INTELIGENCIA EN LA GUERRA DE INFORMACION

Taeda *

Introducción.

Guerra de Información (GI) es un concepto relativamente nuevo que basa la guerra moderna curiosamente en un elemento que desde la antigüedad ha estado presente en las guerras desarrolladas por el hombre: la información. Esta última ha sido desde siempre materia prima en todo proceso de Inteligencia y todas sus actividades están relacionadas con ella.

De lo anterior se desprende que en la GI la Inteligencia tendrá un papel aún más decisivo del que tiene hoy. Para enfrentar los nuevos desafíos y amenazas que la GI presenta, la Inteligencia deberá adecuar algunas de sus actividades y determinar el surgimiento de otras nuevas para cumplir a cabalidad con su papel de apoyo a la toma de decisiones de los mandos o autoridades en todos los niveles de conducción, especialmente para ejecutar la GI.

El objetivo del autor es dar a conocer un punto de vista personal sobre el papel del Sistema de Inteligencia Naval y las orientaciones que debieran tener sus actividades para adecuarse a la GI y aprovechar sus nuevas capacidades asociadas en beneficio de la Armada.

Antecedentes.

En realidad la GI no parece ser algo muy novedoso, pues la mayoría de los elementos que la componen se han aplicado en la historia al arte de la Guerra: obtención de información de las capacidades e intenciones del enemigo, negación de información de nuestras propias capacidades e intenciones, desinformación, engaño, impedir el enlace entre los mandos enemigos y sus fuerzas, operaciones psicológicas, y un sinnúmero de actividades directamente relacionadas con la información.

¿Qué es lo nuevo entonces? Primero, el avance tecnológico de hoy en día ha permitido que los procesos basados en la información alcancen niveles de eficiencia nunca vistos. Segundo, cada vez es mayor la dependencia de los sistemas militares en la tecnología de manejo y traspaso de información. Tercero, esta dependencia ha permitido identificar nuevas vulnerabilidades y debilidades lo que ha propiciado el desarrollo de nuevas tecnologías y procedimientos para explotarlas y, en consecuencia, sus contramedidas. Y cuarto, el interés de los conductores políticos de los Estados de desarrollar guerras más cortas, más baratas y con menos pérdidas de vidas humanas.

Como consecuencia de lo anterior en la actualidad, como nunca antes, la información ha pasado a tener un papel protagónico en el desarrollo de la guerra transformándose a la vez en "recurso, arma y blanco"[1] pudiendo incluso decidir el destino de un conflicto antes de que se inicien las actividades bélicas.

---

* Teniente Segundo. Especialista en Inteligencia Naval. Taeda: palabra del latín que da origen a Tea. La Tea, en el escudo heráldico de la Dirección de Inteligencia de la Armada, representa la luz del saber.

1 Rhode 1996.

El aprovechamiento de las nuevas tecnologías para lograr la "superioridad en información en apoyo a la estrategia militar nacional, afectando la información y los sistemas de información del adversario mientras se refuerza y se protege la información y los sistemas de información propios",[2] es lo que se ha llamado Guerra de Información.

Por ser GI un concepto relativamente nuevo, aún no hay consenso en una sola definición, del mismo modo todavía no se ha llegado a un acuerdo en relación a las actividades propias de la GI por lo que es posible encontrar entre distintas publicaciones algunas divergencias, a las cuales no está exento este artículo. Sin embargo, en algo sí se está de acuerdo, las actividades de GI son de carácter ofensivo y defensivo.

Las actividades Ofensivas de GI tienen como objetivo, tanto en tiempo de paz como en la guerra, la información y los sistemas de información de uso civil y militar y su propósito es:

- Obtener información del adversario ojalá sin que éste se dé cuenta.
- Alterar o dañar la información ya obtenida y almacenada por el adversario con el propósito de engañarlo y hacer que éste confíe en la información que utiliza aún cuando ésta sea falsa.
- Desinformar al adversario proporcionando a sus medios de búsqueda información totalmente falsa o parte de información verdadera cuidadosamente seleccionada para lograr un propósito específico.
- Destruir físicamente información, procesos basados en información y/o sistemas de información del adversario. Esta actividad resulta bastante amplia ya que comprende desde el borrado de un disco hasta la destrucción de un centro de mando y control.
- Negación de los elementos o servicios que requieren para funcionar los procesos basados en información y/o los sistemas de información.

Por su parte, las actividades Defensivas de la GI tienen como propósito evitar que el adversario ejecute con éxito actividades ofensivas sobre la información y los sistemas propios.

