Leonid Savin, US gets ready to knock the world offline Strategic Culture Foundation, 6 de septiembre de 2010 http://www.strategic-culture.org/news/2010/09/06/us-gets-ready-to-knock-the-world-offline.html

[14] Central Intelligence Agency, 26 de abril de 2010 [15] Strategic Culture Foundation, 6 de septiembre de 2010 [16] Chen Baoguo, US controls threaten Internet freedom Global Times, 24 de agosto de 2010 http://opinion.globaltimes.cn/commentary/2010-08/566394.html

[17] Washington Post, 28 de agosto de 2010 [18] Global Times, 24 de agosto de 2010 [19] Ibid [20] Reuters, 26 de septiembre de 2010 [21] Stars and Stripes, 2 de junio de 2010 [22] North Atlantic Treaty Organization http://www.nato.int/strategic-concept/expertsreport.pdf

[23] Sunday Times, 6 de junio de 2010 [24] North Atlantic Treaty Organization, 3 de junio de 2010 [25] Agence France-Presse, 9 de junio de 2010 [26] North Atlantic Treaty Organization, 7 de junio de 2010 [27] Defence Professionals (Germany), 4 de agosto de 2010 [28] Reuters, 7 de octubre de 2010 [29] NATO Provides Pentagon Nuclear, Missile And Cyber Shields Over Europe. Stop NATO, 22 de septiembre de 2010 http://rickrozoff.wordpress.com/2010/09/22/2463

[30] The H Security, 1 de octubre de 2010 [31] Agence France-Presse, 15 de septiembre de 2010 [32] United States European Command, 8 de septiembre de 2010 [33] U.S. Africa Command, 12 de enero de 2010 [34] Asia: Pentagon Revives And Expands Cold War Military Blocs. Stop NATO, 14 de septiembre de 2010 http://rickrozoff.wordpress.com/2010/09/15/asia-pentagon-revives-and-expands-cold-war-military-blocs

rickrozoff.wordpress.com. Traducido por Manuel Talens (Tlaxcala) y Paloma Valverde (IraqSolidaridad)

---

https://www.lahaine.org/mundo.php/el-pentagono-se-asocia-con-la-otan-para