LAS OPERACIONES DE INFORMACION

General (R) Evergisto de Vergara

Todo el arte de la guerra
se basa en el engaño

Sun Tzu

Las decisiones que se toman en un conflicto de intereses que implica el uso violento de los medios a disposición de un Estado requieren el uso de información para decidir las acciones que van a tomarse. Los bandos involucrados tratarán de ocultar su propia información y la forma en que la obtienen, y confundir al bando opuesto sobre la propia. De esa forma, se involucran no solo en la información necesaria para determinar blancos y precisar daños, sino también en lo que se conoce como velo (ocultar, disfrazar) y engaño (hacer algo para simular o fingir lo que no es), a fin de que la mente del decisor oponente tome una decisión equivocada.

El uso de la información puede estar dirigido a informar o a desinformar. Desinformar significa *Dar información intencionadamente manipulada al servicio de ciertos fines*. Además de la tecnología, interviene la inteligencia humana que hace uso de sus resultados.

La competencia en este campo se denomina *Operaciones de Información*. El objetivo es conseguir una ventaja competitiva sobre un oponente. Las operaciones de información son un mosaico de acciones para afectar la capacidad de lucha: puede consistir en recolectar información, confirmar la veracidad de la información propia, distribuir propaganda o desinformación para socavar la moral, afectar la calidad de la información que obtenga el

oponente o negarle la recolección, y otras formas. Vulgarmente, se identifica a las Operaciones de Información únicamente a actividades electrónicas de escucha, pero es un concepto muy incompleto.

Como se lee en el epígrafe, las Operaciones de Información están indisolublemente unidas a las guerras desde hace largo tiempo. El concepto se transformó más popular a partir de mediados de la última década del S XX, debido a los adelantos tecnológicos que permitieron obtener y usar información en provecho de los propios intereses, y para obstaculizar los del oponente.

En este ensayo se denominará aquí como Operaciones de Información a aquellas que se caracterizan por una lucha sobre los sistemas de información. Así entendida, las operaciones de información se enlazan con lo que se conoce como Revolución en Asuntos Militares, entendiendo como tal la influencia de la tecnología en la forma de hacer la guerra. El estudio de la historia militar demuestra que la naturaleza, el propósito y la forma de hacer la guerra cambian según lo haga la tecnología.

Existen varias formas de lucha sobre los sistemas de información, y todas son consideradas esencialmente un solo tipo de lucha. Las técnicas de las Operaciones de Información se consideran aspectos de una única disciplina. Bien dominadas, estas técnicas darán una ventaja decisiva sobre los oponentes y quienes no posean tal dominio, se encontrarán en una desventaja considerable sin que se tenga en cuenta principalmente la fortaleza física únicamente militar. El tema pasa por ordenar el pensamiento para identificar las formas que adopta esta guerra de la información. Algunas se refieren a aspectos estrictamente militares de las luchas tradicionales o convencionales; otras, a las características de las denominadas como *guerra sin restricciones*. De cualquier forma, el uso de las tecnologías de información es de naturaleza dual, tanto civil como militar, por lo que es difícil establecer límites precisos o definir incumbencias y responsabilidades de sectores del poder nacional para su control y uso. Las operaciones de información integran los diferentes sectores de la estrategia general de un país, aunque reconozcan un uso común de esa tecnología.

Todo pasa por poner en orden las ideas y tratar de identificar las diferentes formas de llevar a cabo Operaciones de Información. En definitiva, cualquiera sea su forma, todas persiguen evitar que el oponente reaccione en forma unívoca, y se genere confusión en una organización que será más peligrosa, cuanto más monolíticamente actúe. Luego, todo lo que se exprese en este ensayo debe ser interpretado con una advertencia: no se debe buscar una definición ideal. Lo que se expresa aquí divide un asunto muy amplio en partes concretas, pero siempre es mejor considerar que las Operaciones de Información es un mosaico de formas, antes que formas particulares aisladas.

Cuando se estudian las operaciones de información, se lo hace en forma vaga y generalizada. El propósito de este ensayo es poner en orden al pensamiento, para poder discernir mejor.

Una categorización del pensamiento para entender mejor.

