La guerra de la información

El lado oscuro de la era de la información

Rafael Gomis Pardo
Comandante de Aviación
Roberto Pla Aragonés
Comandante de Aviación

La pasada fase de la civilización (algunas veces llamada de "baja tecnología"), con un alto grado de industrialización y en la que se producían y distribuían recursos naturales, da paso a una nueva era (llamada de "alta tecnología") en la que se produce y disemina información. En un mundo cada vez más global, las grandes redes de información, la mayoría de ellas basadas en ordenadores, acumulan, procesan y distribuyen información, que afecta a todas las personas y a todos los estamentos de la sociedad.

Las Fuerzas Armadas y en especial el Ejército del Aire se encuentran inmersas en esta "revolución de la información". Las redes y los potentes ordenadores, son un medio eficaz para acelerar nuestro propio ciclo de toma de decisiones (percibir, procesar, comparar, decidir y actuar), y mantenernos sobre el ciclo de decisión del enemigo, pero estas mismas redes se pueden volver en contra nuestra y explotar sobre nosotros y a nuestro alrededor, en algunos casos, de manera incontrolada (figura 1).

Irónicamente, este nuevo flanco de vulnerabilidad es un sub-producto del éxito alcanzado en la tecnología militar, que fue la primera en expresar su interés en el desarrollo de las redes.

LA DEFINICION

Este nuevo fenómeno se llama "Guerra de la Información" y las Fuerzas Aéreas de los Estados Unidos lo han definido como: "Cualquier acción para denegar, explotar, corromper o destruir la información del enemigo y sus funciones, protegiendo la nuestra contra sus acciones, y explotando nuestras propias operaciones de información".

La propia definición nos da dos vertientes en este nuevo tipo de "guerra", de las que hablaremos posteriormente, la parte ofensiva y la defensiva.

Ciertos aspectos de la IW (Information Warfare/Guerra de la Información) son tan viejos como la Historia, como por ejemplo atacar la cabeza del enemigo, la decepción en toda la amplitud de la palabra y las operaciones psicológicas. Sin embargo, otros aplican conceptos paralelos a la Guerra Electrónica, que alcanzaron un gran desarrollo durante la Segunda Guerra Mundial. La reciente automatización de los Centros de Mando y Control ha creado objetivos más vulnerables a las bombas lógicas y virus informáticos que a las bombas tradicionales.

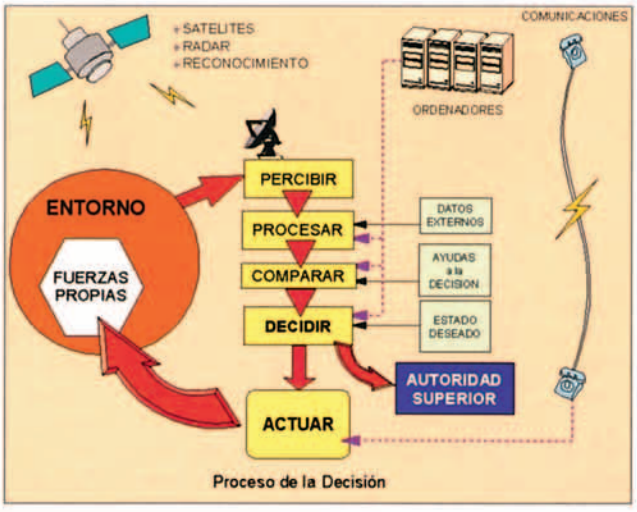
En las sociedades que caminan hacia esta era de alta tecnología, la importancia y frecuencia de este tipo de guerra, tanto contra sistemas civiles como militares, aumentará enormemente. Por supuesto, las operaciones psicológicas y de decepción también se transformarán hasta límites insospechados hace algunos años.

ALGUNOS CASOS

Por todos son conocidos las continuas intromisiones en sistemas, con más o menos inocentes intenciones, que se publican en los medios de comunicación; entre ellos podemos resaltar el de un muchacho argentino de 22 años, que hace aproximadamente cuatro años logró introducirse por medio de Internet en los ordenadores de la universidad de Harvard y a través de ellos en los ordenadores del Departamento de Defensa, departamento de Energía y NASA de los EE.UU., accediendo a información relativa a satélites, diseño de aviones y tecnologías radar.

El laboratorio Roma (New York), la principal instalación de desarrollo de Mando y Control de la USAF, fue atacada más de 150 veces entre marzo y abril de 1994 por dos "hackers" (en su versión de persona habilidosa con los ordenadores que realiza accesos no autorizados a los ordenadores) no identificados.