Materializan la GI la Guerra de Mando y Control (que a su vez se divide en engaño militar, operaciones psicológicas, guerra electrónica, destrucción física, seguridad de las operaciones, todas ellas apoyadas permanentemente por la Inteligencia) y los Ataques de Información, estos últimos materializados por una diversidad de elementos, técnicas y procedimientos informáticos.[3]

Es necesario hacer otras consideraciones. La información en sí ha pasado a ser un recurso con características muy particulares, su existencia es virtual y no física, el valor de ella en ningún caso tiene relación con la cantidad de datos que se posean, una misma información puede estar en poder propio y del adversario y puede ser entregada al mismo tiempo a más de un usuario sin importar en donde se encuentren.

Por otro lado, aun con sus características de intangibilidad, la información es almacenada en medios físicos y forma parte de procesos que requieren de elementos con existencia real.

Esto implica que habrá actividades de GI que se desarrollarán específicamente en un campo virtual, otras en un campo físico y otras que será necesario realizarlas en ambos. Es la posibilidad de aprovechar el espacio virtual para llevar a cabo acciones ofensivas sobre un adversario lo que en definitiva da origen a la GI.

Inteligencia en la GI.

Los conductores de la GI deberán conducir sus esfuerzos a identificar, neutralizar, degradar y/o destruir la malla de información

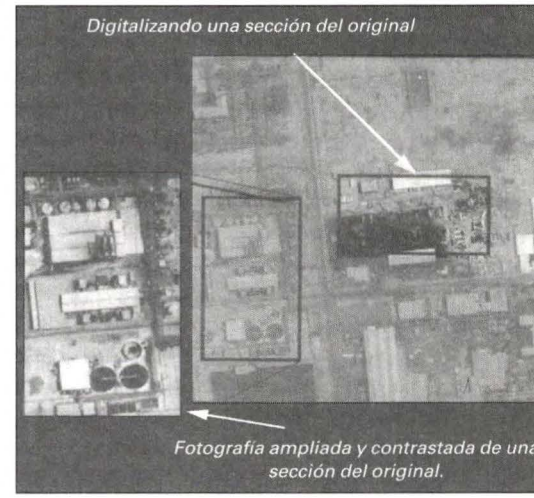
2. Definición del Estado Mayor Conjunto de las FF.AA. de EE.UU.
3. Minoletti, 1996.

formada por nodos y sus enlaces. Los nodos son aquellos puntos de la malla de información en donde se concentran los sistemas, equipos, personal y procedimientos de mando, control e informaciones del adversario ya sean militares o civiles. Todas las alternativas para el traspaso de información entre los diferentes nodos son los enlaces. Pueden distinguirse dos tipos de submallas; la de mando y control, dedicada al transporte de órdenes, coordinación entre los mandos y difusión de inteligencia y la submalla de datos, dedicada al transporte de las informaciones obtenidas por los medios de búsqueda y sensores hasta los centros de análisis o de mando y control. Se debe considerar que habrá segmentos de la malla de información utilizados indistinta o conjuntamente para el mando y control y para la transmisión de datos.

Por otro lado, el conocimiento de los nodos y sus enlaces permitirá identificar los nodos críticos, siendo estos últimos los cuya destrucción o neutralización produce un efecto negativo inmediato tanto en la habilidad de los comandantes para conducir las operaciones como del país para mantener sus procesos basados en la información.

Para obtener el conocimiento que se requiere en relación a los nodos y los efectos de su destrucción, en la ejecución de la GI es posible identificar inicialmente un esfuerzo para obtener la Información que se requiere seguido por un proceso en que a la información obtenida se le da la forma más útil que requieren los usuarios para finalmente hacerla llegar a éstos lo más oportunamente posible. Junto a este proceso de obtención de conocimiento se desarrollan las actividades ofensivas y defensivas de GI.

Si se observa con atención el proceso de obtención de conocimiento, ejecución de actividades ofensivas y de protección; es posible darse cuenta de la similitud que estas actividades tienen con las actividades de Inteligencia materializadas en el Ciclo de Inteligencia, las Operaciones Especiales de Inteligencia y la Contrainteligencia.



Obtención de la información por medio de tecnología satelital computarizada.

El Ciclo de Inteligencia es, a grandes rasgos, un proceso continuo que se inicia en el momento que un mando plantea un EEI[4] al órgano de Inteligencia que le presta apoyo iniciándose en este último la Planificación del Esfuerzo de Búsqueda, etapa en la cual se determina qué información deben buscar los medios de búsqueda con los que cuenta. Cuando se da ejecución a la planificación se inicia la etapa de Búsqueda de Información en la cual los medios de búsqueda explotan las fuentes Abiertas y Cerradas de información a las que tienen acceso para obtener la información solicitada para posteriormente hacerla llegar al organismo de Inteligencia. Una vez recibida la información, se inicia la etapa de Análisis de Información (también llamada Producción de Inteligencia) al final de la cual se obtiene el conocimiento necesario para dar respuesta y satisfacer el EEI planteado por el mando. Para terminar,

4. EEI: Elemento Esencial de Información.

obtenida la Inteligencia ésta debe ser puesta a disposición de los mandos que la requieren de manera oportuna para que puedan tomar las decisiones necesarias en su gestión.

