LA GUERRA INFORMÁTICA

CLAUDIO C. LÓPEZ

El Capitán de Fragata IM Claudio César López ingresó en la Escuela Naval el 19 de enero de 1981, egresando como Guardiamarina de IM en el año 1985.
Estuvo asignado a diferentes funciones en distintas unidades de IM. En el año 2005 obtuvo la Capacitación como Analista Operativo, y desde el año 2006 se encuentra cursando el Magíster en Ingeniería del Software, título que otorga el Instituto Tecnológico de Buenos Aires (ITBA).
Actualmente se encuentra destinado en el Servicio de Análisis Operativo, Armas y Guerra Electrónica, como Jefe de la División Infantería de Marina del Departamento Análisis Operativo.

La guerra informática se anuncia como una herramienta revolucionaria que se empleará en los futuros conflictos armados. Designada normalmente con la expresión **ataque contra las redes informáticas** (*Computer Network Attack, CNA*), las ramificaciones de este tipo de acción o acciones pueden llegar a ser considerables.

Más allá de los debates en curso, es innegable que las guerras del siglo XXI serán muy diferentes de las que caracterizaron al siglo XX. Los trágicos ataques terroristas del 11 de septiembre de 2001 y sus secuelas son el tema dominante en las noticias en estos comienzos del nuevo siglo. En el futuro, quizá sea tan digno de destacar el desarrollo de "guerras informáticas" como medio de combate. Esto planteará problemas a la doctrina vigente sobre la conducción de la guerra, exigirá que se revise el concepto de **espacio** en la batalla y ampliará la gama de métodos y medios de guerra existentes.

La guerra informática es, en pocas palabras, un subconjunto de operaciones de información que puede definirse como **las acciones que se realizan a fin de alterar la información y los sistemas de información del adversario, mientras se protege la información y los sistemas de información propios.** Tales operaciones abarcan, prácticamente, toda medida cuyo objetivo sea descubrir, alterar, destruir, interrumpir o transferir datos almacenados, procesados o transmitidos por un ordenador. Pueden efectuarse en tiempo de paz, durante una crisis o en las etapas estratégica, operativa o táctica de un conflicto armado. El logro del propósito mencionado se obtendrá a través de la superioridad informática, ya sea contando con una tecnología superior o haciendo un empleo más adecuado de las facilidades informáticas propias.

Los ataques a través de redes informáticas son muy variados e incluyen, entre otros recursos, lograr el acceso a un sistema informático a fin de controlarlo; transmitir **virus** y destruir o alterar datos mediante el empleo de "bombas lógicas" que permanecen inactivas en un sistema hasta que ocurra un hecho particular o en un momento prefijado insertando **gusanos** que se reproducen y sobrecargan la red; empleando **programas husmeadores** para interceptar y/o captar datos, etc.

A medida que pasa el tiempo, la infraestructura informática de los países, inclusive el nuestro, es cada vez mayor, constituyéndose en uno de nuestros puntos más vulnerables, dado que somos cada vez más dependientes de esta tecnología en lo que respecta a nuestras comunicaciones, nuestro transporte, nuestras operaciones financieras y, sobre todo, nuestro sistema de defensa. Como consecuencia de ello, dicha infraestructura sería, probablemente, el blanco clave de un Estado agresor o de una organización terrorista.

BOLETÍN DEL CENTRO NAVAL
Número 817
Mayo/agosto de 2007
Recibido: 10.11.2006

En este artículo, que representa el inicio de una serie de otras presentaciones, se muestra una visión general del empleo de los medios informáticos en los conflictos armados actuales, asociados a la doctrina propia de las Fuerzas Armadas.

Operaciones de la guerra informática

Características

Como mencionamos al principio, las acciones que se desarrollan en la guerra informática son aquellas actividades que tendrán como fin el obtener la capacidad de recopilar, procesar y difundir un flujo ininterrumpido de información precisa y fiable, mientras se explota y se priva al adversario de la capacidad de hacer lo mismo.

Las operaciones se caracterizarán por la superioridad en la obtención de información en cantidad y calidad, lo que generará un mayor poder de combate al enlazar a los sensores, a los comandantes y a los sistemas de armas para lograr una apreciación compartida de la situación, mayor capacidad de mando, un ritmo de operaciones más elevado, mayor letalidad y mayor supervivencia.

Además, resulta necesario evaluar los conocimientos y los factores psicológicos como componentes de la relación de fuerzas. El impacto de una disparidad de conocimientos fue claro entre los soldados estadounidenses y los iraquíes en la Guerra del Golfo Pérsico. Las armas de la más alta tecnología empleadas por la Coalición no les habrían servido a los soldados iraquíes, muchos de los cuales eran analfabetos. La guerra del futuro, caracterizada por conocimientos de alta tecnología deberá ser dirigida y conducida por expertos en el empleo de los medios informáticos.

