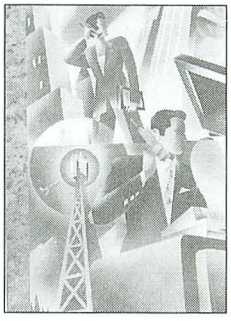
LA GUERRA DE LA INFORMACION

Jorge Minoletti Olivares *
Capitán de Navío



Introducción.

La Guerra de la Información, también conocida como I-War,[1] IW (Information War) y C4I (Mando, Control, Comunicaciones, Computador e Inteligencia), dominará el espectro del conflicto en el siglo XXI. Aunque este tipo de guerra no es nueva, el explosivo desarrollo de la tecnología en las últimas décadas ha generado innumerables posibilidades de explotación de la información.

Se ha descrito la historia de la guerra como en tres olas. Durante la revolución agraria, la guerra era llevada a cabo por una clase guerrera basada en la información. La revolución industrial cambió el sentido de la guerra a una de destrucción masiva. Los estados usaban ejércitos masivos para extender sus dominios con una alta tasa de bajas humanas y materiales. En la era de la información, la capacidad destructiva no es masiva sino que selectiva sobre objetivos específicos y con la mínima cantidad de bajas humanas y materiales. La siguiente tabla muestra las principales características de lo expuesto:

La "revolución de la información" está ingresando progresivamente a nuestros hogares y a nuestro lugar de trabajo. Desde las redes internacionales como Internet hasta las locales que son múltiples, muchos usuarios pueden tener acceso a información que antes les era vedada. Del mismo modo, las actividades tanto civiles como de defensa son cada vez más dependientes de los computadores y de las comunicaciones y muchas veces, sistemas de información que son claves y esenciales de una organización, están siendo cada vez más interlazados. Los llamados "*hackers*"[2] *pueden ahora, aprovechar las oportunidades que les proporciona las vulnerabilidades de estos sistemas* y producir estragos difíciles de cuantificar. En el ámbito de la defensa, esta Guerra de la Información ha adquirido una relevancia especial, por cuanto el logro del dominio de la información sobre el adversario, decidirá conflictos mucho antes que el empleo de otras formas más violenta de aplicación de la fuerza sea necesario. La Armada no está ajena a esta posibilidad y vulnerabilidad. En consecuencia, las medidas que se adoptan para explotarlas o eliminarlas, necesariamente deberán ir de la mano con el desarrollo tecnológico de nuestra Institución. El presente trabajo no pretende otra cosa que ilustrar en la forma más amplia y genérica posible, la relevancia que el acceso a la tecnología ha adquirido en cuanto a las posibilidades de controlar o afectar los procesos de información. Si bien es cierto, es aplicable a todo tipo de actividades, se ha preferido hacer énfasis en aquellos aspectos más relacionados con el ámbito de la defensa.

Definiciones.

La definición más ampliamente aceptada es la del Ejército de los Estados Unidos de Norteamérica:

"La Guerra de la Información son acciones llevadas a cabo para el logro de la superioridad

---

* Oficial de Estado Mayor
1 En inglés, en el original.
2 Se ha optado por traducir el término "hackers" por ser de uso común y para evitar interpretaciones erróneas.

de la información, afectando la información, los procesos basados en la información y los sistemas de información adversarios, mientras se protege la información, los procesos basados en la información y los sistemas de información propios".

Esta definición puede ser aplicada tanto a individuos como a organizaciones, a estados y al ámbito militar. Amplía el campo a información pura, a procesos basados en la información y a los sistemas de información. Incluye los aspectos ofensivos y defensivos. Incluye el campo militar y el civil de los negocios.

También se ha definido lo que se entiende por guerra cibernética y guerra de redes, siendo la primera más aplicable al campo militar y la segunda, más amplia, se refiere a un contexto más general.

Dominio de la Información, también conocido como Superioridad de la Información, se refiere a la situación en que uno de los adversarios posee practicamente una alerta completa en el campo de batalla mientras que al otro, se le niega el acceso a la mayoría de las fuentes de información.

Amplitud.

