La evolución tecnológica y la Internet le han dado un gran impulso al concepto de Guerra de la Información, que hoy es más real que nunca y opera en diferentes áreas, las cuales pueden ir desde ataques por diversión hasta espionaje económico y actividades terroristas.

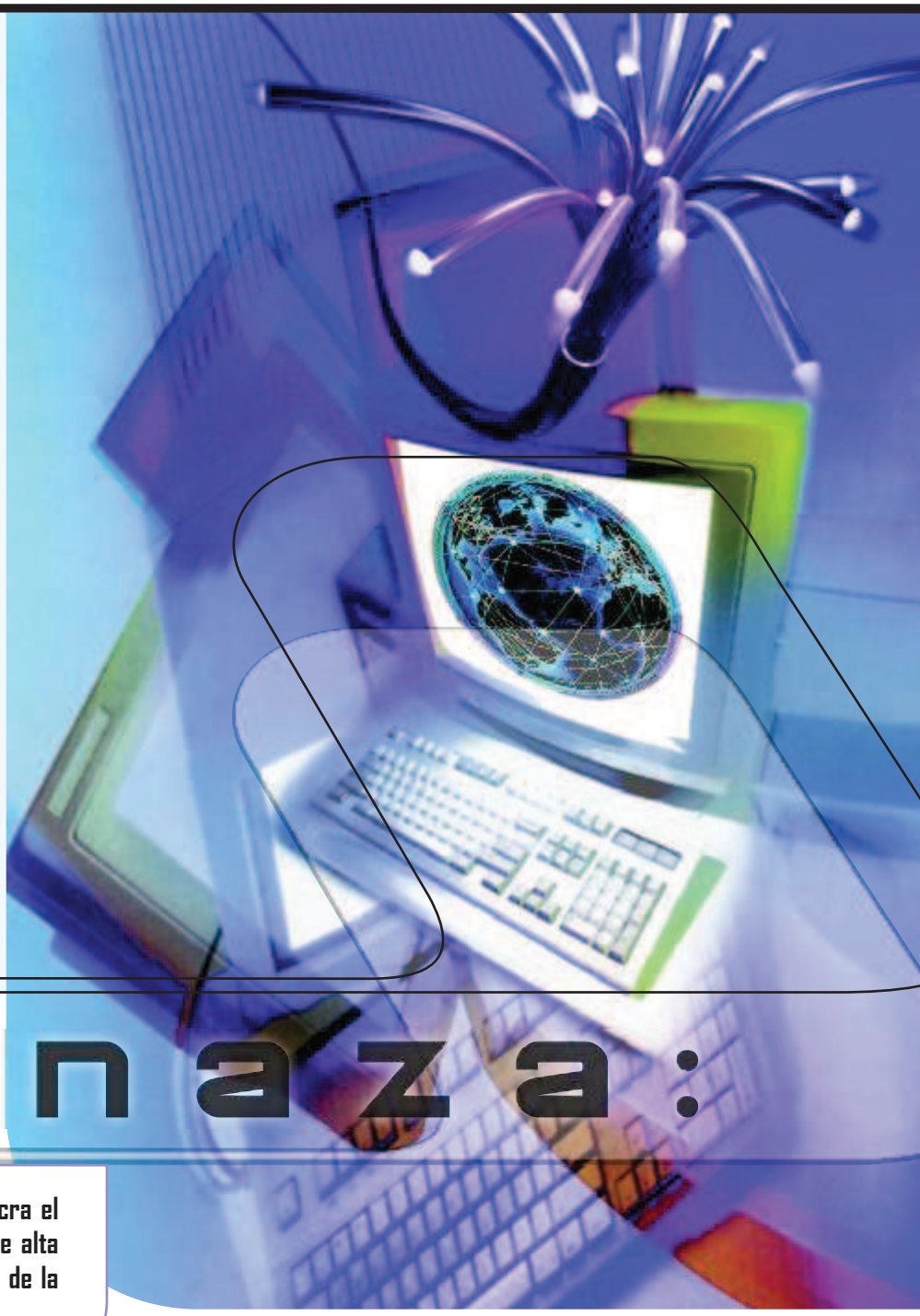
la guerra de la información

Por Capitán de Navío (Perú)
José Luis Gavidia Arrascue

una nueva

En los últimos años, la Guerra de la Información ha capturado la atención de organismos gubernamentales, empresas y especialistas en seguridad de la información. El término se usa para cubrir un amplio espectro de actividades, pero especialmente el escenario en donde el terrorista de información, usando solamente un teclado y un ratón, accede ilegalmente a un computador y causa el choque de aviones y cortes de energía, o sabotea los suministros de alimentos. El terrorista podría sabotear los computadores que apoyan la banca y las finanzas, buscando que las bolsas de valores caigan o que las economías se derrumben. Aparentemente ninguno de estos desastres ha ocurrido, pero la preocupación es que algún día sucedan, dada la facilidad con que algunas personas han podido juguetear, impunemente, con los computadores, incluso aquéllos operados por el Departamento de Defensa de los Estados Unidos. El presente artículo presentará una visión de la Guerra de la Información y por qué es necesario conocerla.

"Si las personas civilizadas ya no ponen prisioneros a muerte, ya no saquean ciudades y ya no ponen tributos a los países pobres, es porque la inteligencia juega un gran papel en su conducta de guerra y les ha enseñado maneras más eficaces de aplicar la fuerza que estas manifestaciones crudas de instinto". Carl Von Clausewitz.



amenaza:

La Guerra de la Información involucra el uso de computadores y aparatos de alta tecnología para dañar los recursos de la informática de un adversario.