Las OO.EE. de Inteligencia son aquellas actividades, por lo general de naturaleza encubierta,[5] planificadas, ejecutadas y controladas por una Organización de Inteligencia y su propósito es prestar apoyos no convencionales a los mandos que lo requieran para el cumplimiento de su misión. Las OO.EE. de Inteligencia son de carácter ofensivo pero también pueden ser ejecutadas con propósitos defensivos pasando a formar parte de las OO.EE. de Contrainteligencia.

Por su parte, las actividades de Contrainteligencia son ejecutadas para evitar que el adversario tenga éxito en sus propias actividades de inteligencia y eventualmente aprovecharlas en beneficio propio. Lo anterior se materializa por medio de medidas de seguridad pasivas (niegan información), las medidas positivas de C.I. (engañan al adversario) y las OO.EE. de Contrainteligencia (contrarrestan las actividades ofensivas).

Si se considera que la búsqueda planificada de información, la preparación de ésta para que sea útil a los usuarios y su distribución a quienes lo requieren son etapas de un proceso de la GI cuyo propósito es entregar a sus ejecutores conocimiento (en este caso relacionado con los nodos y sus enlaces) y siendo la búsqueda del conocimiento la razón de ser de los organismos de Inteligencia, entonces estas etapas de la GI corresponden a actividades propias del Ciclo de Inteligencia, y por lo tanto, de competencia de los Sistemas de Inteligencia correspondientes a los distintos niveles de mando.

En cuanto a las actividades defensivas de la GI, éstas buscan proteger la información y los sistemas de información propios tanto de las actividades de búsqueda como de las actividades ofensivas de GI del adversario con el propósito de otorgar los niveles de seguridad adecuados a nuestros sistemas. Por ser la seguridad responsabilidad de los Sistemas de Inteligencia, las actividades defensivas de la GI deben considerarse parte de la Contrainteligencia.

Si bien tanto el proceso de obtención de conocimiento como el de otorgamiento de seguridad son actividades inherentes a los Sistemas de Inteligencia, el caso de las actividades ofensivas de GI es diferente. A pesar que por medio de actividades de Inteligencia se pueden lograr todos los propósitos ofensivos de la GI, es en este aspecto donde se pueden identificar actividades ajenas a las propias de Inteligencia, ellas son específicamente la Guerra Electrónica y la destrucción física, ambos elementos de la guerra de Mando y Control y eminentemente ofensivos. Especialmente en tiempo de guerra, la planificación y ejecución de ambas actividades pueden materializarse con medios totalmente ajenos a los Sistemas de Inteligencia pero aun así su éxito en gran medida depende de la Inteligencia que se posea sobre los objetivos. Sin embargo, si es necesario materializar tanto actividades de guerra electrónica como de destrucción física en tiempo de paz y se requiere que su ejecución no sea evidenciado, ambos tipos de operaciones deberán ser consideradas como operaciones de inteligencia sean o no ejecutadas por medios especializados de Inteligencia.

Algo parecido a lo anterior podría señalarse en relación a las Operaciones Psicológicas, las que en algunas ocasio-

5 Las OO.EE. de Inteligencia pueden ser:
Encubiertas: No son evidenciadas ni antes, ni durante, ni después de ejecutadas. Sus efectos, si son perceptibles, son confundidos con accidentes, errores involuntarios, fallas, causas naturales, etc.
Clandestinas: a pesar que sus efectos son atribuibles a OO.EE. de Inteligencia, no es posible identificar a quienes las planificaron y ejecutaron realmente.
Manifiestas: tanto sus efectos como sus ejecutores son evidenciados.

nes son consideradas actividades aparte de la Inteligencia y en otras, parte de ellas.

EL CICLO DE INTELIGENCIA PARA LA GUERRA DE INFORMACION.

Planificación del Esfuerzo de Búsqueda.

Como ya se vio, la identificación de los nodos críticos de la malla de informaciones adversaria es la principal prioridad de los conductores de la GI y para ello requieren determinar su estructura y los procesos de información que en ellos se desarrollan.

Para orientar el esfuerzo de búsqueda deberá considerarse que la malla de información del adversario podría dividirse en tres, la de uso exclusivamente militar, la de inteligencia y la civil.

Búsqueda y utilización de información militar.

La malla de información militar es aquella diseñada principalmente para la conducción de los medios militares en la guerra desde los niveles de toma de decisión estratégicos hasta los tácticos. Forman parte de ella las patrullas de reconocimiento y sus equipos de comunicaciones, sistemas de recolección de imágenes (satélites, fotografía aérea), sistemas de SIGINT, enlaces de comunicaciones, sistemas de obtención, proceso y distribución de inteligencia militar, sistemas de presentación de panoramas, bases de datos, todos los servicios anexos para sostener la estructura, etc.; en general, todos los elementos que componen la submalla de mando y control y la submalla de datos.