Desde los puntos de vista expresados, las Operaciones de Información cumplen una función diferenciada en un conflicto. Si se toma como categoría de orden el efecto que producen, pueden identificarse cuatro formas de Operaciones de Información: sobre el comando y control; sobre los datos para el mejor desarrollo de las operaciones en el terreno; sobre los medios electrónicos que se usan; sobre la mente de los individuos en sus diferentes roles; y sobre los medios cibernéticos. Todas estas formas se llevan a cabo para facilitar las propias operaciones, y para dificultar las del oponente, y se llevan a cabo en los ámbitos físicos, informativos y los pertenecientes al conocimiento individual. Estas clasificaciones no son absolutas, en muchas partes estas categorías se superponen y es por eso que es difícil encontrar una definición ideal.

Las operaciones sobre la función Comando y Control.

Si se toman las Operaciones de Información destinadas a disminuir la capacidad de lucha del oponente, la primera de ellas es antigua y consiste en eliminar o interferir gravemente la estructura de comando del enemigo. Eso va desde eliminar físicamente al comandante enemigo hasta la destrucción de los Centros de Comando. La eliminación física del Comandante enemigo es vieja en la historia, y perdura hasta nuestros días: desde que Judith cortara la cabeza a

Holofernes, para que al día siguiente los asirios se desbandasen despavoridos [Santa Biblia, Judith, 13], hasta la eliminación de Bin Laden en el S XXI.

No obstante, más importante que la destrucción física del Comandante, siempre ha sido más efectiva la destrucción de los centros de comando. Aunque es natural que concentrar las estructuras de comando en un espacio reducido es una vulnerabilidad muy grande, todos los intercambios de información que involucren dirección y decisión tienden a concentrarse en espacios reducidos. Hoy los centros de comando son relativamente fáciles de identificar, porque tienen aparatos de comunicaciones y computación visibles asociados a emisiones electromagnéticas, y por el movimiento físico de personas, partes y papeles y toda clase de insumos.

Ni las bombas convencionales ni los ataques físicos de Fuerzas Especiales no son la única manera de destruir un centro de comando. Los sistemas de comando y control pueden ser inhabilitados si se les corta la energía, si se los interfiere electromagnéticamente o si se les importa *malware* en sus sistemas cibernéticos. A pesar de ello, ninguno parece ser más importante que la destrucción física, ya que la mayoría de las armas denominadas *blandas* requieren conocer la exacta ubicación del centro de comando en el terreno. ¿Por cuánto tiempo más los centros de comando van a ser tan fácilmente identificables? Los centros de comando pueden ocultarse en refugios de concreto, pero eso les disminuye sustancialmente la movilidad. Se puede achicar el tamaño de las computadoras, las emisiones de comunicaciones enmascararse electrónicamente, o reemplazarse por una red redundante de cables o *relays* de trasmisión fuera de la vista. Todas las redes generalmente pueden descentralizarse. Las reuniones pueden reducirse por video conferencias en línea. La energía eléctrica puede ser provista o suplementada por generadores, o por energía proveniente de células solares dispersas, de forma tal que no revelen la ubicación del centro de comando. Estos medios significan que un centro de comando puede ser no diferenciado de cualquier otro espacio habitado. Si se fracasa en este ocultamiento, el grado que una instalación de comando pueda ser dañada dependerá de la existencia de una arquitectura de nodos de reemplazo.

Una forma de ocultar los centros de comando que abunda en las guerras de cuarta generación es ocultarlas bajo instalaciones civiles, ya sea escuelas u hospitales. Esto no se permite en el Derecho Internacional de los Conflictos Armados porque vulnera el principio de discriminación. Usar a no combatientes para propósitos militares se denomina perfidia. No obstante, la experiencia muestra que se hace con mucha frecuencia.

Reconfigurar un centro de comando concentrado en un área a uno disperso, cuesta tiempo y dinero e incrementa las dificultades de comando. Los que propongan dispersión tendrán que convencer a los comandantes que dispersar el centro de comando será una medida necesaria y suficiente como para protegerlo. Esto va a depender de la sofisticación tecnológica, la percepción de vulnerabilidad y la autoridad que el comandante decida descentralizar. De cualquier forma, si bien es importante, todo indica que no podría basarse una estrategia solamente en el supuesto que el comando y control del enemigo será severamente afectado. Eso será solamente una preparación para operaciones posteriores, una vez que el oponente esté confundido.

Probablemente las posibilidades de obtener tal estado final deseado se incrementarán si la cultura militar del enemigo en la micro administración, opuesta a la iniciativa de los comandos subordinados. La influencia potencial de las guerras de Comando y Control descansa en la arquitectura de las relaciones entre los atacados. En culturas militares que restringen ampliamente la iniciativa, cortar los delgados lazos entre la cabeza y el cuerpo puede fácilmente inmovilizar al cuerpo. Pudo verse en la Guerra del Golfo en el bando iraquí, donde la ausencia de órdenes motivó la parálisis de las tropas desplegadas en el terreno, sin que mostraran ninguna respuesta creativa. Un oponente rígido y sin iniciativa es una de las posibilidades de éxito.