Las características del software y el hardware de combate deberán prever la inexistencia de fallas. Un diseño defectuoso puede ocasionar numerosas reiniciaciones por día en un sistema comercial, en un sistema militar esas fallas repetitivas podrían ocasionar lesiones o hasta la muerte. Por ejemplo, durante la Operación Paz Duradera, el sistema empleado por cinco soldados estadounidenses para dirigir una bomba autodirigida fue reiniciado y, por sorpresa para ellos, introdujo en el sistema su actual posición en lugar de la posición del blanco. Por consiguiente, la bomba se dirigió hacia la posición donde éstos se encontraban en lugar del objetivo seleccionado. La conclusión es que las aplicaciones militares exigen mayor rendimiento en ciclos de tiempo reducidos que las aplicaciones que no lo son.

Objetivos materiales

Como en la guerra clásica, los objetivos materiales de las operaciones de guerra informática se adecuan al nivel de planeamiento y ejecución de que se trate. En el nivel táctico serán los centros de comunicaciones, comando y control enemigos, de logística o aquellos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la conducción de las operaciones militares. En el nivel operacional, podrán llegar a ser las líneas de comunicación, logísticas, de comando y control operacional del adversario, centros de desarrollo de tecnología, así como capacidades y actividades relacionadas. Por último, en el nivel estratégico, se podrán incluir objetivos nacionales, influyendo en todos los ámbitos (políticos, militares, económicos o relacionados con la información).

Tipos de operaciones

Los tipos de operaciones en la guerra informática podrán ser comparados con los de la guerra clásica clasificando las mismas en operaciones ofensivas y defensivas. Podremos llamar acciones u “operaciones” ofensivas a aquellas que impidan al enemigo hacer un uso efectivo de sus medios y redes informáticas.

Durante la guerra serbio-bosnia, en la década de los 90, las computadoras del portaaviones estadounidense *Nimitz* y el sistema informático principal de la OTAN fueron violados por hackers de todo el mundo que simpatizaban con la causa yugoslava. Las páginas web de la Casa Blanca quedaron bloqueadas durante todo un fin de semana. Estas acciones, desarrolladas entonces por aficionados, constituyen un ejemplo de lo que podemos denominar "ofensiva informática". Las mismas hacen un uso intensivo de "armas digitales" (1) para alterar, destruir, deteriorar o perturbar la información contenida en los ordenadores y redes informáticas enemigos, afectar la performance de sus sistemas operativos, obtener datos, afectar medios físicos de almacenamiento, etc.

Los objetivos de las operaciones ofensivas en la guerra informática podrán ser:

- Propagación de virus computacionales para contaminar el flujo de la información enemiga.
- Controlar los elementos temporales (Internet) mediante la conducción de iniciativas en el ámbito de la información tendientes a inducir, engañar, encubrir, contener, etc.
- Interrumpir o sabotear la información o el sistema de información del enemigo (ej.: bombardeando sus sistemas de comunicaciones), así como su estructura para la conducción de operaciones de información.
- Dispersar las fuerzas, armas y fuegos del enemigo, logrando al mismo tiempo la concentración de las fuerzas, armas y fuegos de las unidades propias.
- Confundir, efectuar diversión o transmitir información falsa al enemigo, persuadiéndolo de que lo real es falso y lo falso es real.
- Cambiar los datos en las redes.
- Diseminar propaganda.
- Divulgar información redundante.
- Obtener información.

Por otro lado llamaremos defensivas a aquellas acciones u "operaciones" que impidan al enemigo tener éxito en su accionar ofensivo. Éstas podrán representar tareas de protección de los sistemas y redes tanto físicas como digitales. Las misiones que pueden ser encomendadas a las fuerzas son en muchos casos coincidentes con los fines perseguidos por las operaciones ofensivas pero con un sentido defensivo.

(1)
Para introducir el concepto de arma digital, primero tendríamos que diferenciarlo del concepto de virus informático. Un virus informático debe tener como características principales: ser dañino, autorreproducible y subrepticio. El daño que pueda producir no depende de su complejidad sino del entorno en el que actúe. Mientras que este último es, normalmente, de origen amateur y sus efectos son generalizados, el arma digital está elaborada profesionalmente con el objeto de producir un daño específicamente dirigido. La programación del arma digital se desarrolla a partir de una tarea de inteligencia previa que define el entorno en el que actuará y sus objetivos. Para el cumplimiento de los mismos, se desarrollan payloads que se disparan a partir de cláusulas, características del entorno, órdenes directas, etc. Asimismo, el programa incluye contramedidas ante recursos de defensa pasiva, activa o automática, y complementos digitales que refuerzan su módulo de defensa y ataque.