La Guerra Fría ha terminado, pero ha sido reemplazada por nuevos tipos de guerra. Estas guerras envuelven el uso de la tecnología como una herramienta para ayudar en la conducción de operaciones destinadas a ganarle al enemigo. Una de ellas utiliza la información como arma principal, por lo cual es llamada la Guerra de la Información. Ella abarca muchas áreas, desde la guerra electrónica, actividades terroristas y hasta incluso el espionaje económico. Este nuevo tipo de amenaza ya viene siendo utilizado en el mundo, aunque no con el poder que realmente tiene, y por esto debemos estar preparados para afrontar todas aquellas armas que existen actualmente, para poder repeler los ataques o disminuir su impacto. Para estar preparados, hay primero que conocer lo que es la Guerra de la Información y lo que ella puede hacer.

La Guerra del Golfo

Entre abril de 1990 y mayo de 1991, cinco hackers holandeses se introdujeron en los sistemas de computadores de por lo menos 34 sitios militares estadounidenses de Internet, incluyendo sitios que estuvieron apoyando directamente la Operación Tormenta del Desierto. Ellos navegaron a través de archivos y correos electrónicos, buscando palabras clave como nuclear, armas, misiles y tormenta del desierto. Ellos obtuvieron información acerca de la localización exacta de las tropas americanas, de los tipos de armas que tenían, de las capacidades de los misiles Patriot y del movimiento de los buques de guerra en la región del Golfo Pérsico. Cuando lograron sus objetivos, los hackers borraron toda huella de los sistemas para esconder su paso, como lo afirma el experto Graeme Browning. Aún pensando en poder identificar a los hackers, el gobierno de los Estados Unidos no hubiese podido hacer nada, ya que en ese tiempo el acceso no autorizado a computadoras no era ilegal en Holanda.

Al entrar en los sistemas de aprovisionamiento de las tropas estadounidenses en el Golfo Pérsico, ellos pudieron enviar cepillos de dientes en vez de balas o pertrechos militares de importancia. Incluso algunos de ellos trataron de vender la información a Saddam Hussein, pero presumiendo una emboscada, el presidente iraquí declinó la oferta.