La Guerra de la Información abarca varios aspectos bien definidos. Entender bien estos aspectos nos ayudará a comprender su amplitud.

Un aspecto de la Guerra de la Información es que abarca todo el espectro del conflicto, a través de la cooperación, la competencia, la crisis y la guerra. Aún en el caso de cooperación como podría ser una coalición, habrán aspectos que no se desearán pasar a los otros integrantes.

Otro aspecto de la Guerra de la Información es que es aplicable a través del tiempo aún cuando el conflicto escale o se distienda. En este caso, el espectro abarca la competencia internacional política o económica, las operaciones militares de tiempo de paz, la crisis, conflictos no declarados, terminación del conflicto y el restablecimiento de la normal competencia política o económica.

Otra faceta de la Guerra de la Información es que abarca espacios que cubren toda la sociedad, tales como lo militar, lo tecnológico, lo económico, lo político, lo social y lo ideológico-religioso.

La Guerra de la Información, como se dijo, es tanto ofensiva como defensiva. Sin embargo, existen restricciones en la capacidad de actuar para lograr un balance entre ambas. Por ejemplo, un gobierno puede tener la capacidad para controlar una acción ofensiva pero no tiene un control directo de toda la información, procesos basados en la información o sistemas de información sobre los cuales se pueda llevar a cabo una acción defensiva ante un contraataque por parte del adversario.

La Guerra de la Información también abarca todos los niveles de la organización y mando, desde un simple individuo hasta estructuras globales, pasando por organizaciones, estados y estructuras internacionales. También es posible que el adversario provenga de diferentes niveles, no necesariamente el mismo desde donde se actúa.

La Guerra de la Información es vulnerable a adversarios tanto internos como externos lo que incidirá en las medidas defensivas a ser adoptadas.

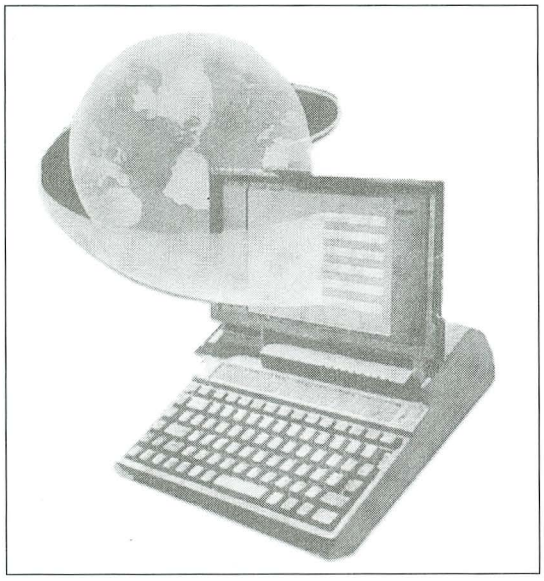
Algunos autores sostienen que existen básicamente siete formas de guerra que caen dentro del campo de la Guerra de la Información. Estas son: guerra de mando y control, guerra basada en inteligencia, guerra electrónica, guerra sicológica, guerra de "hackers", guerra de información económica y guerra cibernética.

La guerra de mando y control es la principal componente en el campo militar de la Guerra de la Información. El objetivo en este caso es de decapitar al adversario de modo que los líderes enemigos no sepan dónde se encuentran sus fuerzas y éstas, no sepan lo que sus mandos esperan de ellas. Sus aplicaciones fuera del campo netamente militar son muy limitadas ya que sus efectos son demasiado drásticos.

La guerra basada en inteligencia corresponde a la componente tradicional de la Guerra de la Información. Sin embargo, se deben actualizar sus conceptos para incluir el mayor campo que cubre en la actualidad.

La guerra electrónica es el elemento de mayor nivel tecnológico de la Guerra de la Información, principalmente en el campo militar. Tradicionalmente ha estado orientada a dominar el espectro electromagnético. Desafortunadamente, si éste es el caso, deja muy vulnerables a los sistemas de información y a los procesos basados en la información. La guerra electrónica requiere entonces integrarse más estrechamente a las otras formas de guerra dentro del contexto de la Guerra de la Información.