No menos asombroso es que durante el 11 de marzo del pasado año se recibieran 30.000 mensajes e-mail a través de Internet en Langley AFB, originados principalmente en Estonia y Australia, y que inundaron sus sistemas produciendo un bloqueo general, obligando a intervenir al "Air Force,s Computer



Proceso de la Decisión

Emergency Response Team", que ha conseguido, colocando múltiples filtros, que este tipo de correo descienda hasta aproximadamente 6.000 mensajes diarios, cantidad que se considera normal.

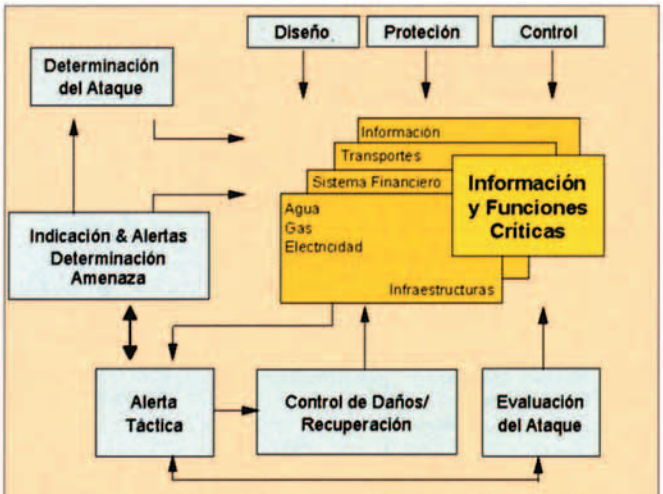
LA FACILIDAD DE OBTENER HERRAMIENTAS

Un CD-ROM titulado "The Hacker Chronicles, Vol II" y disponible por unos 50$, contiene cientos de megabytes de información para "hackers", incluyendo herramientas automáticas para entrar en ordenadores protegidos.

Su cubierta incluye este aviso: "... la información contenida es legal, pero su uso puede ser ilegal. El contenido tiene como único propósito la información y la educación. Toda la información contenida en esta compilación estaba legalmente disponible al público antes de esta publicación".

En Internet, mediante suscripción a listas de correo, lectura de grupos de noticias o acceso a páginas de hipertexto se pueden encontrar cientos de artículos y referencias sobre los más diversos métodos de asalto. Toda esta información es de libre acceso para quien disponga, en cualquier lugar del mundo, de un acceso a Internet.

Trasladando este problema a cifras, podemos decir que durante el pasado año, la agencia DISA (Defense Information Systems Agency), usando herramientas tipo "hacker" atacó 26.170 ordenadores del DoD (Departament of Defense) sin información clasificada. De ellos el 3,6% fueron facilmente atacados por la "puerta frontal", debido a que no se habían tomado las medidas de seguridad más básicas. El 86% pudieron ser penetrados explotando la relación entre ordenadores en redes. El 98% de las incursiones "NO" fueron detectadas por los administradores o usuarios de los ordenadores; en el 2% de los casos detectados sólo fueron denunciados el 5%. Este estudio estadístico demostró que durante 1995 se realizaron aproximadamente unas 200.000 incursiones en los ordenadores no clasificados del DoD de los EE.UU.



Estructura de las Acciones Defensivas en la Guerra de la Información (IW-D)

LA GUERRA DEL GOLFO

La Guerra del Golfo llevó al uso de la decepción de la información y la IW a su cenit. La cantidad de información no daba descanso a los miembros de la Coalición: 700.000 llamadas telefónicas, 150.000 mensajes diarios, gestión de 350.000 frecuencias y control de 2.240 salidas de aviones diarias por parte de los AWACS.

La operación "Desert Storm" dio al Pentágono la primera idea de como sería la guerra en el futuro. Uniendo entre sí técnicas de Guerra Electrónica, Guerra de Mando y Control, y operaciones psicológicas, la coalición lanzó un ataque contra el sistema de información iraquí que aceleró el final de la guerra. Los oficiales encargados del planeamiento de las operaciones militares identificaron 78 nodos del Sistema de Mando y Control iraquí que, siguiendo con la doctrina diseñada por el coronel John Warden III, materializaban los centros de gravedad del anillo central de la estrategia de la parálización. Fueron los primeros objetivos seleccionados. A los 28 minutos después del comienzo de la guerra, las unidades iraquíes estaban incomunicadas de sus cuarteles generales, sin inteligencia ni dirección. El ataque fue llevado a cabo mediante bombas y misiles; en el futuro podrían ser realizados mediante virus, bombas lógicas, saturando de información falsa los sistemas o alterando la información en ellos contenida.