La era de la información

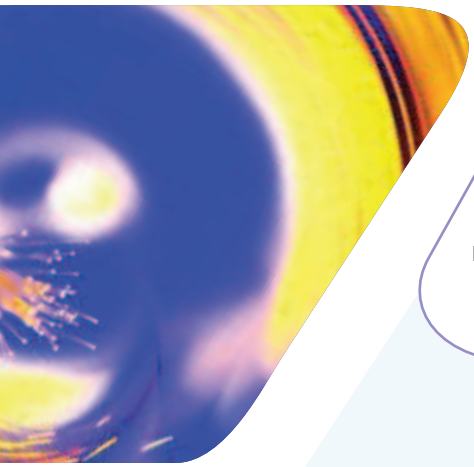
Estamos inmersos en la era de la información. Ya no existe el peligro de una bomba H, sino de una bomba I (de información). Por ello, los países luchan para lograr su control. La revolución de la información está en sus comienzos y, para entender por qué va a ser tan vital, es importante conocer la manera como la tecnología está cambiando las formas en que manejamos dicha información.

Lo que caracteriza a esta era son los modos completamente nuevos en que la información se puede intercambiar y manipular, y la velocidad cada vez mayor a la que podemos manejarla. Las capacidades de los computadores están transformando los dispositivos convencionales de comunicación, ya que permiten reunir, clasificar y distribuir múltiples datos, así como mostrarlos gráficamente.

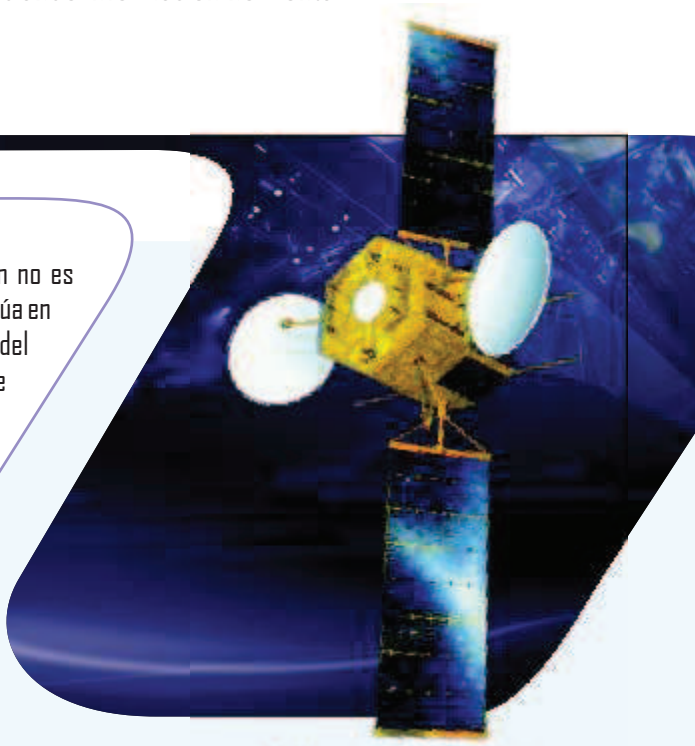
Mientras la tecnología de las comunicaciones se digitaliza y el cable de fibra óptica reemplaza poco a poco al de cobre, posibilitando transportar una gran cantidad de señales por su mayor ancho de banda, la autopista de la información se va estructurando. Esta autopista será indispensable porque ofrecerá una inmensa combinación de información disponible en todo momento. Contamos en la actualidad con los beneficios de una red de fibra óptica que se amplía constantemente, y que resulta impermeable a las interferencias, interrupciones y cuellos de botella de los servicios que ofrecían las redes antiguas.