La guerra sicológica reconoce el elemento humano de la Guerra de la Información. Se dice



que es una batalla por la mente humana. En este contexto, la guerra sicológica debe abarcar las nuevas capacidades que le otorga la tecnología. Por ejemplo, el uso de computadores para efectuar análisis de posibles grupos objetivo, en el diseño de la propaganda o mensajes apropiados y en la difusión más eficiente de éstos.

La guerra de los "hacker" es el típico elemento no militar de la Guerra de la Información. Es el elemento que recibe mayor atención en los medios de comunicación y aprovecha las oportunidades que ofrece la tecnología a la sociedad en general.

La guerra de información económica comprende las oportunidades para afectar la economía adversaria. Por ejemplo, un país que tenga una inversión relativamente importante de capitales en un país adversario, puede retirarlos con el consiguiente deterioro de su economía. La tecnología puede permitir que se alcance a retirar una cantidad significativa de ellos, antes de que una reacción pueda congelarlos.

La guerra cibernética representa actualmente los otros elementos de la Guerra de la Información y que muchas veces cae en la ciencia ficción. Representa el conjunto de elementos que pueden o no ser realistas, tanto en el presente como en el futuro.

Política y Estrategia.

Existen tres grandes temas de discusión respecto a la política de la Guerra de la Información.

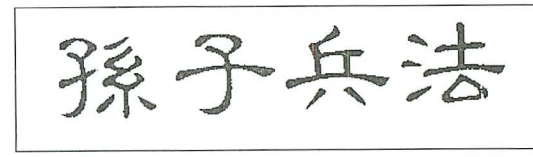
El primero es si este tema debe ser abierto a debate público o no. Será muy difícil convencer al sector privado que tomen en serio este tema si es que no se les ha mostrado las amenazas que esto representa.

Desafortunadamente, una discusión abierta le entregará valiosa información al adversario respecto a las vulnerabilidades a ser explotadas.

El segundo tema es si el gobierno debe o no controlar directamente la defensa o si las medidas de protección deben ser dejadas en manos del sector privado. En un sistema de libre mercado de alta competencia, la seguridad de la información adquiere un bajo nivel de prioridad. Por otro lado, la mejor defensa es aquella que se adopta desde un principio en contraste con aquella que se aplica en un sistema que ya está operando. Lo que se necesita es una política que controle la defensa del bien común pero que a la vez no restrinja la independencia y la capacidad de innovar.

El tercero es respecto a si determinadas operaciones de la Guerra de la Información pueden ser consideradas actos criminales. Por ejemplo, algunos países sostienen que matar a los Jefes de Estado durante un conflicto constituye un acto criminal por el gran efecto desestabilizador que genera. Del mismo modo, podría considerarse el atacar los computadores del sistema financiero de una nación adversaria.

El objeto de la Guerra de la Información es el logro del Dominio de la Información. Haciendo un símil con la Estrategia Marítima, se puede argumentar que éste es imperfecto a la vez que muy difícil de cuantificar. La intención no es otra que seguir las enseñanzas de Sun Tzu: Derrotar al enemigo antes de entrar en combate, el logro de 100 victorias en 100 batallas no es la esencia de la guerra sino que ésta es derrotar al enemigo sin combatir. Al definir las prioridades para seleccionar el Centro de Gravedad, Sun Tzu establece que la primera es atacar la estrategia y el plan del enemigo y la segunda, romper las alianzas, antes del inicio de la guerra o del uso de la fuerza. Esto se puede llevar a cabo mediante el empleo de las armas particulares de este tipo de guerra que más adelante se describen, eliminando la capacidad del enemigo de comunicarse o atacando las



interconexiones entre sistemas. Donde haya una interfase, habrá una vulnerabilidad a explotar.

Características del teatro de operaciones.

Bajos costos de entrada. En comparación con los altos costos de las fuerzas estratégicas, un ataque a la información puede ser efectuado sin necesidad de recurrir a un gran financiamiento y además, por cualquier individuo u organización.

Ambigüedad de fronteras. En este espacio, las fronteras entre naciones y el sector privado no está totalmente delimitado lo que hace que la diferencia entre guerra y crimen o entre intereses públicos y privados tenga menos significación.