El ataque alcanzó tal éxito que los oficiales americanos se plantearon qué hubiera pasado si Sadam Husein hubiera intentado lo mismo contra ellos, y en el estudio de sus defensas encontraron grandes deficiencias: necesidad de inteligencia más precisa, mejor interoperabilidad en las comunicaciones, mejores capacidades en equipos de navegación e identificación, mejores medios de reconocimiento, así como una defensa organizada de sus sistemas de información contra accesos incontrolados.

LA IW OFENSIVA

La parte ofensiva de la IW es muy atractiva para muchos, debido a que es muy barata en comparación con los costes de desarrollo, mantenimiento y uso de sofisticados sistemas de armas.

Esta parte de la IW, comúnmente llamada IW-O, incluye actos tales como el robo o la corrupción de datos, distribución de información errónea o falsa, denegación del acceso a los datos, y la destrucción física de discos, plataformas o edificios que sean parte del sistema de almacenamiento y distribución de datos.

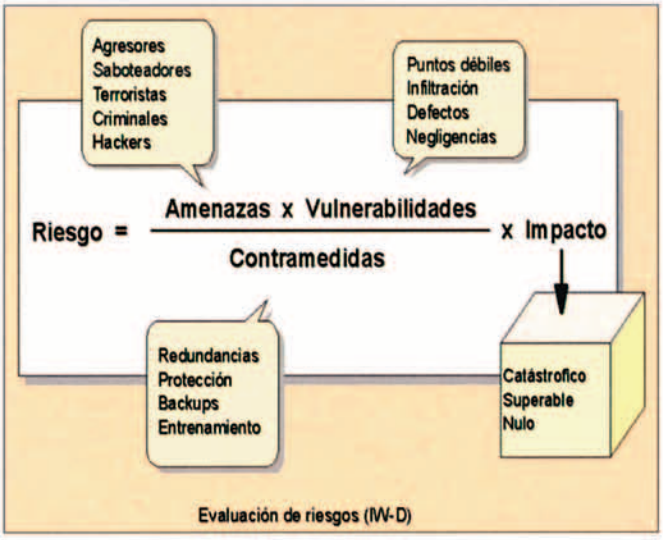
Mediante el soborno, chantaje o infiltración puede conseguirse la colaboración de un usuario autorizado del sistema que genere falsa información, manipule la existente o introduzca "bombas lógicas" en los sistemas de información conectados a la infraestructura global de comunicaciones.

LA IW DEFENSIVA

La IW-D utiliza medios como detectores y eliminadores de virus, encriptación y protocolos de autenticación y certificación de la información para prevenir la IW-O, así como controles de acceso (desde la simple palabra clave hasta complejos ordenadores especializados en el filtrado de accesos, llamados "cortafuegos" o sofisticados programas de análisis de protocolos de

comunicaciones). La IW-D también comprende el planeamiento y ejecución de las actividades necesarias encaminadas a paliar los efectos de un ataque de IW.

Es importante resaltar que las inversiones en esta faceta de la IW no están en correlación con las que se deben hacer en la parte ofensiva para alcanzar un mismo grado de capacidad. El valor de la inversión no está en función de la información o sistemas de información a defender, sino en función de la importancia que tiene para el defensor la información que contiene o el proceso de información que realizan esos sistemas y que pueden estar sujetos a un ataque.



Evaluación de riesgos (IW-D)

Si el defensor deja desprotegidas funciones vitales tanto sociales como económicas o defensivas que dependen de servicios de información, está invitando a potenciales enemigos a hacer la inversión necesaria para obtener sistemas para atacarle esas funciones. Para disuadir a un posible atacante se deben establecer, y demostrar que se poseen, robustos sistemas para proteger y en su caso restaurar las funciones y procesos esenciales.

LA AMENAZA

Las organizaciones económicas y comerciales son bien conscientes de este peligro, ya que poseen la experiencia que han adquirido al ser víctimas de fraudes, robos y sabotajes. Ello les ha forzado a tomar medidas para proteger sus cuentas, y en definitiva, su capital. Por otra parte el inmenso potencial de negocio que puede suponer el comercio a través de la red Internet está forzando a desarrollar sistemas de transacción seguros, no tanto porque no existan ya varios de ellos, sino por la dificultad de acuerdo que suponen los altísimos intereses en juego a la hora de establecer una estandarización.