Áreas de aplicación

Las áreas de las operaciones militares que se ven más beneficiadas o afectadas por este tipo de guerra son: las Comunicaciones, la Inteligencia y el Comando y Control. A continuación desarrollaremos cada una de ellas.

Comunicaciones

El establecimiento oportuno de la conectividad en las redes de comunicaciones es esencial para el éxito y supervivencia de las fuerzas en los entornos de la guerra actual y futura. Conflictos recientes han comprobado la necesidad de contar con despliegues y reacciones rápidas ante los escenarios que cambian vertiginosamente. La toma de decisiones eficaz y oportuna se torna imposible si no contamos con comunicaciones adecuadas locales y a gran distancia (por ejemplo, alta frecuencia o satélite) tanto dentro como fuera del teatro de operaciones. La adaptación de la tecnología de emisiones radioeléctricas y red local (LAN) facilita el establecimiento rápido de redes de datos de alta velocidad.

El hecho de que la transmisión de información a través de las redes (LAN, WAN, Internet) emplee todos los medios de comunicaciones conocidos crea una vulnerabilidad en el uso de los dispositivos informáticos a la guerra electrónica desarrollada por el enemigo. Por lo tanto es necesario un análisis de las acciones tanto activas (malware (2)) como pasivas que se deben implementar a fin no sólo de asegurar el flujo de información digital propio sino, tam-

(2)
Cualquier programa cuyo objetivo sea causar daños a ordenadores, sistemas o redes y, por extensión, a sus usuarios.

bién, perturbar el del enemigo. Esto incrementará sustancialmente la complejidad del planeamiento de las comunicaciones en razón del volumen de información que será necesario transmitir y proteger a la vez.

Acciones de la guerra electrónica, como la interferencia, la escucha, el análisis del trafico, el engaño, tendrán su correlato en la guerra informática en acciones como el fraude digital, la intrusión en las redes enemigas, la inundación de virus, etc., por lo que la batalla digital tendrá doble alcance, o sea, afectará a las comunicaciones y a los medios informáticos.

Inteligencia

En la guerra del futuro la obtención de información acerca del enemigo y el campo de combate o área de conflicto se verá favorecida por dispositivos que empleen una combinación de fotografía /video digital con la transmisión de grandes volúmenes de datos a grandes distancias. Esto permitirá al Comandante o Jefe, inclusive en los más bajos niveles, tener la situación de sus fuerzas clara en tiempo real, permitiendo de esta manera contribuir a la adopción de decisiones correctas. Los mencionados dispositivos podrán ser satélites, aviones o vehículos terrestres no tripulados que podrán ser armonizados con los sistemas de armas desplegados y que hasta posibilitarán dirigir sus medios de lanzamiento, visualizar los efectos en el blanco, corregir errores, etc.

La actividad de sabotaje y espionaje que un hacker realizaba en forma manual hace algunos años, hoy puede ser efectuada por un virus informático. Éstos están programados para dañar una parte del sistema informático de una determinada organización, empleando características particulares del propio sistema para aumentar su subrepticidad e incluyendo contramedidas específicas para el antivirus que se utilice.

Esta característica permite que las tareas de Inteligencia se desarrollen en un marco adecuado para la consecución de sus objetivos. Armas digitales como troyanos, spyware *(3)*, spoofing *(4)* o snifes *(5)* entre otros permiten adentrarse en los sistemas adversarios y obtener información así como afectar el normal desempeño de sus equipos y redes.

La actividad de contrasabotaje y contraespionaje se desarrolla empleando distintos medios informáticos que permiten garantizar, en lo posible, el intercambio de datos seguros. Entre éstos se pueden nombrar el encriptado, la firma digital, los firewall, los códigos de seguridad *(6)*.

Internet podrá tornarse en una arma de guerra psicológica importante. Si bien son los países centrales (sobre todo los EE.UU.) quienes tienen todavía el control de la red, es poco probable que en épocas de conflicto la misma quede desarticulada en razón de la ventaja que representa su empleo. De hecho, en la actual guerra contra el terrorismo internacional, organizaciones como Al-Qaeda emplean la red con el fin de difundir información, adiestrar a sus agentes, captar seguidores, etc.

Medios para la obtención y transmisión de información.

Está claro que, como sabemos, todas estas actividades se pueden llevar a cabo durante tiempos de conflicto, pero sobre todo en épocas de paz, por lo que es necesario adoptar políticas que lleven a reducir la vulnerabilidad de los sistemas. Un aspecto a tener en cuenta en este sentido es la capacitación de los usuarios y administradores a los fines de evitar sobre todo los excesos de confianza. Una permanente evaluación de los sistemas permitirá, asimismo, una correcta evaluación y corrección de errores. Todo aquello que tenga que ver con la seguridad física de los medios, también contribuirá en este sentido. Por ultimo, una legislación adecuada creará un marco legal para permitir incluir cláusulas de confidencialidad en los contratos con posibles proveedores de hardware y software.

