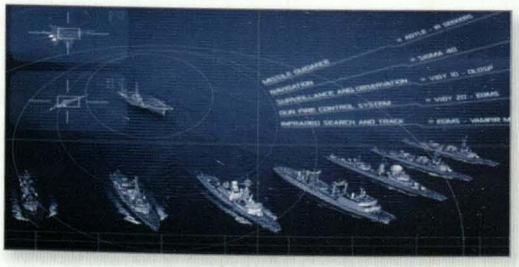
Empleo de las Operaciones de Información como armas ofensivas



Capitán de Navío
ALBERTO ABRAHAM ARNILLAS BRENDER



Introducción

La evolución tecnológica realizada en los últimas décadas, ha provocado una revolución en los asuntos militares, empleándose en el plano táctico nuevas armas,que han desplazado los antiguos conceptos de masa y fuerza, existiendo actualmente aviones no tripulados (UAV), misiles de largo alcance con altas probabilidades de impacto, sistemas de vigilancia tridimensionales, buques y aviones invisibles al radar enemigo, equipos de posicionamiento (GPS) para Fuerzas sumamente móviles, flexibles e interoperables, debiendo ser apoyadas por robustos sistemas de comunicaciones, comando, control y cómputo, que permitan tomas de decisiones en tiempo real.

Las Operaciones de Información son un concepto relativamente nuevo, que basa la guerra moderna en un elemento que ha estado presente en los conflictos a lo largo de la historia de la humanidad: *la información*, la cual se ha convertido en un recurso estratégico vital para la Seguridad Nacional de un país en todos los ámbitos de acción, requiriéndose para su empleo una adecuada explotación, planificación, coordinación y sincronización, debiéndose asignar estas acciones al Comando Conjunto de las Fuerzas Armadas (COCOFA), como la Institución del más alto nivel estratégico militar.



Las Operaciones de Información pueden definirse como el uso integrado de las capacidades centrales de la guerra electrónica, operaciones de redes de cómputo, operaciones sicológicas, engaño militar y operaciones de seguridad; en conjunto con las capacidades específicas de apoyo y relacionadas para influenciar, interrumpir, degradar o usurpar la toma de decisiones adversas humanas y automatizadas, protegiendo al mismo tiempo las nuestras.

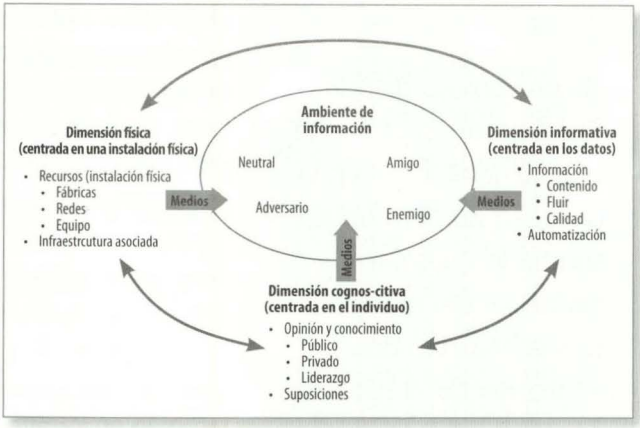
Respecto al entorno de la información, existe una *dimensión física*, compuesta por los sistemas de comunicaciones, comando, control y cómputo, así como la infraestructura de apoyo, que permiten a las personas y organizaciones conducir operaciones a través de los dominios del aire, mar, tierra y el espacio. Existe, así mismo, una *dimensión informacional*, consistente en el contenido y flujo de la información, la cual es colectada, analizada, almacenada, diseminada y mostrada; por lo tanto, esta dimensión debe también ser protegida.

Finalmente, existe una *dimensión cognitiva*, que es la más importante, debido a que las decisiones se tomarán en base a cómo el Comandante percibe la realidad, influenciando también el entrenamiento, la moral y los valores que pueden significar perder una campaña o un conflicto en el subconsciente.

La guerra informática es el subconjunto de Operaciones de Información de carácter ofensivo, que puede definirse como las acciones que se realizan a fin de alterar la información y los sistemas de información del adversario, mientras se protegen los propios, con el propósito de obtener la superioridad de la información, lográndose en ese escenario, desarrollar acciones tendientes a recolectar, controlar, explotar y defender la información, sin oposición efectiva del adversario, quien se encontrará confundido al habérsele negado el acceso a la información útil, y retrasado respecto a la toma de decisiones nuestras.