Asimismo, se está desarrollando un cinturón de comunicaciones satelitales en órbita baja que cubriría toda la tierra (66 satélites a 780 kilómetros) y que se utilizaría para transmisiones de televisión, de datos y también para la telefonía fija, como alternativa a la fibra óptica. Ello posibilitaría el uso de terminales de tamaño de bolsillo, en los que el número del celular satelital identificará sólo al usuario, sin ninguna relación con el lugar en que se encuentra.

El ámbito militar también se ve favorecido, gracias a la confluencia de los avances de la tecnología digital en las comunicaciones y la informática. Las Fuerzas Militares de la mayoría de los países se encuentran en un proceso de actualización de sus doctrinas y medios, para adaptarlas a los cambios que está produciendo la era de la información. De acuerdo con Cronin (1999), en una determinada situación donde la complejidad e incertidumbre es la norma, ganar la Guerra de la Información permitirá a todos los niveles de una organización, militar o civil, compartir en tiempo real una misma percepción de la situación, intercambiando información horizontal y verticalmente.



La Guerra de la Información no es una actividad aislada: ella se sitúa en el contexto de la acción y del conflicto humano y por ello se divide en cuatro áreas: juego, crimen, derechos individuales y seguridad nacional.



Por ello, que el objetivo será llevar la información que está disponible a cualquier elemento de la organización que la necesite. Así mismo, tendrá prioridad el dominio sobre los sistemas de información del enemigo y de la competencia.

Definiciones

¿Qué es la Guerra de la Información? 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 de la información, afectando la información, los procesos basados en la información y los sistemas de información enemigos, 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, y abarca el campo militar y el civil de los negocios.

La Guerra de la Información involucra el uso de computadores y aparatos de alta tecnología para dañar los recursos de la informática de un adversario. Esto puede

hacerse para obtener información de un enemigo, causar estratos a una nación o la industria al romper su infraestructura de información, o para difundir propaganda cuando otros medios no podrían ser prácticos.

Según Schwartau (1996), una vista popular descompone la Guerra de la Información en tres clases: guerra de información personal, guerra de información corporativa, y guerra de información global. Lo que distingue las tres categorías es si el asunto del ataque es un individuo, una empresa comercial o un gobierno, respectivamente.

La Guerra de la Información está estrechamente relacionada con la guerra infraestructural, la cual involucra la ruptura de un gobierno sin causar pérdida de vidas necesariamente. Cuando más computadores se conecten a sistemas usados por la sociedad, la capacidad de usarlos para comprometer en la guerra infraestructural aumentará.

Algunos autores, como Libicki (2002), sostienen que existen básicamente siete formas de guerra que caen dentro del campo de la Guerra de la Información: 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 comando 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 a su vez 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. Un ataque electrónico deja muy vulnerables los sistemas de información y los procesos basados en ésta. La guerra electrónica requiere una relación más estrecha con 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 hackers 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 afectan 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 estos capitales antes de que una reacción pueda congelarlos.

La guerra cibernética representa actualmente los otros elementos de Guerra de la Información y que muchas veces caen en la ciencia ficción. Representa el conjunto de elementos que pueden ser realistas o ficticios, tanto en el presente como en el futuro.

Sus características

En el libro de Denning (2001) se muestran las siguientes características de la Guerra de la Información:

Bajo costo. 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, puede ser ejecutado por cualquier individuo u organización.

Ambigüedad de fronteras. En este espacio, las fronteras entre naciones y el sector privado no están totalmente delimitadas, 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 masiva pueden aumentar sustancialmente la desinformación, lo cual puede dificultar que los 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 deberán 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 o falla de sistemas. 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 personales. A los potenciales combatientes de la Guerra de la Información se les presenta ahora un nuevo abanico de objetivos estratégicos de alta significación.