En aquellos países en los que existen Sistemas de Inteligencia a nivel nacional y en algunas actividades especializadas ejecutadas por los Sistemas de Inteligencia de las Fuerzas Armadas, podría esperarse una malla de información exclusivamente orientada a actividades de Inteligencia. A diferencia de la malla de información militar, la de Inteligencia cumplirá su papel principal tanto en tiempo de paz como en la guerra y se encuentra formada por los medios de búsqueda de información y sus elementos de transmisión, los sistemas para procesar la información y difundir la inteligencia y los sistemas para materializar actividades ofensivas y defensivas de GI. En algunos casos, la malla de información de Inteligencia podría incluso aprovechar parte de las mallas de informaciones del adversario.

La malla de información civil la componen todos los sistemas para la manipulación, almacenamiento y traspaso de información utilizados para fines no militares o de inteligencia, ya sean gubernamentales o privados, como por ejemplo las bases de datos de empresas privadas y públicas, sistemas de control de la aeronavegación, redes de comunicaciones y datos de organismos públicos o privados, emisoras de radio y televisión, bibliotecas, sistemas de control de la distribución de gas, agua y electricidad, banca electrónica, etc.

Ninguna de las tres mallas nombradas es independiente de las otras. La militar, especialmente en tiempo de guerra, deberá ser capaz de recibir o entregar información a los sistemas de información de Inteligencia y estos deberán integrarse a los militares para contribuir al esfuerzo de la guerra; en tiempo de paz, la integración de ambas mallas deberá contribuir a la planificación y su comprobación. Ahora bien, tanto la malla militar como la de inteligencia se verán apoyadas en la civil por cuanto en la actualidad es

cada vez mayor su dependencia, especialmente en el área de las comunicaciones, a los sistemas civiles. Por otro lado, para la ejecución de algunas operaciones, como por ejemplo las psicológicas, será necesario utilizar algunos de los medios de la malla civil como la radio o televisión.

Sin duda, los puntos de integración de las tres mallas señaladas serán los nodos críticos más importantes que deberá identificar la inteligencia para la GI.

Búsqueda de información.

En la época de la GI lo más importante para materializar esta etapa del Ciclo de Inteligencia es identificar las nuevas posibilidades de explotación de fuentes abiertas y cerradas de información.

Como fuentes abiertas, las redes públicas a nivel mundial dan acceso a los organismos de inteligencia a una gran cantidad de información en un lapso de tiempo mucho menor. Organizaciones no gubernamentales de distintos países ponen a libre disposición de los usuarios de las redes públicas muchos datos de interés.

Por otro lado, información que hasta hace poco no era puesta a disposición del público en la actualidad se ofrece a la venta, como por ejemplo antecedentes comerciales de personas, inscripciones en los registros electorales o registros de vehículos motorizados. Además empresas particulares, como los servicios informativos, se dedican a la recolección de información de acuerdo a las necesidades de sus clientes. Hay empresas como la Economic Intelligence Unit con sede en Londres cuyos servicios consisten en análisis económicos de países o regiones y dentro de éstos, de sectores comerciales específicos, es más, esta misma empresa ofrece a la venta análisis de la situación interna de los países que el cliente requiera. Asimismo, la Jane's Intelligence ofrece un completo panorama de la situación interna de países de distintas regiones del globo. Lo mismo sucede con las cadenas de televisión que en la actualidad tienen la capacidad de abarcar acontecimientos en todas las regiones del mundo e incluso ofrecen a sus televidentes comentarios especializados de distintos ámbitos. Ni siquiera es necesario estar físicamente en el país en el que se origina la señal para tener acceso a ella. Canales de Televisión chilenos son vistos hoy en día en toda América y sus noticiarios o programas especiales son una excelente fuente de información para quienes tengan interés en Chile.

En cuanto a las Fuentes cerradas, la integración de redes informáticas civiles con las militares o las de inteligencia ofrece la posibilidad de acceder a información supuestamente protegida lo que combinado con las actividades tradicionales de explotación de fuentes cerradas puede poner a disposición de los servicios de inteligencia información valiosísima.

Para efectuar el despacho de la información recolectada a los organismos de Inteligencia, los sistemas de comunicaciones actuales hacen posible, por ejemplo, la transmisión en tiempo real de imágenes digitalizadas captadas por una patrulla de reconocimiento en territorio enemigo hacia el departamento de inteligencia de una fuerza. Lo mismo puede hacerse desde satélites, aeronaves, vehículos no tripulados, agentes de inteligencia, buques, etc.