No obstante, otras culturas militares fomentadas en época de paz pueden permitirles más autonomía a los comandantes locales. La del otro extremo a la cultura restrictiva es la que permite a los subordinados mayor autonomía dentro de la intención del Comandante supremo. Un caso paradigmático es el de las tropas de Vietnam del Norte, organizadas muy jerárquicamente pero en sus operaciones gozaban largos períodos sin ataduras. Eso permitió el ejercicio de iniciativa que compensó las fallas propias de una carencia de coordinación que podía haber resultado de la ausencia de conducción central. Se dice que en la contracara, los oficiales

de Estados Unidos desplegados en el terreno luchando contra el Vietcong deseaban fervientemente que se cortaran las comunicaciones entre ellos y Saigón, o al menos las comunicaciones entre Saigón y Washington. Una cultura militar burocrática antes que las tecnologías, va a determinar el grado de vulnerabilidad de cualquier sistema de pasaje de información.

Desde mediados del S XIX las redes militares han sido montadas sobre comunicaciones telefónicas, y desde comienzos del S XX, sobre comunicaciones radioeléctricas. Interrumpir estas líneas de comunicaciones es algo antiguo: lo que es nuevo es el actual volumen de comunicaciones en la era de la información. Cortar los enlaces de comunicaciones requiere conocer de qué forma se comunica el oponente. Si la arquitectura es alámbrica, los nodos son más difíciles de detectar en su tráfico, pero más fáciles de detectar en sus instalaciones, y más vulnerables. Como en todos los centros de comando, los sistemas de comunicaciones son alimentados por generadores, o por tuberías de gas. Si la arquitectura es electromagnética, frecuentemente los nodos claves son visibles, por ejemplo las torres de microondas. Si se usan satélites para las comunicaciones, se las puede interferir, distorsionar o anular. En teoría, el Derecho Internacional impide que el espacio sea usado con fines militares, pero se discute si usar satélites como medios de comunicaciones con propósitos militares, no necesariamente bélicos, está o no permitido.

El impacto del ataque depende del adelanto tecnológico que tenga el oponente: una grilla de comunicaciones compuesta por muchos elementos pequeños – mayor adelanto tecnológico - irradia menos y es menos fácil de detectar en el terreno que una compuesta por elementos más grandes. La grilla pequeña ofrece la posibilidad de implementar sistemas redundantes, y confunde al proceso de selección de blancos del enemigo. La redundancia es un atributo que no solo poseen los países desarrollados: cuando finalizó la Guerra del Golfo donde el primer Plan de Operaciones consistía en destruir las instalaciones de comando y control iraquíes, los aliados se dieron cuenta que quedaban más que los iniciales, a pesar del número que destruyeron. No obstante, parece ser que los iraquíes tenían muchos sistemas de comunicaciones, más aún de los que conocían, desde sistemas de radio hasta de contratistas de petróleo occidentales que habían dejado en el lugar líneas telefónicas rurales que unían a las principales ciudades.

Claro que esto fue una redundancia de medios accidental, que es menos eficiente que una redundancia de medios deliberada. Los sistemas que replican el tráfico de mensajes multiplican la probabilidad que el mensaje llegue a su destinatario altamente degradado, y pueden reducir la capacidad global del sistema. Esta redundancia puede ser protegida, ya sea mediante tecnologías que eliminen errores en un ambiente de gran interferencia, o técnicas sofisticadas de corrección de errores usando códigos preestablecidos. De cualquier forma, una estrategia de redundancia cibernética de medios abre la posibilidad de tener que administrar para distinguir los bits vitales de los meramente útiles.

Al igual que se dice entre la diferencia de causar heridos o muertos, dado que los heridos generan una gran impedimenta logística, quizás el ataque sobre el comando y control pudiera rendir mejores frutos si se degrada a los sistemas y no se los destruye totalmente. Si se destruyen canales de comunicación seguros, eso va a inducir al uso de canales menos seguros y eso generará demoras en la reacción, permitiendo obtener un *tempo* para el atacante.

Las guerras por el Comando y Control dentro de las Operaciones de Información es un aspecto valioso en las operaciones militares. La revolución en tecnologías de información permite ahora reducir la vulnerabilidad de los centros por la duplicación de los sistemas, y ahora no puede asegurarse que todos los centros de comando puedan ser destruidos en el primer intento.