Desde el punto de vista de la sociedad y de la defensa, los ataques al sistema financiero pueden suponer una grave amenaza sobre la logística de las Fuerzas Armadas. El espionaje industrial puede afectar a los sistemas utilizados por la defensa y los ataques a ordenadores privados pueden suponer precedentes para el asalto a sistemas militares, que en muchas ocasiones usen los mismos equipos, sistemas operativos y protocolos.

No olvidaremos aquí la amenaza física, por constituir un aspecto sobradamente conocido el tema, que comprendería la destrucción física de equipos o redes de comunicaciones.

El riesgo debe ser gestionado protegiendo partes seleccionadas de la infraestructura que soporte las funciones críticas y las actividades necesarias para mantener los intereses políticos, militares y económicos (figura 2).

La evaluación del riesgo para nuestro país es una de las primeras tareas a realizar. En el campo de la infraestructura civil, la red eléctrica y otros servicios cuentan con sistemas de monitorización de fallos y control remoto, que podrían ser afectados por acciones de IW-O. El sistema financiero, se basa en la red IBERPAC, de la compañía telefónica, para sus operaciones internas y numerosos bancos empiezan a abrir a sus clientes la posibilidad de operar a través de Internet, un sistema revolucionario en Europa y en el mundo, que permite el acceso a cualquier ciudadano a la red a precio de llamada local.

En el campo de la defensa, la red SCTM (Sistema Conjunto de Telecomunicaciones Militares) todavía no ha sido completada en todos sus tramos, aunque va aumentando el grado de integración con las redes preexistentes, como la Red de Microondas del Ejército del Aire y la Red Territorial del Mando del Ejército de Tierra, a las que en un futuro debe englobar. Aunque la SCTM se ha diseñado poniendo especial énfasis en su capacidad de supervivencia, mediante la duplicación de los tramos más críticos a través de diferentes medios (radioenlaces, líneas punto a punto o vía satélite) no puede descartarse un acceso ilegal, que podría producir un grave impacto en los sistemas que apoyan sus telecomunicaciones, como el sistema SADA, los enlaces con el sistema de Defensa Aérea francés, la información del tráfico aéreo civil o las comunicaciones con los organismos OTAN.

Desde el punto de vista físico estas redes tienen "cuellos de botella" o nodos críticos, que en caso de ser suprimidos afectarían gravemente a su operatividad. La única protección posible contra este riesgo es la duplicación de los caminos físicos, contemplando incluso la utilización de líneas comerciales, con un sistema de encriptación adecuado, para evitar la mayor posibilidad de un acceso incontrolado en estas líneas menos seguras.

LA ORGANIZACION

Lejos de "militarizar" los aspectos relacionados con la seguridad informática, decretando restricciones difíciles de hacer cumplir, una organización efectiva en el campo de la IW debe estar formada por equipos de personas con acceso fluido a las últimas novedades en el campo de la seguridad de sistemas informáticos, protocolos y redes de comunicaciones y que deberán trabajar en estrecha colaboración con las empresas desarrolladas de estos sistemas y los usuarios de los mismos, los laboratorios de investigación y los centros de estudio.

También es cierto que si bien la defensa en este campo no puede ser exclusivamente militar, sí es conveniente que las Fuerzas Armadas cuenten con

personal especializado, capaz de desarrollar, en un momento determinado, las acciones ofensivas o defensivas necesarias, así como la supervisión diaria de los sistemas de información militares y su seguridad.

La organización deberá ser capaz de asegurar: alerta táctica, control de daños, localización de ataques y restauración de la situación normal. La alerta táctica incluye la monitorización, detección y comunicación de ataques o incidentes, y ello sin duda, requiere iniciativas en la política, clarificaciones legales y programas de investigación y desarrollo. Las funciones básicas de monitorización, detección, control de daños y restauración, deberán encontrarse al nivel operativo más bajo posible (figura 3).