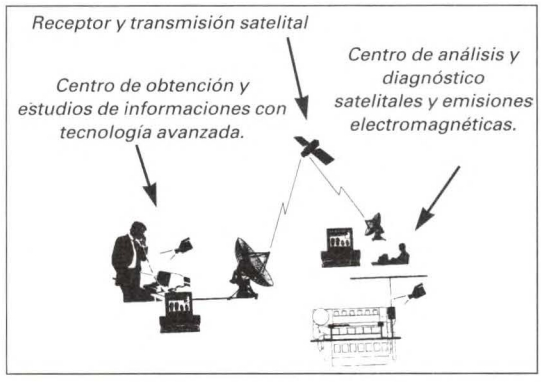
Análisis de información.

El gran volumen de información que es posible reunir en mucho menor tiempo por los medios de búsqueda y la necesidad de los usuarios de la Inteligencia por contar con ella lo antes posible, hace que los Sistemas de Inteligencia deban incorporar a su producción lo más complejo en tecnología de la Información.

Se requiere más que nunca mayores capacidades de almacenamiento en bases de datos diseñadas para facilitar a los analistas la búsqueda de los datos que requieren para sus análisis separando la información esencial de la que no lo es. Para

lo anterior se requerirán mayores velocidades de acceso y presentación de los datos.

Se necesitan herramientas cada vez más poderosas para efectuar el criptoanálisis de sistemas día a día más complejos. Se requieren identificar las herramientas informáticas más adecuadas para el análisis de diferentes tipos como el de sonidos, de emisiones electromagnéticas, de imágenes, de textos, etc. En el ámbito de la Contrainteligencia, existen en otros países softwares capaces de escudriñar en las bases de datos comerciales conectadas en red para ayudar a los analistas a reconocer en ellos algún tipo de relación o patrón de conducta útil para la identificación o ubicación de, por ejemplo, grupos terroristas o espías operando en el país.[6]



Utilización de la tecnología en la Producción de Inteligencia.

Por otro lado, en la presentación de la Inteligencia producida deberán aprovecharse también las ventajas de la tecnología de información actual, como maquetas tridimensionales con recorrido en tiempo real, discos ópticos o transmisión de panoramas a fuerzas de tarea en altamar.

Difusión de la inteligencia.

Los órganos de inteligencia requieren, especialmente en tiempo de guerra, incrementar la velocidad de difusión de la inteligencia producida utilizando la malla de información propia, militar, civil o una combinación de las tres con un nivel de seguridad adecuado para proteger la inteligencia en caso que caiga, ya sea por error propio o por capacidad del adversario, en manos enemigas. Deberán conocerse todas las alternativas de difusión en caso de que falle alguna y debe identificarse exactamente el camino que sigue la inteligencia para llegar a los destinatarios que la requieren para identificar posibles fugas de Inteligencia.

OO.EE. de Inteligencia como actividades ofensivas de GI.

A diferencia de las actividades de la GI asociadas a recolección, análisis, difusión y seguridad que se relacionan directamente a tareas propias de los Sistemas de Inteligencia (Ciclo de Inteligencia y Contrainteligencia), no sucede lo mismo con las actividades ofensivas de GI, las cuales, una vez iniciada la guerra, pueden ser ejecutadas por medios ajenos a los Sistemas de Inteligencia. Sin embargo, todos los objetivos del aspecto ofensivo de la Guerra de Información pueden ser alcanzados ejecutando OO.EE. de Inteligencia especialmente en la paz.

Las OO.EE. de Inteligencia tienen como principal característica su naturaleza encubierta, es decir, no son evidenciadas ni antes, ni durante, ni después de ejecutadas, lo que es especialmente beneficioso para los ejecutores de la GI pues les permitirá lograr el dominio de la información mucho antes de iniciada la guerra y sin que el enemigo siquiera se haya dado cuenta de lo que podría, desde evitar el conflicto hasta impedir que el enemigo sea capaz de controlar sus fuerzas una vez iniciado.

Espionaje.

La obtención encubierta de información del adversario ha sido uno de los objetivos principales de las OO.EE. de Inteligencia,

6. Toffler, 1993.

específicamente por medio del espionaje. Permite a quien lo gesta tener conocimiento con anterioridad de las intenciones y capacidades del adversario y a la vez saber cuan profundo es su conocimiento de las intenciones o capacidades propias con el consiguiente beneficio en la toma de decisiones.

En la era de la GI la actividad del espionaje no debería sufrir mayores cambios en cuanto a su ejecución, más bien serán los espías los que se encontrarán con nuevas alternativas para poder acceder a la información de alto valor y celosamente protegida. En efecto, probablemente no será necesario cambiar los procedimientos de selección, reclutamiento y manipulación de los espías pues éstos seguirán teniendo las mismas motivaciones o debilidades humanas que por siglos han sustentado el espionaje. Lo nuevo que se requerirá de ellos, y por lo tanto de quienes los manipulan, es el conocimiento de nuevas tecnologías que les permitan extraer información confidencial de los sistemas de información que manejan en su trabajo diario así como de las técnicas que deban dominar para poder traspasarla a quienes los "contratan".