Es oportuno señalar que en las Operaciones de Información no debe haber diferencias entre el tiempo de paz y guerra, debido a que en cualquier

momento una computadora componente de un sistema de comando y control, podría activar un virus programado como un arma digital elaborada profesionalmente a partir de una tarea de Inteligencia, para producir un daño específicamente dirigido, debiéndose romper los paradigmas existentes para desarrollar sistemas informáticos con una arquitectura informática que esté preparada para ser atacada, lanzando contramedidas como recursos de defensa y activando alarmas que permitan informar del citado ataque.



Incluso ya estamos viviendo una guerra informática o ciberguerra, con organizaciones como Anonymous, que ha emprendido una serie de ataques dirigidos a las organizaciones contrarias a Wikileaks, la cual filtró en el año 2010 una serie de documentos de carácter diplomático de Estados Unidos; además, existen otros actores ocultos siempre en el anonimato y de intereses diversos, como son los *ciberterroristas,* piratas informáticos, *hackers*, espías, entre otros, que operan en las redes informáticas para obtener información sensible con bombas lógicas y programas husmeadores.

En el *ciberataque* más exitoso alcanzado hasta la fecha, se cree que Estados Unidos, conjuntamente con Israel, infiltró en los sistemas de control de la central nuclear situada en Bushehr, en Irán, un virus con una potencia sin precedentes, denominado *Stuxnet*, el cual permanece dormido hasta que recibe una orden proveniente de su creador, y que en el caso de Irán, tenía el objetivo de acceder e inutilizar los sistemas de control (SCADA) de la central nuclear de Bushehr y de la planta de enriquecimiento de uranio de Natanz, dentro de la "Operación Myrtus".

Otro paradigma que es oportuno romper, es pensar que la guerra de la información es la guerra del futuro; por el contrario, consideramos que es la guerra de hoy, como ya lo ha interiorizado Estados Unidos, que ha anunciado a la comunidad internacional que responderá a este tipo de ataques, incluso a través de la fuerza militar tradicional, incrementando de 900 a 4.000 los efectivos del área de Operaciones de Información del Departamento de Defensa y

"El prestigioso diario *The Economist*, advierte una vulnerabilidad en la cantidad de fibra óptica submarina desplazada alrededor del mundo, con la finalidad de interconectar al planeta; en sí, los cables pueden ser saboteados en cualquier parte del mundo".

elevando su presupuesto a 23.000 millones de dólares, lo cual demuestra la importancia de contar con expertos en medios informáticos, quienes en el futuro deberán reemplazar a los soldados convencionales.

Además, el prestigioso diario *The Economist*, advierte una vulnerabilidad en la cantidad de fibra óptica submarina desplazada alrededor del mundo, con la finalidad de interconectar al planeta; en sí, los cables pueden ser saboteados en cualquier parte del mundo y también en los alrededores de Nueva York, el Mar Rojo o el estrecho de Luzón, en las islas Filipinas; lugares donde se encuentran los servidores de dominio potencialmente más sensibles, que manejan la mayor parte del tráfico de internet.

A continuación se describirán las capacidades en que se basan las Operaciones de Información ofensivas, como la guerra sicológica, decepción militar, ataque electrónico, operaciones de redes de cómputo y, complementariamente, operaciones de seguridad, además de otras relacionadas que permitirán influenciar, interrumpir, dañar, usurpar o negar la toma de decisiones adversarias, tanto humanas como automatizadas, mientras que se protege la propia superioridad de la información.

Operaciones Sicológicas

Se definen como aquellas operaciones planeadas en tiempos de paz, crisis y guerras, dirigidas a audiencias amigas, neutrales y de interés, para influir en actitudes y conductas que ayuden a la consolidación de los objetivos políticos, estratégicos y militares, con la finalidad de debilitar la voluntad del adversario, reforzar la moral de las Fuerzas propias y ganar el apoyo de los neutrales, debiendo tener en cuenta que la capacidad de contar con una óptima relación con los medios de comunicación (asuntos públicos) es esencial para conseguir la máxima eficacia, enfocándonos en las operaciones del tipo "guerra sicológica", por ser de carácter ofensivo.