(3)
Los spywares o archivos espías son unas diminutas aplicaciones cuyo objetivo es enviar, a un lugar en el exterior, datos del sistema donde están instalados mediante la utilización subrepticia de la conexión a la red. Estas acciones son llevadas a cabo sin el conocimiento del usuario.

(4)
Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall.

(5)
Programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo, con el objetivo de conseguir alguna información.

(6)
Permiten la autenticación del usuario del sistema a través de la biométrica, con usuarios locales, o mediante el empleo de protocolos, con usuarios remotos.

Comando y Control

La era de la información ha creado una explosión en la cantidad de información que está (o estará) disponible para los Comandantes en todos los niveles. Algunos observadores opinan que, para el año 2010, éstos podrán contar con una cantidad increíble de información acerca de cada objetivo. Nunca lo sabrán todo, pero podrán percibir con más certeza la situación en su área de combate acerca del enemigo que en guerras anteriores. Con esta información, los Comandantes organizarán operaciones con precisión y velocidad sin precedente. Se aprovecharán de los adelantos revolucionarios en la transferencia de información, almacenamiento, reconocimiento y la depuración de información para dirigir ataques sumamente eficaces en tiempo real.

Cuarto de Operaciones del futuro.

El Comandante militar tiene que poder vivir en el futuro, entender el impacto de las decisiones que se toman hoy en el espacio de batalla de mañana. Mientras más jerarquía tenga el Comandante, podrá prever un futuro más lejano. Con base en su entendimiento, su capacidad de predecir los resultados de las acciones bajo estudio, los Comandantes en todos los niveles toman decisiones continuamente y deciden sobre los modos de acción. Esa capacidad surge años después de haber recibido entrenamiento, contar con una amplia experiencia y haber pasado por un proceso de selección. Sin embargo, inclusive los más avezados pueden analizar solamente dos o tres posibles modos de acción para todas las situaciones menos las más sencillas. Para lograr una elaboración adecuada de cada modo de acción, el Comandante tiene que tratar numerosos asuntos técnicos complejos, además de lidiar con características culturales, organización de las fuerzas enemigas, tecnología disponible por parte de éste, etc. Todo esto viene a colación de la enorme posibilidad que con los sistemas actuales cuenta el decisor ya que los mismos posibilitan hoy por hoy una capacidad de simulación enorme de manera que el Comandante puede visualizar mejor los futuros posibles que resultan de las acciones militares. Esa capacidad de simulación se ha denominado “espacio de batalla sintético conjunto”.

Posibles aplicaciones para el Comando y Control.

Sala de Comando y Control.

Sobre la base de esto podemos decir, con seguridad, que los próximos años darán testimonio del surgimiento de una tecnología que le proporcionará al Jefe de Unidad una capacidad de simulación sincronizada y real.

Por lo tanto, la tecnología de la información no sólo ha mejorado la lectura de la situación de los Comandantes en el campo de combate actual y futuro, sino que también ha aumentado la complejidad del entorno de la toma de decisiones.

Conclusión

La guerra informática constituye, hoy en día, una parte del conflicto armado que se encuentra en pleno desarrollo. Las investigaciones actuales, en el plano de la Defensa, apuntan a transformar tecnologías de informática en capacidades bélicas críticas en campos tales como señales, imágenes, inteligencia, fusión de información, gestión de información, computación avanzada, operaciones cibernéticas (empleo de robots) y Comando y Control.

Sin embargo debemos tener presente que el empleo de la informática en los conflictos armados, sobre todo por parte del terrorismo internacional, puede constituirse en un arma devastadora. El hecho de que se pueda sabotear, por ejemplo, un sistema de control aéreo de un aeropuerto o los sistemas de control de una central nuclear, nos da pie a imaginar que la guerra informática puede ser tan cruel como la guerra clásica y sus efectos tan terribles como los de ésta.

Por lo tanto se hace imprescindible el aprovechamiento de esta tecnología para proteger y atacar objetivos de carácter militar o no. Una de las ventajas es que puede contribuir a lograr la disminución de las capacidades de combate enemigas sin causar bajas propias, empleando distintos artilugios para afectar las comunicaciones, redes y equipos del adversario. Nuestra doctrina, entonces, tiene que estar a la altura de las circunstancias dado que, como consecuencia de la globalización, cualquier conflicto que se desarrolle en el mundo puede llegar a tener efectos inmediatos en el propio Estado.

Una adecuada política de seguridad informática de alcance nacional constituirá, entonces, el cimiento fundamental donde se apoyará el planeamiento de las acciones, tanto en tiempo de paz como de crisis, proveyendo las herramientas que posibiliten afectar la infraestructura informática enemiga a los fines de contribuir a quebrantar su voluntad de lucha. ■