Por otra parte, para lograr la obtención encubierta de información puede que ya no sea necesario estar físicamente en el lugar donde ésta se encuentra. Las tecnologías de información han permitido que desde un continente a otro sea posible efectuar una penetración encubierta a bases de datos con información muy reservada sin los riesgos que involucra la manipulación de un espía o la ejecución de operaciones en territorio adversario.

Como ejemplo de lo anterior se puede citar un artículo aparecido a fines del mes de noviembre de 1995 en el diario "The Independent" de Londres. Según revelara, un "Hacker"[7] logró ingresar en sistemas de información secretos del reino, incluyendo los del MI5, MI6 y dependencias militares. Según el artículo, entre otras cosas, el "Hacker" robó información sobre un "refugio" construido para el primer ministro en el centro de Inglaterra para ser utilizado en caso de un ataque nuclear. Asimismo logró penetrar en un centro de datos del gobierno donde figuran direcciones reservadas del personal militar, los teléfonos privados del Primer Ministro, los de los miembros de la familia real en los palacios de Buckingham y Kensington y de los organismos de inteligencia británicos. El primer ministro de la época, John Major, habría reconocido la gravedad del caso y dispuso una investigación para esclarecer esta falla o debilidad del sistema informático británico.[8]

Los sistemas de inteligencia deberían identificar y explotar todas las ventajas que ofrecen estas tecnologías de la información para la ejecución del espionaje combinándolas adecuadamente con la utilización de espías. Probablemente ya no será necesario, como en la segunda guerra mundial, enviar a un agente propio a territorio enemigo para contactarse con la persona dispuesta a entregarle los planes del enemigo. Hoy tal vez sólo sea necesario ubicar una persona dispuesta a dejar encendido el PC de su oficina para que por medio de Internet un agente navegue por la red de la que forma parte. Por otro lado, en la era de la información quizás sea más valioso reclutar a un administrador de redes que a un miembro de la dotación de un buque.

Sabotaje.

A diferencia del espionaje, la forma de materializar el sabotaje como OO.EE. de Inteligencia en el contexto de la GI podría sufrir varias transformaciones, especial-

7. Hacker: término en inglés dado a quienes utilizando sus habilidades en informática explotan las debilidades de los sistemas de información para evadir sus controles de seguridad e ingresar a ellos.
Craker: Hacker que además altera o destruye la información de los sistemas a los que ha ingresado.
8. Manual de Informaciones del Estado Mayor Conjunto de las FF.AA. de Argentina, 1996.

mente debido a las posibilidades que las herramientas informáticas ofrecen hoy en día para ingresar a sistemas de información y alterar o destruir en forma encubierta los datos almacenados en ellos. Pero no sólo la información y los sistemas de información serán objetivos del sabotaje en la GI sino que también todos los procesos o sistemas que de alguna u otra forma ayudan a sostener la malla de información de un país. Es así como, por ejemplo, los altamente automatizados sistemas de producción y control de energía eléctrica se han transformado en un objetivo tan prioritario como la misma información en el campo de batalla de la GI.

Las nuevas herramientas disponibles para el sabotaje le dan a éste todo un nuevo campo de acción en el plano virtual de la GI, incluso con consecuencias concretas en el plano real o físico. El 25 de septiembre de 1995, en el marco de un ejercicio conjunto de la Fuerza Aérea y la Armada de EE.UU., personal de la Base Aérea de Hanscom, Massachusetts, logró penetrar con un PC normal vía Internet a la casilla electrónica de un buque operando en el océano Atlántico. Una vez conectados, navegaron por los sistemas de mando y control del buque pudiendo incluso haber dado órdenes falsas de navegación.[9] Un ejemplo de ataque de información en el campo virtual que podría haber tenido consecuencias en el campo real.

Operaciones Psicológicas, Subversión e Insurgencia.

La influencia de la información sobre las personas y las sociedades es un hecho incuestionable más aun cuando en la actualidad la velocidad de difusión de las informaciones, sean verdaderas o falsas, las hacen llegar a los hogares casi inmediatamente con los consiguientes efectos sobre las familias. La proliferación de herramientas digitales para la obtención, procesamiento y difusión de imágenes y sonido hace posible la modificación e incluso la creación de situaciones ficticias con un efecto psicológico tal sobre los grupos objetivos que pueden ser suficientes para generar ya sea subversión e insurgencia en la población como alteración de la moral de las tropas en el campo de batalla. Imaginemos los efectos que podría haber causado en los soldados alemanes durante la II Guerra Mundial la difusión de una película de Hitler firmando la rendición.