Se puede emplear una amplia gama de medios de comunicación como la radio, los altavoces, la televisión y el cine; pero en una campaña de largo plazo, estos son

medios costosos y que suponen una preparación y planificación elaboradas antes de ser llevados a cabo; por lo que en el corto plazo se recomienda la utilización de volantes y *posters*, los cuales tienen como ventaja su bajo costo y que, por ser un mensaje impreso, persiste su finalidad hasta que sea destruido, pasando de mano en mano y entregándose a un objetivo específico, evitándose que llegue a una audiencia imprevista o incluso no deseada.

> "Se puede emplear una amplia gama de medios de comunicación como la radio, los altavoces, la televisión y el cine; pero en una campaña de largo plazo, estos son medios caros y que suponen una preparación y planificación elaboradas antes de ser levados a cabo".

Como inconvenientes, los volantes carecen de la inmediatez de las transmisiones tanto de radio como de televisión, pudiendo su distribución verse afectada por la situación táctica, dificultándose la transmisión de ideas complejas; para lo cual es muy importante conocer la forma de pensar, los valores y los factores subyacentes que se encuentran de forma oculta en el accionar de los grupos de interés. Estas ventajas y desventajas podrían mencionarse en tiempo pasado, debido a que actualmente los folletos podrán ser enviados como correos *spam* a todos aquellos que se desee contactar, por lo cual las redes de comunicaciones facilitan las operaciones sicológicas.

En la Guerra del Golfo, las operaciones sicológicas realizadas por la coalición jugaron un importante papel para obtener la victoria, para fortalecer la moral de los combatientes y minar la del enemigo, empleándose coberturas en radio, televisión, altavoces y especialmente por los volantes que se arrojaron desde el aire y que sirvieron para que el 44% del Ejército iraquí deserte, 17.000 hombres pasaran al bando enemigo y cerca de 90.000 se rindiesen.

Operaciones de Decepción

Son acciones que se ejecutan para confundir y engañar al adversario a fin de que el enemigo tome decisiones erróneas en relación a sus capacidades militares, intenciones y ejecución de operaciones, logrando que dichas equivocaciones repercutan en un mayor desgaste de sus Fuerzas. Diversos casos de engaño se han dado a lo largo de la historia, siendo uno de los primeros en realizarlas Aníbal Barca, comandante cartaginés que siempre realizaba estratagemas con la finalidad de obtener la ventaja táctica.



El éxito del desembarco de Normandía suponía un punto de inflexión en la Segunda Guerra Mundial; sin embargo, el planeamiento y ejecución de una operación de tal envergadura, tenía que estar acompañada de una serie de maniobras deceptivas, a fin de distraer la atención del alto mando alemán y a la vez desconcentrar sus Fuerzas, que ante el inminente avance aliado, reforzó las defensas de las playas de toda la zona norte francesa.

La operación de engaño consistió en crear una división fantasma del Ejército, conformada por actores, especialistas en efectos especiales, guionistas, expertos en comunicaciones, apoyados por tropas reales que ensayaban en las costas de Calais un desembarco, contando con tanques, campamentos y vehículos falsos, que eran inflados con compresoras de aire, designándose al General Patton como Comandante del "Primer Grupo del Ejército Estadounidense" (FUSAG), como fue denominado.

Además, en la mañana de la ya famosa operación, se lanzaron muñecos paracaidistas y una división de aviones arrojaba papeles color plata que actuaron como señuelos, activándose un comando encargado de dirigir órdenes falsas, teniendo tanto éxito esta maniobra, que luego del desembarco en Normandía, aún los alemanes pensaban que se realizaría otro en el paso de Calais.

Operaciones de Redes de Cómputo

Las Operaciones de Redes de Cómputo (CNO) inician sus operaciones ante el incremento del uso de los sistemas de información y terminales informáticos en red por organizaciones civiles y militares, utilizadas para atacar, engañar, degradar, interrumpir, denegar, explotar la infraestructura del enemigo y defender la propia.