Las armas utilizadas

Las armas de la Guerra de la Información, según el artículo de Kirkendall (2002), son las siguientes:

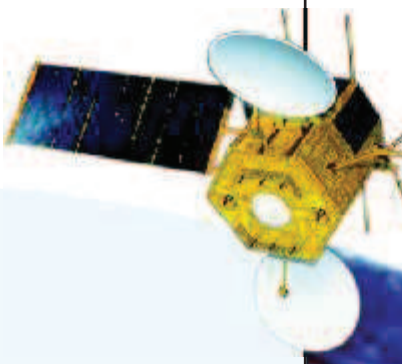
Software malicioso. Tal vez lo más común son los famosos virus, gusanos, caballos de Troya y bombas lógicas. A pesar de que estas armas tienen un enorme potencial de causar grandes daños, es sumamente difícil controlar a manos de quién van a pasar. Una vez que un virus es lanzado, puede llegar a infectar 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 un programa huésped. Luego, en la medida que el virus se reproduce, infecta otros programas. Un gusano es un programa independiente que se reproduce de un computador a otro, normalmente inserto en una red, y a diferencia del virus, no modifica otros programas. Los 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. Por último, una bomba lógica es una especie de caballo de Troya usado para lanzar un virus, gusano u otro tipo de ataque. Puede ser un programa independiente o un fragmento de programa codificado.

Chipping. Es la práctica de fabricar chips 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 para que emitan una señal característica para poder ser localizados.

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 puede descifrar fácilmente un mensaje cifrado con ese chip.

Armas electromagnéticas. 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



Existen básicamente siete formas de guerra que caen dentro del campo de la Guerra de la Información: guerra de mando y control, guerra basada en inteligencia, guerra electrónica, guerra sicológica, guerra de hackers, guerra de información económica y guerra cibernética.

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. Son pequeños robots, más chicos que una hormiga, que se pueden dispensar en un centro de información del enemigo. Caminan por las paredes y las 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. Puede ser monitoreada, lo que se conoce como Tempest, y así se puede 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 / autentificación. Es el envío de señales falsas. Se puede efectuar mediante el envío de una señal electromagnética o suplantando una fuente de entrada para desbaratar un sistema de información.

Mutación de imágenes. Puede ser un arma usada para hacer aparecer a un líder adversario diciendo algo que no ha dicho, y hacerle perder credibilidad.

Operaciones sicológicas. Se benefician con la capacidad de conducir investigaciones de mercado y de análisis de datos para definir grupos objetivos y mensajes apropiados.

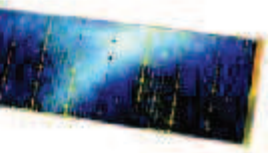
Ataques al sistema bancario, interrupciones en el control del tráfico aéreo, negación de servicio. Se pueden considerar varios tipos de operaciones con efectos obvios, tales como anulación del sistema de conmutación telefónica, golpes al mercado de valores, ataques al sistema ferroviario, interferir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

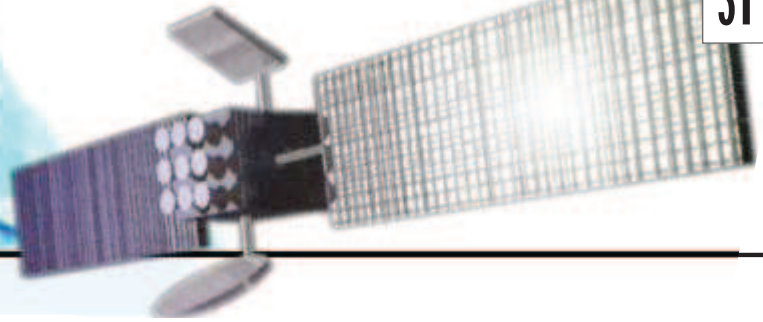
Sensores Stand-off y Close-in. En el aspecto militar, los sensores fuera y dentro del alcance de las armas pueden ser considerados como armas de la Guerra de la Información, en cuanto a la generación de datos se refiere.

Apoyo a la toma de decisiones. 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 y evaluar los cursos de acción y los daños.