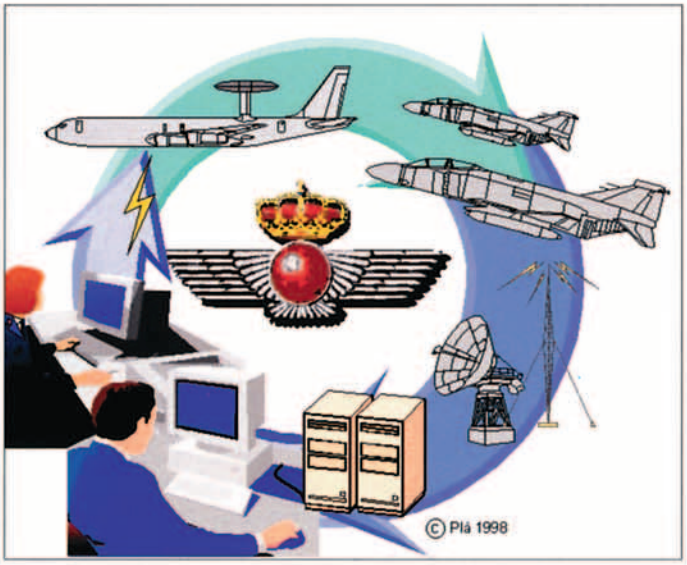
LOS PASOS A SEGUIR

Las primeras medidas han sido adoptadas por parte de los responsables de la informática de gestión en el Ejército del Aire, éstas son tan sencillas como la adopción de unas normas que prohiben el uso de aplicaciones de software no autorizado, establecen unos estándares de material y unos sistemas de protección contra ataques de virus, primer paso para la adquisición de una cultura de seguridad informática por parte de los usuarios, auténtica base y requisito imprescindible para establecer una defensa de nuestros sistemas.

Toda vía de comunicación constituye un camino de invasión. Aunque cierto, este argumento no parece que deba aconsejar un aislamiento total como mejor sistema defensivo. Es claro que aquellos ordenadores que permanecen aislados físicamente son evidentemente poco vulnerables a otro ataque que el convencional, pero ni la sociedad ni sus fuerzas armadas pueden aislarse por completo prescindiendo de las ventajas que puedan obtener de las redes de comunicaciones. Este aislamiento sería una forma de ignorar un problema, no de solucionarlo.

Además de las medidas físicas y lógicas que se adopten, debe realizarse un esfuerzo de formación, dirigido a todos los usuarios de sistemas, para crear una conciencia de "Seguridad Informática" en cuanto a conocimiento de su sistema, protección del mismo, discreción sobre sus características y sistemas de protección.

Para que esto se pueda realizar, deberemos seleccionar y formar adecuadamente al personal que formará parte de lo que podría ser el "Equipo de respuesta en caso de crisis" y que establecerá un contacto contínuo con las fuentes de información, civiles y militares, tanto nacionales y aliadas como otras fuentes exteriores en colaboración con los organismos de inteligencia adecuados.



LAS PRIMERAS UNIDADES

Dentro de las Fuerzas Armadas, el Ejército del Aire, por su nivel tecnológico y su dependencia de las redes de comunicaciones, tanto para el cumplimiento de su misión como para la selección de objetivos, basada en inteligencia obtenida a través de sistemas de información, debe ocupar una posición preeminente en la organización de "Escuadrones de Guerra de la Información", de la misma forma que es un referente claro en los temas de Guerra Electrónica.

Estados Unidos creó en 1996 su primer Escuadrón de Guerra de la Información, el 609th IWS (Information Warfare Squadron), ubicado en Shaw AFB (Carolina del Sur) enfocado principalmente a la defensa y recuperación de sistemas de información, y en principio sin atribuciones en lo relativo a IW-O. Por otra parte, en abril de 1997 se abrió el Information Warfare Training Laboratory en Goodfellow AFB (Texas), con el objetivo de entrenar personal de inteligencia capaz de combatir este nuevo tipo de guerra.

LA CONCLUSION

El contenido de este artículo pretende dar a conocer un nuevo campo de actuación que se abre ante nosotros, y que sin duda dará mucho que hablar en un futuro no muy lejano. El Ejército del Aire no puede mantenerse ajeno a la nueva amenaza ni a este nuevo tipo de guerra, que ya se considera, por algunos expertos, como la guerra del siglo XXI.

La primera necesidad del EJército del Aire es establecer un "punto focal" para la coordinación de todos los aspectos relativos a la IW, posteriormente y como consecuencia de profundos estudios se podrían adoptar medidas tales como la formación de una organización y un centro para la IW-D, que deberá realizar el planeamiento y la coordinación, así como la creación de un organismos de control de sistemas, redes y diseño de infraestructuras y por último, el establecimiento de un equipo de respuesta en caso de crisis. El camino a recorrer es largo y los pasos intermedios muchos, pero el Ejército del Aire posee medios y personal con capacidad y cualificación para dar el primer paso.

Como conclusión final, podemos transcribir una frase del jefe del Estado Mayor de la USAF: *El dominio del espectro de la información es tan crítico en los conflictos actuales, como ocupar la tierra o dominar el espacio aéreo lo fueron en el pasado.* ■