Percepción política. Las nuevas técnicas basadas en la información pueden aumentar sustancialmente la potencialidad de actividades tales como la decepción y la manipulación de imágenes. La desinformación puede hacer muy difícil que gobiernos apoyen políticamente actividades necesarias para la Seguridad Nacional.

Escasez de inteligencia. Las vulnerabilidades de la guerra de la información no son bien comprendidas. Puede que la identidad de los posibles adversarios no sea conocida y los métodos clásicos de recolección y análisis de inteligencia no sean aplicables. Se deberá desarrollar nuevos métodos de análisis y de relaciones entre organizaciones.

Dificultad en la toma de decisiones. Existirán enormes dificultades para distinguir un ataque de guerra de la información de otro tipo de actividades y eventos tales como espionaje, accidentes, falla de sistemas y acciones de los "hackers". La incapacidad de efectuar tales distinciones puede llevar a respuestas militares muy cautelosas ante reales situaciones de crisis regionales.

Dificultad en estructurar y mantener coaliciones. La estructura de una coalición estará en riesgo en el punto más débil de sus enlaces de comunicaciones. La incapacidad de darse apoyo mutuo en la protección contra la guerra de la información puede poner en peligro la capacidad de crear y sostener coaliciones.

Vulnerabilidad interna. La economía y la sociedad actual están descansando cada vez más en una infraestructura de redes de información de alto rendimiento en todo aspecto, desde vuelos comerciales y distribución de electricidad hasta la administración de cuentas bancarias personales. A los potenciales combatientes de la Guerra de la Información, se les presenta ahora un nuevo abanico de objetivos estratégicos de alta significación.

Principios de la Guerra de la Información.

Se han propuesto 8 principios de la Guerra de la Información, catalogados en 4 grupos de dos principios cada uno:

Decapitación. Este principio establece que el mando y control, los sistemas de apoyo a la

CATEGORIA		PRINCIPIO
Negación	1	Decapitación
	2	Prioridad de Sensores
Potenciamiento de la Fuerza	**3**	**Conocimiento**
	4	**Volatilidad**
Supervivencia de la Alerta y del	5	Supervivencia
Mando, Control y Comunicaciones	6	Interoperatibilidad
Niveles	**7**	**Jerarquía**
	8	**Intensidad**

toma de decisiones y las comunicaciones debieran ser el principal objetivo de la Guerra de la Información de modo de aislar al mando adversario de sus fuerzas de combate.

Prioridad de Sensores. Este principio establece que todos los sensores enemigos deben ser suprimidos o destruidos antes de entrar en combate.

Conocimiento. El principio del conocimiento indica que debe estar disponible tanta información como sea posible para aquellos que la necesitan y que su distribución debe ser lo más fluida como se pueda. En otras palabras, establece que la información de inteligencia debe dejar de ser enviada a un mando central para su posterior distribución. Esta es una medida defensiva y no ofensiva como se pretende.

Volatilidad. Este principio establece que debe haber una estrecha relación entre el sentido de urgencia y el proceso de toma de decisiones. Esto reconoce lo efímero de la naturaleza de la información.

Supervivencia. La política y la estrategia deben ser centralizadas, pero la planificación y la ejecución deben ser descentralizadas, para dificultar tanto como sea posible, un ataque del enemigo. En otras palabras, todos deben tener claro el panorama general para estar en las mejores condiciones de contribuir al logro de los objetivos cuando el mando central se vea afectado en su sistema de mando y control. En vez de operar con una estructura jerárquica tradicional, se debe actuar en un ambiente de red.

Interoperatibilidad. Los sistemas de comunicaciones y de almacenamiento de información deben ser lo más interoperables posible de modo de compartir al máximo la información disponible. Muchas veces la tecnología actual impide traspasar información vital por problemas de compatibilidad de equipos de comunicaciones. Por ejemplo, un controlador aéreo adelantado de la Fuerza Aérea debiera estar en condiciones de comunicarse con el piloto de una aeronave de la Aviación Naval que lo sobrevuele, en vez de tener que seguir toda la cadena de mando a través de los centros de la Armada y de la Fuerza Aérea.