Las operaciones para obtener información y llevar a cabo operaciones.

Este tipo de Operaciones de Información es la más conocida, y se dirige esencialmente a la obtención de blancos y la evaluación de daños. La proliferación de sensores más exactos, de diferentes tipos y en cantidades capaces de alimentar con datos a los sistemas de control de fuego permite hacerlo en tiempo real. En este sentido, tiene más ventajas que los informes humanos porque permite obtener datos más exactos y desapasionados, pero tienen el inconveniente que pueden ser electrónicamente engañados. El conocimiento profundo de cómo funciona estos sistemas permite que se ponga en funcionamiento la creatividad humana.

Una vista rápida a los diferentes sensores disponibles permite identificar a cuatro tipos: *sensores en puntos lejanos* (la mayoría en el espacio, pero también existen sísmicos y acústicos); *sensores en puntos cercanos* (RPVs con radares de microondas pasivas, y con artefactos de inteligencia electrónica); *sensores en el lugar* (acústicos, bioquímicos, ópticos) y *sensores de detección de armas* (infrarrojos, de alcance, de detección de luz o de pintura). Esto muestra la complejidad de las tareas de engaño, porque éstas pueden funcionar contra uno o dos tipos de sensores, pero no contra una integración completa de los diferentes tipos. Por ahora la integración es manual, y el desafío es integrar los diferentes tipos de sensores en forma automática.

Las Operaciones de Información defensivas basadas en la inteligencia son desarrolladas para preservar la invisibilidad, o por lo menos ampliar la distancia entre la imagen y la realidad del campo de combate, es decir evitar la información en tiempo real. Los sensores montados en avión, el más conocido el AWACS que ya tiene más de 30 años de antigüedad permiten realizar un seguimiento de los vehículos terrestres y de algunas aeronaves, y recoger y trasmitir imágenes a los comandantes tácticos. Existen diferentes tipos de aeronaves donde se muestran estos radares de inteligencia, reconocimiento, adquisición de blancos y vigilancia. Brasil los tiene montados en aviones Embraer, aunque en el mundo occidental, la mayoría se encuentran montados en aviones Boeing. Por supuesto que estos sensores son costosos, y sería mejor usar sensores más baratos.

Además de ser costosos, esto sensores pueden ser atacados de una manera barata, inhabilitando los sistemas que usan mediante virus informáticos, o anulándolos o corrompiéndolos mediante recursos de guerra electrónica. Muchos arguyen que la diseminación de medios técnicos hasta el soldado individual puede crear una gran vulnerabilidad porque si es capturado, revelará la capacidad de guerras de la información que se tiene, revelará la forma en que se obtiene y aún peor, los lugares sobre los que no se puede obtener información y donde se puede actuar sin peligro. De cualquier forma, cuando la lectura técnica de un sensor sea precisa y exacta, las contramedidas que se puedan tomar consistirán en distorsionar lo que los sensores

leen, y lo que los sensores concluyen. El ingenio humano tiene un amplio campo de acción aquí, ambos en el encubrimiento y en el engaño.

En los ambientes de alta densidad como las áreas urbanas o las selvas, las mejores estrategias de encubrir y negar información sobre lo que en realidad pasa es explotando o multiplicando el desorden y la confusión. Aunque se corra el riesgo de vulneración del DICA, hay muchos casos en los que los elementos militares han buscado confundirse con elementos civiles. La adhesión irrestricta de evitar daños colaterales según rijan RDE aumentará la capacidad de velo y engaño de las propias operaciones. Estas estrategias de velo y engaño han sido ampliamente aplicadas por los árabes de Irak, Pakistán y Afganistán. Los señuelos tendrán gran aplicación, siempre sosteniendo la teoría que es más fácil esconder un árbol dentro de un bosque, que rodeándolo con una pared.

El concepto principal es que cualquiera sea la información que puedan detectar los sensores en sus diferentes formas, siempre deberán ser comparados con otros, la información deberá filtrarse, y siempre se dudará de su confiabilidad. El hombre deberá decidir cuál información es confiable, cuál no lo es, y decidir cuál es el daño colateral de cualquier contramedida que se tome.

La tecnología de la información puede ser valiosa en la adquisición de blancos, y cuando sea preferible usarla en vez de hacerlo mediante adquisición directa. Sin embargo, todavía no está claro que aquel bando que tenga tecnologías de información avanzada pueda superar al bando que posea tecnología inferior. El ingenio humano es inagotable.

