Una nueva amenaza: La Guerra de la Información

Teniente Segundo
Róger Valencia Reyes

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 actividad pero especialmente el escenario en donde el "terrorista" de información, usando no más que un teclado y un ratón, accesa ilegalmente en una computadora y causa el choque de aviones, cortes de energía, o sabotea los suministros de alimentos. El "terrorista" podría sabotear las computadoras que apoyan la banca y las finanzas, causando que las bolsas de valores caigan o que las economías se derrumben. Aparentemente ninguno de estos desastres ha ocurrido, pero la preocupación es que ellos, y otros como ellos ocurran, dada la facilidad con que algunas personas han podido juguetear con las computadoras con impunidad, incluso aquellas operadas por el departamento de defensa de los EE.UU. El presente artículo presentará una visión de la Guerra de la Información y por qué es necesario conocerla.

Palabras llave: ***Guerra de la Información, seguridad de la información.***

"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 las maneras más eficaces de aplicar la fuerza que estas manifestaciones crudas de instinto."

Carl Von Clausewitz

Introducción

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 utilizada en el mundo, mas no con el poder que realmente tiene, y es por eso que se debe de estar preparado para afrontar todas aquellas "armas" que posee para poder repeler el ataque o disminuir su impacto. Para estar preparado, 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 computadoras de por lo menos 34 sitios militares americanos de internet, incluyendo sitios que estuvieron apoyando directamente la "Operación Tormenta del Desierto". Ellos navegaron a través de archivos y correos electrónicos, buscando palabras llave 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. Cuando lograron sus objetivos, los hackers borraron toda huella de los sistemas para esconder su paso (Browning 1997). 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.

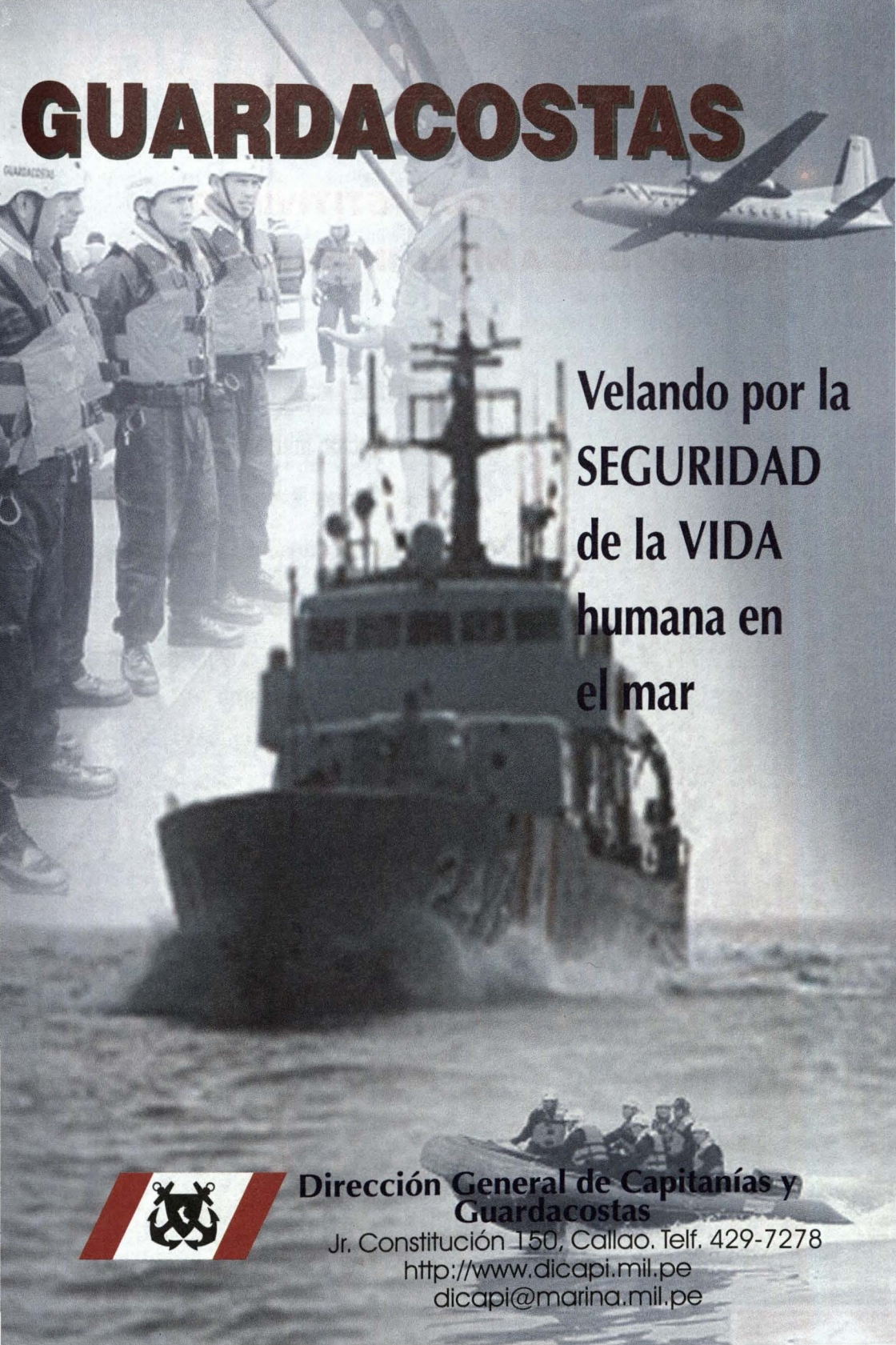
Al entrar en los sistemas de aprovisionamiento de las tropas americanas en el Golfo Pérsico, ellos pudieron enviar cepillos de dientes en vez de balas o pertrechos militares de importancia. Incluso algunos de ellos trataron de vender la información a Saddam Hussein, pero presumiendo una emboscada, el Presidente iraqui, 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" (información), es por esto que los países luchan para lograr el control de la información. La revolución de la información está en sus comienzos y, para entender por qué va a ser tan vital, es importante conocer el modo en que 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 las computadoras están transformando los dispositivos convencionales de comunicación, ya que permiten reunir, clasificar y distribuir múltiples datos, así como mostrarlos gráficamente.