Jerarquía. Este principio indica que se deberá aplicar en contra del adversario, toda la tecnología disponible para llevar a cabo una Guerra de la Información, aunque parezca que el enemigo no es capaz de desarrollar este tipo de guerra.

Intensidad. Se deberá desarrollar todo el esfuerzo posible y se deberá evitar interferencias políticas en el nivel operacional. Restricciones en este sentido representan vulnerabilidades que pueden ser explotadas por adversarios internos o externos.

Sistemas de armas.

Software malicioso. Tal vez lo más común de encontrar son los famosos virus, gusanos, Caballos de Troya y bombas lógicas. A pesar de que estas armas tienen un enorme potencial de causar grandes daños, es sumamente difícil controlar a manos de quien van a parar. Una vez que un virus es lanzado, puede llegar a infectar tanto a los sistemas adversarios como a los propios.

Un virus es un fragmento de programa codificado que se copia él mismo en un programa más grande, modificándolo. Se ejecuta solamente cuando corre su programa huésped. Luego, en la medida que el virus se reproduce, infecta otros programas.

Un gusano es un programa independiente. Se reproduce de un computador a otro, normalmente inserto en una red. A diferencia del virus, no modifica otros programas.

Caballos de Troya son fragmentos de programas codificados ocultos en otro programa y desarrollan una función de eliminación. Son un mecanismo popularmente usado para eliminar virus y gusanos. Un ejemplo de esto es el programa SATAN (Security Administrating Tool for Analyzing Networks) para verificar sistemas UNIX, disponible en forma gratuita en Internet.

Una bomba lógica es una especie de Caballo de Troya usada para lanzar un virus, gusano u otro tipo de ataque. Puede ser un programa independiente o un fragmento de programa codificado, implantado por un programador o al desarrollar un sistema.

Chipping. Es la práctica de fabricar "chips"[3] electrónicos vulnerables a desarrollar una determinada función no conocida por el usuario. Por ejemplo, algunos chips pueden ser diseñados para fallar cuando reciban una señal específica o después de un determinado período de tiempo como también, que emitan una señal característica para poder ser localizados.

3 Se optó por no traducir la palabra "chip" por la misma razón anterior.

Puertas traseras. Las puertas traseras se diseñan para anular los sistemas de seguridad. Por ejemplo, el fabricante de un chip electrónico cifrador podría diseñar una puerta trasera secreta de modo que él pueda descifrar fácilmente un mensaje cifrado con ese chip.

Armas electromagnéticas. Estas armas son diseñadas para quemar los receptores de los equipos electrónicos adversarios. Existen los cañones HERF (High Energy Radio Frecuency) y las bombas EMP (Electromagnetic Pulse). Los primeros son emisores de alta potencia para saturar los circuitos electrónicos. Las segundas, provienen de explosiones atómicas o convencionales que pueden ser detonadas por Fuerzas Especiales cerca de un centro de información del enemigo.

Microbios destructivos. Actualmente existen investigadores que están trabajando en desarrollar microbios que se coman los componentes electrónicos de modo que en un eventual conflicto, puedan ser introducidos en el equipamiento electrónico adversario para producir fallas. Actualmente existen microbios que comen aceite. ¿Se podrán desarrollar microbios que coman silicio?

Nanomáquinas. Estos son pequeños robots, más chicos que una hormiga, que se pueden dispersar en un centro de información del enemigo. Caminan por las paredes y oficinas hasta encontrar un computador, introduciéndose por sus ranuras y dañándolo.

Radiación Van Eck. Es una radiación de muy bajo nivel que emiten todos los equipos electrónicos. Esta puede ser monitoreada, lo que se conoce como Tempest y disponer de la información que por ejemplo, emite un computador.

Criptografía/criptoanálisis. A pesar del significativo desarrollo de la criptografía, el criptoanálisis seguirá siendo importante,
apoyado por el también significativo avance de los sistemas de computación.

Spoofing[4]*/Autentificación*. Spoofing es el envío de señales falsas. Se puede efectuar mediante el envío de señal electromagnética pero también, suplantando una fuente de entrada para desbaratar un sistema de información.