Las operaciones sobre las emisiones electrónicas.

Las dos primeras formas de Operaciones de Información tratadas hasta aquí son ataque a sistemas (información de Comando y Control) o por sistemas (información para las operaciones). La tercera forma es la información electrónica o técnicas operacionales: las radioeléctricas y las criptográficas. Luego, este tipo de Operaciones de Información es del reino de las comunicaciones. La guerra electrónica intenta afectar las bases físicas para transferir la información, en tanto que la guerra criptográfica trabaja entre dígitos binarios (bit, la unidad

básica de información en computación y telecomunicaciones) y bytes (múltiplo del bit, y byte=8 bits).

Las técnicas antirradar pueden asimilarse a técnicas contra sensores (por ejemplo el uso de bengalas para confundir misiles guiados infrarrojos, o el uso de chaff para confundir el guiado de misiles). La característica de un radar es que recibe ondas reflejadas, en vez de radiación electromagnética pasiva. Por lo tanto, las ondas de radar pueden ser atacadas cuando se emiten y cuando se reciben. Una gran cantidad de la comunidad de Guerra Electrónica trata con radares de adquisición y de tiro. Aquí la máxima preocupación es la interferencia y la contrainterferencia. Los radares tradicionales generan una señal con una frecuencia. Si se conoce la frecuencia, es más fácil interferirlo. Los radares más modernos saltan de una banda de frecuencia a otra. Para atacar un radar, hoy los que deseen interferir deben ser capaces de adquirir la señal entrante, determinar su frecuencia, sintonizar la emisión de la señal de interferencia conforme a eso y enviar un enturbiador de señal lo suficientemente rápido para minimizar la longitud y la intensidad de la señal reflejada.

Para poner un ejemplo, un sistema de defensa aérea funciona conectando los radares de adquisición con los radares de tiro. Un radar de adquisición puede basarse en la detección de ecos o de frecuencias. Cuando un avión se encuentra dentro del alcance de un radar de adquisición, se enciende una luz de advertencia en el tablero del piloto. Si el operador de defensa aérea deja aproximar a un avión enemigo sin encender el radar de adquisición, y recién lo hace cuando está claramente en alcance, simultáneamente activará el radar de tiro y el avión no tendrá tiempo de escapar. La frecuencia de un avión comercial es diferente a la de de un avión de combate. Solo basta encontrar el método para anular la detección de tal frecuencia en los radares de adquisición para que las piezas antiaéreas no disparen. Por otro lado, los ecos de radar pueden ampliarse en *drones*, si se les coloca micrófonos. Tal treta la aplicaron los israelíes en el bombardeo a la defensa aérea del valle del Beeka: enviaron drones con micrófonos en las alas para que los radares sirios los detectasen como aviones reales de combate, hacia allí apuntaron automáticamente las piezas, en tanto que los aviones de combate reales venían rasante a tierra desde direcciones opuestas. Solo era necesario conocer si los radares de adquisición trabajaban por ecos o por frecuencias.

Aviones de interferencia electrónica que vuelen integrados en formaciones de aviones de ataque frecuentemente borran las señales de retorno (la que se debilita engañando sobre la distancia entre el blanco y el radar) mediante el fortalecimiento de esas señales, pero al hacerlo se hacen muy visibles y se transforman en blancos. Los misiles anti radar aire- tierra como el HARM (High Speed Anti Radiation Missile) y el renovado AARGM (Advanced Anti Radiation Missile) obligan a que los radares se apaguen, o se enciendan y apaguen en cortos lapsos. Igualmente, a pesar de la tecnología y los avances de la digitalización, el ingenio humano puede superar obstáculos penados como insalvables. Los radares de adquisición de blancos y de dirección de tiro están enlazados. Así, las piezas se apuntan automáticamente según las señales del radar. Si los radares de adquisición detectan los aviones de ataque según su frecuencia, solo habría que "borrar" por algún medio en esos radares de adquisición la detección de esa frecuencia. Luego, el sistema de tiro de la defensa aérea estaría anulado.

Es de esperar que en el futuro, las frecuencias emisoras de los radares sean más complejos y proliferarán para hacer más difícil la tarea de los misiles antirradar, que se transformarán en artefactos caros. Las frecuencias receptoras se volverán más complejas y por tanto menos vulnerables, y eso ocasionará que los radares no sean considerados blancos tan importantes como hasta ahora.