Cuatro grandes áreas

La Guerra de la Información no es una actividad aislada: ella se sitúa en el contexto de la acción y del conflicto humanos, y por ello se divide en cuatro áreas: juego, crimen, derechos individuales y seguridad nacional.





El área del juego cubre a los piratas informáticos, particularmente el acceso ilegal a sistemas y los actos realizados por pura diversión. Involucra el conflicto entre los piratas informáticos y los dueños del sistema que ellos penetran y aprovechan.

El área del crimen, por su parte, envuelve los actos ilegales, incluyendo los crímenes sobre la propiedad intelectual, el fraude y el abuso informático. Involucra los conflictos entre los perpetradores y las víctimas de los crímenes.

El área de los derechos individuales cubre la libertad de expresión y el derecho a la privacidad. Esta área se da entre los individuos y, entre los individuos y las organizaciones o gobiernos.

El área de seguridad nacional se dirige hacia los conflictos de un país. Incluye las operaciones de inteligencia extranjera, guerra y conflictos militares, terrorismo y guerra de red.

Estas áreas no son completamente aisladas. Por ejemplo, la piratería informática normalmente es un crimen y a menudo viola la privacidad. Es más que un juego de niños y puede ser empleada por grupos de crimen organizado, agencias gubernamentales de inteligencia, unidades militares u organizaciones terroristas.

La amenaza está presente

No se debe considerar la Guerra de la Información como un tema nuevo. Ha

existido desde tiempos remotos, y no se deben ignorar los múltiples acontecimientos que nos muestra la historia y que caen dentro de este concepto.

Tradicionalmente, la Guerra de la Información había estado orientada 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 atiende sólo en un aspecto, se corre el riesgo de dejar vulnerabilidades sin cubrir.

Los principios de la Guerra de la Información demuestran claramente que requiere de un alto grado de compromiso para definir objetivos con la suficiente antelación y para estructurar y desarrollar una campaña que permita alcanzarlos. La Guerra de la Información no se puede tomar a la ligera ni aplicarse parcialmente. Sus armas son de una tecnología nunca antes vista, y así también son los blancos por atacar o defender.

La amenaza existe. Está ahí y no debe ignorarse. Es difícil de identificar y por consiguiente de prevenir y de enfrentar. Puede manifestarse en un amplio espectro de situaciones, desde tiempos de paz hasta conflictos de alta intensidad, y tener diferente finalidad y distintos efectos. No es una amenaza del futuro: es una nueva amenaza contra la que hay que empezar a prepararse desde ya, para asegurar el éxito a largo plazo.

Los objetivos de la amenaza van desde el nivel más alto, que puede comprometer la seguridad nacional, al mero usuario particular que puede ser objeto de la agresión. La amenaza evoluciona de forma paralela a la de las nuevas tecnologías, y la aceleración del cambio es impresionante.

El sector privado el principal usuario y creador de sistemas de información y comunicaciones, y va mucho más rápido y se adapta mejor a este cambio constante que los gobiernos. Por ello, más que nunca, la colaboración es fundamental el sector privado y el público, y la solución del problema debe abordarse de una forma multidisciplinaria, dirigida desde el nivel político.

Siempre deberá buscarse un equilibrio para respetar los derechos individuales y conseguir

el grado de seguridad deseable. La clave, como en otros campos, se encuentra en la educación, en el nivel cultural de cada uno de los individuos, ahora aplicado a este nuevo ámbito.

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 las armas. Con el propósito de ser exitosos en la Guerra de la Información, se deberá tener conciencia y estar alerta con respecto a sus amenazas en todos los niveles de comando. 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.

Dentro de esta nueva era de la información, Colombia no está libre de sufrir algún ataque con armas que se emplean la Guerra de la Información. El país está adaptándose a las exigencias mundiales del manejo de la información y al crecimiento cada vez mayor del comercio electrónico, con lo cual, obligatoriamente, tendrá que adaptarse también a la Guerra de la Información.

.