Las Operaciones de Redes son aplicables en todos los niveles de Comando; sin embargo, conducidas en apoyo de un comando específico pueden afectar a los escalones subordinados. Por ello, las operaciones de redes deben ser planeadas de manera centralizada, en el más alto nivel, por la autoridad competente y capacitada. Se subdividen en:

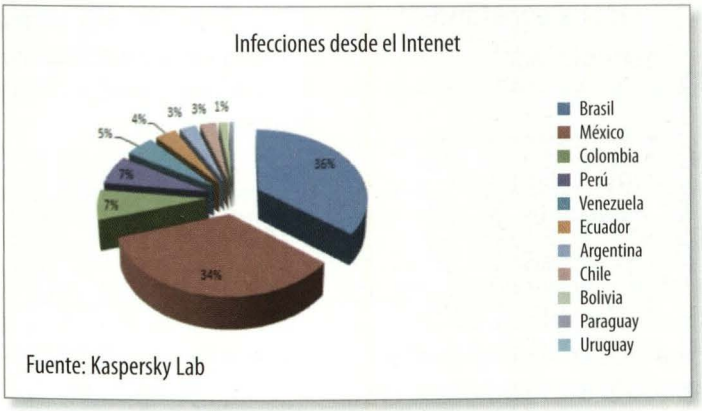
- Ataque a Redes de Computadoras (*Computer Network Attack*,CNA)
- Defensa de Redes de Computadoras (*Computer Network Defense*, CND)
- Explotación de Redes de Computadoras (*Computer Network Explotation*, CNE)

Ataque a Redes de Computadoras

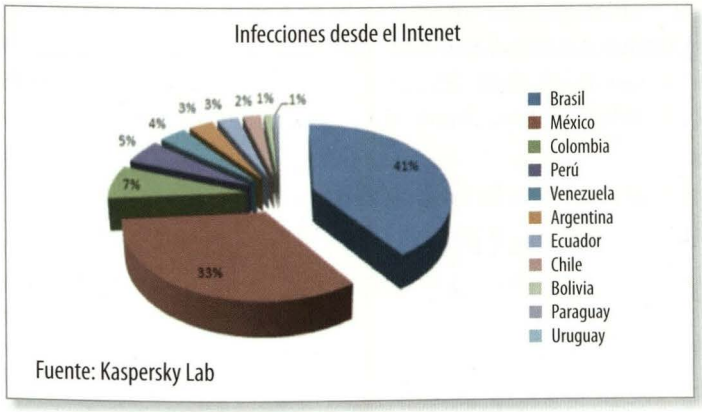
Son las medidas que se adoptan buscando interrumpir, negar, degradar, desorganizar o destruir información en las redes de computadoras de los sistemas de comunicaciones, comando, control y cómputo del adversario. Sus acciones comprenden la denegación de servicio o de *hacking*, para lo cual se pueden utilizar *malware*, virus, troyanos, *spam*, entre otros modos de ataques informáticos, debiendo el responsable a cargo realizar la planificacióny coordinar estrechamente con la sección de Inteligencia.

En el informe de la empresa de antivirus Kaspersky del año 2012, se señala el porcentaje de infecciones recibidas en las computadoras de los países de Sudamérica, dentro de las redes informáticas y fuera de ellas, por contagios por medios externos, como los conocidos USB. En dicho informe se observa que el Perú, en ambos casos, tiene un 7% del total, siendo Brasil el país con el mayor porcentaje de virus, con un 41% y 36%, respectivamente, según los siguientes cuadros:

Por su parte, el presidente Barack Obama ha dispuesto reforzar la lucha contra los *ciberataques*, después de conocerse los ataques atribuidos a China a empresas como Facebook, Apple o Twitter, con el intento de espiar y conocer la información que se maneja dentro de las redes de esas compañías; sin embargo, la Unión Europea acusa a Estados Unidos de haber



Fuente: Kaspersky Lab



Fuente: Kaspersky Lab

"Durante la Segunda Guerra Mundial, la perturbación de las transmisiones de las estaciones de radiodifusión adversarias, orientada a impedir la difusión de los programas de propaganda enemiga, constituyó una práctica constante y generalizada".

espiado sus redes, en un hecho sin precedentes, conociéndose además –como se dijo anteriormente– que este país, en conjunto con Israel, atacó el programa nuclear iraní, a través del famoso virus Stuxnet, lo que demuestra a la luz de estos acontecimientos, que la *ciberguerra,* es una guerra actual y no del futuro.

Operaciones de Guerra Electrónica

Desde el surgimiento del radar en plena Segunda Guerra Mundial, la lucha por tener la mayor tecnología para contar con el control del espacio electromagnético, así como negarlo al enemigo, ha sido una constante, desarrollándose una amplia gama de sistemas militares vinculados para el ataque (*hardkill*) y otros relacionados con la defensa electrónica (*softkill*).