La guerra electrónica contra las comunicaciones generalmente es más difícil de llevar a cabo que la guerra electrónica contra radares. El concepto inicial es que las radios trabajan en diferente tipo de modulación, y hay algunas que son más seguras que otras. Los sistemas VHF son más difíciles de interceptar que los BLU, pero tienen menos alcance.

Las señales de comunicaciones se debilitan con la distancia. Mientras los radares tratan de iluminar el blanco, (y por lo tanto envían una onda hacia los artefactos del otro bando), las comunicaciones tratan de evitar el otro bando por completo y por tanto, apuntan en direcciones específicas del espectro electromagnético donde el oponente no puede actuar. Las comunicaciones se mueven hacia saltos de frecuencia, espectros ensanchados y la tecnología de

canales de División de Código de Acceso Múltiple (CDMA por sus siglas en ingles), que son difíciles de interferir e interceptar.

Uno de los conceptos en la comunicación de datos es la idea de permitir que varios trasmisores envíen información simultáneamente sobre un único canal de comunicación. Eso permite a varios usuarios compartir una banda de frecuencias. A este concepto se lo denomina acceso múltiple. La CDMA emplea la tecnología de espectro ensanchado y un esquema de codificación especial para permitir que múltiples usuarios usen el mismo canal físico. Aquí la señal modulada codificada tiene un ancho de banda de datos mucho mayor que si se dividiese la modulación en tiempo o por frecuencias.

Las Operaciones Electrónicas también son usadas para ubicar geográficamente al emisor. Cuanto más ruidoso sea el ambiente, va a ser más dificultosa esta tarea. Una manera de defenderse es multiplicar las fuentes emisoras, o dispersar los medios. En el S XXI han aparecido misiles denominados "inteligentes" con capacidad de ubicar fuentes de emisión electrónica. También ha hecho su aparición el GPS (Global Positioning System) que permite ubicar coordenadas que pueden introducirse en la base de datos de los misiles. El talón de Aquiles de los sistemas de comunicaciones distribuidos es que requieren enlaces de comunicaciones entre sensores, sistemas de comando y armas dispersas. Estos enlaces son los que hay que atacar.

Aunque el hecho está todavía no completamente aclarado por ser la información clasificada, se dice que el líder guerrillero de las FARC Raúl Reyes fue abatido en mayo de 2008 en territorio ecuatoriano, cuando un misil se "montó" en las emisiones de su teléfono portátil. Esto no ha sido confirmado.

En cuanto a la criptografía, mezclar el contenido de los propios mensajes y ordenar los del otro bando es la quinta esencia de las Operaciones de Información: Aunque la criptografía continúa atrayendo a las mejores mentes en matemáticas, lamentablemente para una historia larga y gloriosa, los éxitos en este asunto pronto revestirán solo interés histórico. Hoy, descifrar mensajes generados por computadoras es casi imposible. Una prueba casera de ello es el

navegador *google*, o los navegadores de páginas web denominados "seguros" que comienzan su URL con https:// Con motivo de las precauciones contra ataques terroristas, el gobierno de EEUU pidió a *google* su codificación, lo que fue negado por la empresa con el argumento que vulneraría las libertades individuales. Cuanto más barata sea la codificación, y más profusas las técnicas de esconder señales como saltos de frecuencia, o espectro ampliado, será más difícil descifrar mensajes cifrados.

Aparte de estas dificultades en la codificación, ahora ha tomado auge tecnologías de firma digital para conocer el grado de seguridad de quien envía un mensaje.

Las operaciones contra la voluntad de lucha.

La información dirigida contra la mente humana se denominan acciones psicológicas. Hay tres categorías de acciones psicológicas: 1) Operaciones contra la voluntad nacional; 2) Operaciones contra los comandantes enemigos; y 3) Operaciones contra las tropas.

El uso de las operaciones psicológicas contra la voluntad nacional oscila entre el guante de terciopelo, o el puño de hierro. Esta política se viene aplicando desde Tucídides hasta hoy. Algunos lo llaman "ofensivas en la paz"; solo basta ver los desfiles rusos, chinos y coreanos, o en Chipre las ejercitaciones militares de ambos bandos, dirigidas a mostrar el poderío. Es un concepto de seguridad denominado disuasión.[1]

Hay otras formas que emplean los más débiles. El líder del clan Somalí Mohamed Aideed pareció ser un maestro en el uso de las operaciones psicológicas. En la confrontación con los *rangers* de EEUU, conocido ampliamente en la película La Caída del Halcón Negro", que costara la vida a 19 Rangers, el bando de Aideed perdió 15 veces ese número, que representaba casi la tercera parte de su fuerza. Sin embargo, las fotografías de somalíes arrastrando los cuerpos de soldados de EEUU por las calles de Mogadisho fueron trasmitidas por CNN a los Estados Unidos y terminaron por convencer a la audiencia que era necesario evacuar la presencia

[1] Ag 40/553 Conceptos de seguridad ONU, 1986. El documento está a disposición en la Biblioteca de ONU en UN NY.

de EEUU en Somalia. También Aideed usó con ingenio las comunicaciones satelitales y radiales dentro de la ciudad, de forma tal que las ondas rebotaran y no pudieran ser localizadas.