Mutación de imágenes. Esta puede ser un arma usada para hacer aparecer un líder adversario diciendo algo que efectivamente no ha dicho y hacerlo perder credibilidad.

Operaciones sicológicas. Las operaciones sicológicas se benefician con la capacidad de conducir investigación de mercado y de análisis de datos para definir grupos objetivos y mensajes apropiados.

Ataque al sistema bancario, interrumpir el control del tráfico aéreo, negación de servicio. Se pueden considerar varios tipos de operaciones con efectos obvios tales como anulación del sistema de conmutación telefónica, golpe al mercado de valores, ataque al sistema de ruteo ferroviario, interferir cuentas bancarias, interrumpir el control del tráfico aéreo y negar el servicio de empresas.

Sensores stand-off y close-in.[5] En el aspecto militar, los sensores fuera y dentro del alcance de las armas pueden ser considerados como armas de la Guerra de la Información en cuanto a la generación de data se refiere.

Apoyo a la toma de decisiones. Esta es un arma clave en la Guerra de la Información, especialmente en el aspecto defensivo. Si bien es cierto que los sistemas de información pueden ser controlados por el hombre, se requiere de un gran nivel de automatización para poder manejar la gran cantidad de datos que se requiere para detectar ataques, identificar el tipo de ataque, generar los cursos de acción defensivos, evaluar los cursos de acción y evaluar los daños.

Conclusiones.

No se debe considerar la Guerra de la Información como un tema nuevo. Este ha existido desde tiempos remotos y no se debe ignorar los múltiples acaecimientos que nos muestra la historia y que caen dentro de este concepto.

Tradicionalmente, la Guerra de la Información había estado orientado a un ámbito bastante reducido. Con el desarrollo tecnológico y su incidencia en el manejo de la información, este ámbito se ha extendido por toda la sociedad y en todos los campos. Si se ignora este gran panorama y se concentra sólo en un aspecto, se corre el riesgo de dejar vulnerabilidades sin cubrir.

Los principios de la Guerra de la Información demuestran claramente que sobre todo, ésta requiere de un alto grado de compromiso para definir objetivos con la suficiente antelación y para

4 En inglés, en el original.
5 En inglés, en el original.

estructurar y desarrollar una campaña que permita alcanzarlos. La Guerra de la Información no se puede tomar a la ligera ni aplicarse parcialmente.

Las armas de la Guerra de la Información son de una tecnología como nunca antes vista. Así también, son los blancos a atacar o a defender.

El objeto de la Guerra de la Información es el de ganar el dominio de la información con el propósito de resolver un conflicto antes de que éste comience.

Con el propósito de ser exitosos en la Guerra de la Información, deberá haber conciencia y alerta respecto a sus amenazas en todos los niveles de mando. No es otro el propósito de este artículo.

Por último, aún existe mucho que decir respecto a la Guerra de la Información. Sin embargo, el punto de partida será definir la política en su aplicación para posteriormente pasar a establecer los objetivos y así, estructurar la planificación correspondiente. La Armada de los EE.UU. de N.A. estructuró un plan llamado "Copérnico" que incluye lo aquí tratado.

BIBLIOGRAFIA

1 Griffith, Samuel B., Sun Tzu, The Art of War, traducción.
2 Handel, Michael I., Masters of War: Sun Tzu, Clausewitz and Jomini.
3 Haeni, Reto E., An Introduction to Information Warfare, en Internet, reto@seas.gwu.edu
4 Magsig, Daniel E., Information War, In the Information Age, en Internet, dmagsig@seas.gwu.edu
5 Resumen de investigación de RAND efectuada para el Instituto de Investigación de Defensa Nacional basado en el artículo: Strategic Information Warfare: A New Face of War, por Roger C. Molander, Andrew
S Riddile y Peter A. Wilson en Internet order@rand.org
6 Toffler, Alvin y Heidi, Las Guerras del Futuro.
7 Glosario del Institute for the Advanced Study of Information Warfare (IASIW), en Internet.
8 US. Navy, Naval Doctrine Publication, NDP-1 Naval Warfare.