Durante la Segunda Guerra Mundial, la perturbación de las transmisiones de las estaciones de radiodifusión adversarias, orientada a impedir la difusión de los programas de propaganda enemiga, constituyó una práctica constante y generalizada; muchas estaciones estaban interferidas u ocultas bajo ruidos metálicos, sonidos fuertes u otros tipos de ruidos, aplicándose también, aunque en menor medida, al campo de las comunicaciones militares para impedir al enemigo el uso eficaz de su equipo de radio.

Sin embargo, los ataques electrónicos en la actual era digital y de redes, pueden desarrollarse por medio de virus informáticos, como ya se ha venido comentando, que afectarían a las computadoras principales de los sistemas de comunicaciones, comando y control enemigos.

Operaciones de Seguridad

Son parte del proceso de identificación de la información crítica y clasificada, así como del análisis subsiguiente de las acciones propias y otras actividades que permiten identificar la información que podría ser necesaria para que el adversario tenga suficiente conocimiento de nuestros movimientos, capacidades

e intenciones, con el fin de negarle esta información. Están asociadas con las Operaciones de Información Defensivas, pero que deben estar totalmente relacionadas con las Ofensivas, a fin de obtener una superioridad de la información en el plano estratégico, operacional y táctico.

Operaciones de Apoyo

Las capacidades descritas anteriormente no se podrían concretar, si es que no se toman en cuenta ciertas capacidades de Apoyo que permitirían consolidar los objetivos impuestos al inicio de una crisis o una campaña operacional, describiéndose a continuación las más importantes:

"Toda Operación de Información Ofensiva debe estar acompañada de una adecuada comunicación de los sucesos, lo cual transmite confianza a nuestras tropas y población, debiéndose contar para ello con excelentes relaciones con los medios de comunicación".

Ataque Físico

Es el punto culminante de toda operación militar y donde se debe atacar los centros de gravedad o puntos vulnerables del enemigo que afecten su capacidad de lucha. Dadas sus múltiples posibilidades a través de las capacidades ya conocidas, el grupo de trabajo ha considerado no extenderse en este punto, en beneficio de ahondar en las Operaciones de Información Ofensivas.

Cabe resaltar que una interesante vulnerabilidad en la guerra informática, la representa el ataque a los cables de internet que se encuentran sumergidos en el mar y que podrían afectar a los centros de toma de decisiones rivales, como un posible curso de acción propio.

Asuntos Públicos

Toda Operación de Información Ofensiva debe estar acompañada de una adecuada comunicación de los sucesos, lo cual transmite confianza a nuestras tropas y población, debiéndose contar para ello con excelentes relaciones con los medios de comunicación, con la finalidad de que sirvan de enlace entre nosotros, como integrantes de las Fuerzas Armadas, y el público objetivo, tanto interno como externo, tratando que informen los hechos sucedidos de acuerdo a cómo nosotros queremos que se den a conocer los acontecimientos.

Además sirven para contradecir los efectos de la propaganda enemiga, revelando información oportuna y confiable, debiéndose materializar en medidas activas, como ruedas de prensa, comunicados, artículos y puntos de discusión específicos.

Asuntos Civiles

Acciones militares para establecer, mantener, influenciar o explotar relaciones con organizaciones, autoridades y población civil, y que deben de desarrollarse en forma permanente como una tarea implícita a todo miembro de las Fuerzas Armadas, y que durante una Operación Ofensiva deben de servir para evitar la interferencia civil en el desarrollo de las operaciones militares.

"Las Operaciones de Información tienen un carácter estratégico y, por lo tanto, deben ser asumidas en el ámbito militar del Comando Conjunto de las Fuerzas Armadas (COCOFA), que deberá desarrollar las acciones de planeamiento, coordinación y ejecución".