Otro caso fue el del presidente egipcio Anwar el Sadat, durante la Guerra del Yom Kippur. Allí, pese a que el tercer Ejército Egipcio estaba rodeado, se festejó en El Cairo con grandes desfiles triunfales, resultando en la devolución de la península del Sinaí. En nuestra historia, en ocasión del enfrentamiento de las fuerzas de Buenos Aires y la Confederación en la batalla de Cepeda de 1859, si bien fue perdida por las fuerzas porteñas, en Buenos Aires se llevaron a cabo festejos por el triunfo. Con ello se logró que la Provincia de Buenos Aires fuera incorporada de derecho a la Confederación Argentina.

Hoy los medios de comunicación globales – CNN y Al Jazirah por ejemplo – aseguran que los eventos se conozcan de inmediato en todo el planeta. Se suma a esto que el ser humano tiene la tendencia de creer todo lo que dicen los medios, y hasta que se descubra la verdad, lleva un tiempo, las contramedidas pueden resultar tardías y las consecuencias ya se han producido. Si se usan las emisiones de satélites, los líderes de una nación no necesitan permiso para hablar directamente a gente de otra nación y esta posibilidad está disponible para todos a un costo relativamente bajo. También tiene su influencia la capacidad de editar videos, haciendo aparecer como real lo que no lo es. De cualquier forma, las audiencias tienen pre juicios, y se encontrará aquellos que creen cualquier cosa, otros que no crean nada, y otros que crean lo opuesto a lo que divulguen los medios.

Nada desorienta confunde y desorienta más a los comandantes enemigos que la acción psicológica apuntadas a ellos, para llevarlos a decisiones erróneas o tardías. Los comandantes toman decisiones sobre la base de eventos inesperados. Si la realidad es diferente de la que se toma como base para decidir, toma tiempo adaptarse a una nueva realidad contradictoria. Instintivamente, los eventos con baja probabilidad de ocurrencia son descartados, y si ocurren, son pocos los comandantes que pueden adaptarse. Los alemanes estaban convencidos que los Aliados cruzarían por el Paso de Calais, y que el ataque principal provendría donde estaba asentado el general Patton en el Reino Unido. Los japoneses estaban convencidos que las fuerzas de EEUU provendrían de las Aleutianas. No ocurrió así.

El experto en difundir informaciones en oportunidad era Mussolini. Cuando decidía hacer algo con impacto en la comunidad internacional, lo difundía los viernes, conociendo que el ámbito diplomático se involucraba en sábado y domingo en infinitos asuntos protocolares. Cuando el lunes al reiniciar el trabajo se daban cuenta de los hechos, ya habían pasado tres días. [2]

Los medios pueden jugar un rol importante en esta desorientación de los comandantes. Un caso típico pasó en la Guerra del Golfo de 1991, donde los medios trasmitieron que dos portaaviones estadounidenses estaban atravesando el Canal de Suez el mismo día en que se inició el ataque aliado. Ello llevó a pensar a Sadam que el ataque aún no se lanzaría. Tal información resultó falsa[3]. Asimismo, los medios colaboraron como elemento de comando de los aliados, negando los micrófonos a Sadam, incrementando así su aislamiento internacional. En esta Guerra del Golfo, los iraquíes estaban convencidos que la guerra aérea sería corta – duró 40 días – y que el esfuerzo principal sería terrestre. También creían que la intención de los aliados era reconquistar Kuwait desde el mar. Para eso, los medios divulgaron ambas concepciones, la primera difundida a través de CNN, la segunda enviando buques de guerra aliados a patrullar intensamente las costas.

Históricamente, en el nivel operacional esta manera de engaño psicológico usando las Operaciones de Información ha rendido más frutos en el bando que tenga mejor idea de lo que el otro bando hará o dejará de hacer. El conocimiento profundo de la cultura militar imperante en el oponente juega un rol importante en esto.