No sólo la alteración de la realidad puede ser aprovechada en actividades de operaciones psicológicas, subversión o insurgencia. Las posibilidades que ofrece, por ejemplo, Internet hace posible que se transmita directa y simultáneamente a millones de personas información que los gobiernos quisieran evitar, es así como grupos terroristas, paramilitares e incluso sectas de todo el mundo han aprovechado la red de redes para conseguir apoyo económico o legitimizar sus acciones. Basta recordar la página Web editada en favor de los terroristas del FPMR que se encontraban en la Cárcel de Alta Seguridad, CAS. De la misma manera, es posible esperar que en una operación de inteligencia se utilice este u otros métodos para hacer llegar al grupo objetivo mensajes que logren efectos desestabilizadores ya sea en la población como en las FF.AA.

Contrainteligencia y Seguridad en la GI.

Como ya se dijo, las actividades defensivas en la GI buscan evitar que se materialice cualquier actividad ofensiva adversaria de GI sobre los sistemas propios y forman íntegramente parte de la Contrainteligencia. Es en el campo virtual donde se deberán concentrar los mayores esfuerzos de los Sistemas de Inteligencia para lograr una adecuada seguridad en la GI.

Esta actividad presenta sin duda grandes problemas para su correcta aplicación. En primer lugar, y como en todo sistema de seguridad, los usuarios serán reticentes a la implementación de las medidas de seguri-

9. Cooper y Olivien, 1995.

dad por varios motivos. Normalmente la seguridad en cualquier ámbito genera gastos que muchas veces los usuarios no están dispuestos a enfrentar; por otro lado, las medidas de seguridad involucran, en ocasiones, incomodidades y molestias que hace que los usuarios las eviten.

En segundo lugar, las actividades de seguridad de la GI deben considerar todas las posibilidades que podría utilizar el adversario para materializar las actividades ofensivas de GI, lo cual en ocasiones es imposible; por el contrario, para lograr una acción ofensiva de GI sólo se requiere identificar una pequeña falla en el dispositivo de seguridad del adversario. Junto con lo anterior, la Contrainteligencia debe considerar que especialmente en el plano virtual las actividades ofensivas de GI, aún cuando pueden ser detectados sus efectos, raramente son identificadas como tal.

Tal es la dificultad para lograr los adecuados niveles de seguridad que en EE.UU., país que reconoce su elevada dependencia a los sistemas de información, los estudios de la Agencia de Defensa de los Sistemas de Información (Arlington, Virginia) indican que el 88% de los sistemas computacionales de defensa son fáciles de penetrar. De las penetraciones exitosas, el 96% no se detecta y lo que es peor, el 95% de las penetraciones detectadas no se informan ni se responden.[10] Preocupante si se considera que en 1995 la citada Agencia efectuó 38000 ataques de información comprobatorios sobre los sistemas de información del Departamento de Defensa de ese país.[11]

Explotando los mismos métodos que los utilizados para materializar las OO.EE., las OO.EE. de Contrainteligencia podrán materializar acciones sobre informaciones que ya posee el adversario con el propósito de engañarlo o desinformarlo.

Para terminar.

Es probable que el lector se pregunte si en Chile estamos en condiciones para materializar actividades de GI o si tanto el País como la Armada se ven amenazados por actividades ofensivas de GI.

Para responderse basta con darse cuenta del nivel de avance en las tecnologías de la información y en las comunicaciones que muestra Chile en estos momentos. Si bien en algunos aspectos pueda identificarse algún tipo de retraso en relación a otros países, en otros podemos decir que estamos al mismo nivel de los más avanzados del mundo y la tendencia nacional es ir modernizando e interconectando todo tipo de procesos en los que se vea involucrada la información.

Se debe recordar que las mallas de información de un país o institución no sólo se ven amenazadas por acciones planificadas por un adversario sino que también por acontecimientos fortuitos o mal intencionados propiciados ya sea por fanáticos de la computación así como por hackers o crackers (como le sucedió a la página web que el Gobierno editó con motivo de la última cumbre iberoamericana realizada en Chile, ocasión en la cual un grupo de crackers alteraron el contenido de dicha página).[12]

Lo mismo sucede con las FF.AA. en general y con la Armada en particular. La modernización de los sistemas de armas, de las comunicaciones y en general la incorporación de nuevas tecnologías necesariamente involucrará aspectos relacionados con los sistemas de información y junto a ello las ventajas y desventajas de incorporar al quehacer diario el campo virtual.

La posibilidad de recibir daño en forma fortuita o por medio de actividades ofensivas de GI dependerá directamente del nivel de dependencia que se tenga de la información, de los sistemas de información y de los medios de protección que ellos tengan. Obviamente, toda organización o Institución tiende a la modernización y ello implica hoy en día la incorporación de nuevas tecnologías de la Información y procesos basa-

10. Rhode, 1996.
11. Cooper, 1996.
12. Valdés, 1996.

dos en ellos y por supuesto la Armada no está ajena a ello. Así como en Chile, otros países y otras Armadas se ven o verán enfrentadas a los nuevos desafíos que presenta la GI y posiblemente estén dispuestos a efectuar acciones ofensivas de GI sobre los sistemas propios, aun en tiempo de paz, especialmente estimulados por lo inadvertido de su accionar en el campo virtual. Si esto sucede y es posible detectarlo es necesario considerar las posibles respuestas o acciones que se deberán tomar.