GUARDACOSTAS



Velando por la SEGURIDAD de la VIDA humana en el mar

Dirección General de Capitanías y Guardacostas

Jr. Constitución 150, Callao. Telf. 429-7278

http://www.dicapi.mil.pe

dicapi@marina.mil.pe

PUERTOS PERUANOS

EFICIENCIA Y COMPETITIVIDAD RECONOCIDAS A NIVEL INTERNACIONAL

- Tarifas justas, sin sobrecostos
- Atención ininterrumpida las 24 horas
- 10 días libres de pago por almacenaje
- Seguridad y garantía integral
- Personal calificado
- Atención especial a naves de turismo
- Interconexión vía internet



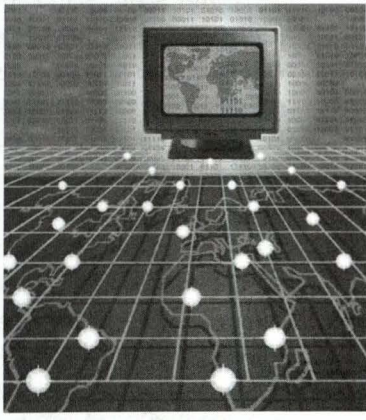
ENAPU S.A.
EMPRESA NACIONAL DE PUERTOS S.A.

MTC
Ministerio de Transportes, Comunicaciones, Vivienda y Construcció

Mientras la tecnología de las comunicaciones se digitaliza y el cable de fibra óptica reemplaza al de cobre, posibilitando transportar una gran cantidad de señales por su mayor ancho de banda, la "autopista de la información" se va estructurando. La misma 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 permeable 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 km.), y que se utilizaría para transmisiones de televisión, de datos a banda ancha y también para la telefonía fija, como alternativa a la fibra óptica. Ello posibilitaría el uso de terminales de tamaño de bolsillo, en donde 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.



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

Guerra de la Información

• 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. Incluye el campo militar y el civil de los negocios.