Las operaciones psicológicas contra las tropas es antigua. La primera de ellas es crear temor y respeto por el Comandante enemigo. El caso paradigmático es el de Rommel en la Campaña de África, donde el respeto por Rommel llevó a Montgomery a prohibir a sus tropas que se lo nombrase. Tal respeto se acentuó cuando una noche, por equivocación, Rommel inspeccionó un hospital de campaña inglés, y se interesó por la salud de los enfermos. Las otras dos facetas consisten en imponer miedo a la muerte o a las pérdidas, o acentuar la brecha entre las comodidades del palacio y las trincheras.

[2] Citado por John Gunther, "Líderes del Siglo XX", Editorial Bruguera, Barcelona, 1968, original en inglés
[3] Quiao Liang y Wang Xiangsui, Unrestrited Warfare, Pan American Publishing Company, Panama, 1999, P. 60.

Este tipo de acción psicológica se lleva a cabo por ondas de radio – todos los soldados llevan radios portátiles al combate, los del mundo desarrollado llevan teléfonos móviles – actualmente por internet y las redes sociales, y el más antiguo de los métodos pero usado hasta hoy, por panfletos arrojados desde el aire. En la Guerra del Golfo, las fuerzas de la coalición desparramaron la idea mediante panfletos y convencieron a muchas tropas iraquíes que si abandonaban sus vehículos, vivirían más. Eso lo hicieron luego de tomar como blancos con sus armas de precisión, a vehículos blindados iraquíes. Otro caso más conocido es el de la Rosa de Tokio en la IIGM, sobrenombre dado por los servicios de contrainteligencia aliados a las radioemisiones en AM en idioma inglés de locutores japoneses angloparlantes, con mensajes dirigidos a las tropas aliadas. Asimismo, en la Guerra de Malvinas, una locutora inglesa ubicada en la flota británica trasmitía noticias tanto en español como en inglés, dirigidos a las tropas argentinas.

Conclusiones

La importancia de las Operaciones de Información se ha acentuado con la aparición de numerosísimas tecnologías de información. Aunque no se disponga de todos los adelantos tecnológicos que aquí se citan, para poder tomar contramedidas será necesario conocer cómo trabajan.

La abundancia de información va a causar tres efectos: el primero de ellos será que la información de los diferentes tipos de sensores puede ser contradictoria, y eso va a valorizar más la estimación humana sobre la confiabilidad; el segundo efecto será la proliferación de información que va a tener que ser analizada y filtrada, antes que llegue como elemento decisor al Comandante, ya que mucha información será útil, y mucha más absolutamente inútil. Eso demorará las decisiones. El tercer elemento devendrá de la disponibilidad de la misma información en todos los niveles, desde el comandante supremo al soldado individual: esto sembrará dudas sobre la eficacia y oportunidad de las resoluciones.

Toda esta proliferación de información afectará a uno de los dos principios de la guerra enunciados por Clausewitz: la rapidez. Clausewitz sostenía que la rapidez de reacción era una cualidad apreciada en cualquier comandante, cuando decía "El segundo principio [N del R: el primero es el de masa] es la rápida utilización de nuestras fuerzas".[4] En este sentido, coincide con Sun Tzu: "La rapidez de acción es el factor esencial de la condición de la fuerza militar, aprovechándose de los errores de los adversarios, desplazándose por caminos que no esperan y atacando cuando no están en guardia. Esto significa que para aprovecharse de la falta de preparación, de visión y de cautela de los adversarios, es necesario actuar con rapidez". Ninguna otra cosa que la que sostenía Alvin Toffler en su obra "La Tercera Ola": con la rapidez, los conocimientos se vuelven rápidamente obsoletos y se puede decidir erróneamente.

Esto será el desafío de la guerra del futuro, porque la rapidez necesaria para triunfar incrementará los riesgos a los que el conductor se verá expuesto.

De la seguridad y defensa cibernética se hablará en el siguiente capítulo.

Bibliografía:

Libicki Martin, What is Information Warfare, National Defense University, Institute for National Strategy Studies, Washington DC 1996.

Patrik Thomé, Major, Swedish Army, The Role of Information Operations in Strategy, Conventional War and Low Intensity Conflict, 2006, obtenible en http://www.au.af.mil/info-ops/iosphere/iosphere_summer06_thome.pdf , fecha de consulta 15 Abril 2013.

[4] Clausewitz Carl, De la Guerra, Edición del Ministerio de Defensa Español, traducción de la edición de la Universidad de Princeton, Madrid, 1999, Libro VIII Cap. 9, P.877.