Conclusiones

a. La era de la información digital obliga a los líderes de las organizaciones a estar un paso adelante en los acontecimientos que puedan presentarse en el futuro, ya que el ciclo de la toma de decisiones es cada vez más veloz, con la finalidad de minimizar los impactos negativos provenientes del entorno, debiendo efectuar una Inteligencia operativa permanentemente, que sirva para observar y analizar los movimientos de los competidores, así como de los enemigos en el plano militar.

b. Las Operaciones de Información tienen como principio coordinar y sincronizar las cinco capacidades básicas para lograr los objetivos planteados o prevenir que el adversário logre alcanzar los suyos, empleándose para ello, la decepción militar, la guerra sicológica (como parte de las operaciones sicológicas), el ataque electrónico (como parte ofensiva de la guerra electrónica), las operaciones de seguridad y finalmente las operaciones de las redes de cómputo, derivadas del desarrollo de la tecnología en la actual era de la información digital.

c. No es posible concebir en la actualidad Operaciones de Información Ofensivas sin que se tomen en consideración las Defensivas, con la finalidad de estar preparados para repeler con éxito un ataque proveniente de fuerzas enemigas, debiéndose entender a este nuevo concepto como un todo y nunca de manera separada.

d. Las Operaciones de Información tienen un carácter estratégico y, por lo tanto, deben ser asumidas en el ámbito militar del Comando Conjunto de las Fuerzas Armadas (COCOFA), que deberá desarrollar las acciones de planeamiento, coordinación y ejecución, con la finalidad de apoyar el esfuerzo de lucha y el objetivo final trazado.

"En el plano militar, el avance de la tecnología ha desencadenado una revolución de los asuntos militares, que han ayudado a que los tomadores de decisiones cuenten con una mayor información; sin embargo, activando ciertos virus se podrá generar operaciones de decepción y ataques electrónicos".

e. Para la planificación y conducción de Operaciones de Información, se debe romper viejos paradigmas para concebir que no se tiene que pasar a una situación de conflicto para recibir un ataque por vías de las redes informáticas, ni tampoco pensar que este escenario se daría en un futuro, puesto que en internet se han enfocado los intereses de múltiples actores (estados, *ciberterroristas, piratas, hackers,* crimen organizado), que permanentemente están buscando vulnerar las plataformas, a fin de efectuar operaciones de espionaje, sabotaje, robos, a través de virus maliciosos que han sido programados con anterioridad.

f. En el plano militar, el avance de la tecnología ha desencadenado una revolución de los asuntos militares, que han ayudado a que los tomadores de decisiones cuenten con una mayor información; sin embargo, activando ciertos virus se podrá generar operaciones de decepción y ataques electrónicos a los sistemas de comunicaciones, comando, control y cómputo propios, debiéndose tener en consideración que es vital tener la superioridad de la información, a fin de asegurar los objetivos militares y, por ende, los objetivos estratégicos inicialmente concebidos en un teatro de guerra.

Bibliografía

- Apuntes de Clase Alberto Arnillas (2007): "Marketing Internacional". Profesor Rolando Arellano. CENTRUM-Católica. Lima-Perú.
- Apuntes de Clase (2013): "Empleo Estratégico de las Operaciones de Información". Docente: Capitán de Navío (r) Luis Martínez Enrique. La Punta-Perú.
- Bachoir Vidaurre, Víctor;Leclere Pineda,Juan Carlos;Posito Luján,Marco; Reyes Lazo,Carlos Enrique; Valenzuela Gallegos, Richard (2010): "Las Operaciones de Información: Un recurso estratégico vital para la Seguridad Nacional". Revista de la Escuela Superior de Guerra. Lima-Perú.
- De Arancelis Mario (1983): *Historia de la Guerra Electrónica. Desde la Batalla de Tsushima, al Líbano y las Malvinas*. Madrid: Editorial San Martín.
- Doctrina de Operaciones de Información de Estados Unidos (2012).
- Ministerio de Defensa de España (2011).*Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio.* Madrid: Imprenta del Ministerio de Defensa de España.
- Ministerio de Defensa del Perú (1998). *Conocimientos Básicos para las Operaciones Psicólogas*. Lima.
- Olsen,Soren (2012): "El Boxeo con un contrincante imaginario: La Guerra Cibernética y el ataque económico estratégico".*MilitaryReview.*
- http//www.centronaval.org.ar/boletin/BCN817/817lopez. "La Guerra Informática".
- http//www.wikipedia.org. "Guerra Electrónica"
- http//www.intelpage.info/web/exterior/textos/opsic. (2013): "Notas sobre el empleo de las Operaciones Sicológicas".
- Wegener, Henning (2001). "La Guerra Cybernética". Revista de Política Exterior. Alemania.