La guerra de información involucra el uso de computadoras 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 estragos 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 guerra de información en tres clases: la guerra de información personal, guerra de información corporativa, y la 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 información está estrechamente relacionada a la guerra infraestructural, la cual involucra la ruptura de un gobierno sin causar pérdida de vidas necesariamente. Cuando más computadoras se conecten a sistemas usados por la sociedad, la capacidad para usar las computadoras para comprometer en la guerra infraestructural sólo 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. 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 comando 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. Esta deja muy vulnerables a los sistemas de información y a los procesos basados en la información. 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 hacker es el típico elemento no militar de la Guerra de la Infor-

mación. 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.

• **Características de la Guerra de la Información**

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, 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 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 administra-

ción 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.

- **Armas de la Guerra de la Información.** Las armas de la Guerra de la Información según el artículo de Kirkendall (2002) son las siguientes

Software malicioso. Tal vez lo más común de encontrar son los famosos virus, gusano, Caballo 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 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 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.

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 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 ad-

versario 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 /autentificación. Es el envío de señales falsas. Se puede efectuar mediante el envío de señal electromagnética o 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 no ha dicho y hacerle perder credibilidad.

Operaciones sicológicas. Estas 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. 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. 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 los daños.

- **Áreas de la Guerra de la Información**

La guerra de información no es una actividad aislada, ella se sitúa en el contexto de la acción humana y del conflicto humano. La Guerra de la Información 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 envuelve a los actos ilegales, in-

cluyendo los crímenes sobre la propiedad intelectual, el fraude y 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 la privacidad. Éstos se dan entre los individuos y, entre los individuos y organizaciones o gobiernos. Finalmente, el área de seguridad nacional se dirige hacia los conflictos a un nivel nacional. Incluye las operaciones de inteligencia extranjera, guerra y conflictos militares, terrorismo y guerra de red.

Las áreas no son completamente separadas. 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.



Actos delictivos que amenazan la economía de una nación tienen implicaciones de seguridad nacional. Actos que infringen la privacidad o la libre expresión pueden ser crímenes. Los actos terroristas también son crímenes.

Conclusiones

No se debe considerar la Guerra de la Información como un tema nuevo. Ésta 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 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 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 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. Así también, son los blancos a atacar o a defender.

La amenaza existe. Está ahí y no debe ignorarse. Es difícil de identificar y por consiguiente actuar contra ella. Puede manifestarse en un amplio espectro de situaciones, desde tiempos de paz a la de con-

flicto de alta intensidad y con diferente finalidad y 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 pareja a la de las nuevas tecnologías, y la aceleración del cambio es impresionante.

El sector privado es hoy el principal usuario y creador de sistemas de información y comunicaciones, y va mucho más rápido y se adapta mejor a este cambio constante, de lo que hacen las administraciones de los gobiernos de los estados. Por ello, más que nunca, la colaboración es fundamental entre ambos y la solución del problema debe abordarse de una forma multidisciplinaría, 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 otras tantas cosas, 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 el propósito de ser exitosos en la Guerra de la Información, deberá tenerse 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, el Perú no está libre de sufrir algún ataque por parte de las armas que posee la Guerra de la Información. El Perú está adaptándose a las exigencias mundiales del manejo de la información y al crecimiento cada vez mayor del comercio electrónico, con ello, obligatoriamente, tendrá que adaptarse también a la Guerra de la Información.

Bibliografía.

- Browning, Graeme. Counting Down. *National Journal*, Washington, v. 19, n. 16, p.746-749, abr. 1997.
- Cronin, Blaise, Crawford, Holly. Information Warfare: Its application in military and civilian context. *The Information Society 15* (4), Indiana, p. 257-263, feb. 1999.
- Denning, Dorothy. *Information Warfare and Security*. Toronto: Addison Wesley, 2001. 522p.
- Kirkendall, Erick. *Information warfare and the civilian agency*. [online]. Disponible en Internet via www.url: http://www.gitec.org/assets/pdfs/pdf96/infowar.pdf. Archivo capturado el 20 de agosto del 2002.
- Libicki, Martin. *What is Information Warfare?*. [online]. Disponible en Internet via www.url: http://www.ndu.edu/inss/actpubs/act003/a003cont.html. Archivo capturado el 20 de agosto del 2002.
- Schwartau, Winn. *Information Warfare:* Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1996. 432p.