El Sistema de Inteligencia Naval y sus miembros, especializados o no, deberán prepararse para aprovechar las posibilidades que ofrecen las nuevas tecnologías de la información para materializar el Ciclo de Inteligencia, para reconocer y proteger a la Institución de eventuales ataques de GI y en caso que se requiera, para ejecutar actividades ofensivas por medio de OO.EE. de Inteligencia en el campo virtual o real.

Conclusiones.

Los avances de la tecnología en los sistemas asociados a la información y la necesidad de contar con ella lo más rápidamente posible, ha llevado a que en la actualidad tanto la información propiamente tal como sus procesos relacionados, adquieran cada vez mayor trascendencia para la conducción de todo tipo de gestiones tanto en el ámbito civil como en el militar. La necesidad de asegurar el flujo de las informaciones ha dado pie a la creación de mallas de información capaces de enlazar en forma permanente a quienes requieran de esa información. Estas mallas están compuestas por nodos y enlaces de comunicaciones en los cuales se procesa, almacena y circula la información. Estos nodos y enlaces han generado un nuevo espacio o dimensión en la cual es posible planificar y ejecutar actividades que pueden causar daños a un adversario: el espacio virtual.

La Guerra de Información reconoce en los sistemas militares modernos y en la manera de conducir la guerra una dependencia creciente en las mallas de información e incorpora el espacio virtual como una nueva dimensión para ejecutar acciones bélicas. Lo anterior ha permitido identificar nuevas vulnerabilidades y debilidades que hacen posible acciones ofensivas y necesarias actividades defensivas de GI.

La obtención planificada, el procesamiento y la difusión de información es un proceso que cumple los mismos objetivos que el Ciclo de la Inteligencia y son equivalentes, por lo que estas etapas de la GI deben considerarse actividades de Inteligencia.

Los Sistemas de Inteligencia, como responsables de la Contrainteligencia, deben considerar dentro de sus tareas todas las actividades defensivas de GI así como aquellas que tienen el propósito de engañar al adversario o de contrarrestar sus actividades ofensivas de GI.

Las OO.EE. de Inteligencia cuentan en la actualidad con una amplia gama de posibilidades para ejecutar todo tipo de actividades ofensivas de GI especialmente en el espacio virtual. En este plano, las herramientas informáticas permiten la ejecución de este tipo de operaciones con un altísimo nivel de encubrimiento lo que las hace especialmente aptas para materializarlas en tiempo de paz.

Tanto la Armada como el Sistema de Inteligencia Naval se van modernizando y junto con ello van integrando nuevas tecnologías que traen consigo vulnerabilidades y capacidades susceptibles de ser aprovechadas en el marco de la GI. Por otro lado, otras Armadas están haciendo lo mismo y probablemente estén dispuestas a desarrollar acciones ofensivas de GI sobre sistemas propios por lo que se requiere estar preparado.

* * *

BIBLIOGRAFIA

- Rhode, William: "What is Info Warfare?". Proceedings, febrero de 1996.
- Minoletti Olivares, Jorge: "La Guerra de la Información". Revista de Marina N° 834, Sep-Oct de 1996.
- Toffler, Alvin y Heidi: "Las Guerras del Futuro". Little, Brown & Company, New York 1993.
- Seguridad Informática en Peligro. Manual de Informaciones del Estado Mayor Conjunto de las FF.AA. de Argentina. 16 de julio de 1996.
- Cooper, Pat y Olivieri, Frank: "Hacker evidencia debilidades de EE.UU.". Defense News N° 40, 9 al de octubre de 1995.
- Cooper, Pat. U.S.: "Lawmakers Examine vulnerabilities of Internet". Defense News, 27 de mayo de 1996.
- Krauss: "Information Warfare in 2015". Proceedings, agosto de 1995.
- Cooper, Pat: "Militares demuestran enlace de comunicación global". Defense News, 9 al 15 de octu bre de 1995.
- Cooper, Pat.: "C3I, los datos se transforman en los blancos del campo de batalla". Defense News, 4 al 10 de diciembre de 1995.
- Naval Doctrine Publication (NDP) 2, Naval Intelligence. Department of the Navy, Office of the Chief of Naval Operations and Headquarters United States Marine Corps, 30 de septiembre de 1994.
- Valdés, Hernán: "Confesión de un Hacker". Qué Pasa N° 1338, 30 de noviembre de 1996.
- En Internet: file:///CI/FERNANDO/CYBER.HTM.
  Daniel E. Magsig at dmagsig@seas.gwu.edu o magsig@comm.hq.af.mil.