
**ESPECIALIZACION EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO**

# TRABAJO FINAL INTEGRADOR

**TEMA:**

Principios de la guerra y nuevas tecnologías de la información.

**TÍTULO:**

Dificultades para la obtención de la sorpresa en el nivel operacional ante el avance de las nuevas tecnologías de la información.

**AUTOR:** Mayor Juan Martín Barbosa Larronde.

**Año 2012**

**RESUMEN**

En este trabajo se exponen las capacidades y, fundamentalmente, las limitaciones de los actuales recursos tecnológicos de la información para poder obtener enseñanzas que puedan ser consideradas en la búsqueda de la sorpresa en el nivel operacional mediante el velo y el engaño.

La sorpresa otorga una ventaja a una fuerza militar sobre su oponente sin embargo, en el nivel operacional es muy difícil de lograr y demanda una gran asignación de medios, lo que la convierte en una ventaja altamente costosa.

A la dificultad de su logro, por la magnitud de fuerzas que implica este nivel, se le suma la tecnología de la información aplicada a la seguridad operacional, como recurso válido para reducir a su menor expresión la posibilidad de ser sorprendido por el enemigo.

A través de la lectura de este trabajo, se podrá confirmar que el obstáculo de la sorpresa, más que la tecnología, está en la capacidad de quienes la emplean, en su imaginación para desarrollar nuevos procedimientos y planes de operaciones originales. El límite está, en consecuencia, en el hombre más que en los sensores.

**PALABRAS CLAVE:** Sorpresa – velo y engaño – seguridad operacional – tecnologías de la información.

## 1. TABLA DE CONTENIDOS.



## 2. TABLA DE CUADROS E IMÁGENES.

## *INTRODUCCIÓN.*

En su doctrina, las fuerzas armadas argentinas identifican a la sorpresa como un principio de la guerra que permite obtener una ventaja sobre un enemigo actuando en un lugar, momento, de forma o con medios inesperados por éste quitándole la posibilidad de adoptar contramedidas eficientes.

De esta definición, surge que la sorpresa se puede lograr ocultando información al enemigo, velando, o induciéndolo a falsas conclusiones, engañándolo. Es, entonces, mediante el velo y el engaño que se evitará que el enemigo esté en capacidad de preparar una respuesta adecuada a las acciones propias para que pueda ser empleada en la oportunidad y el lugar necesario.

El concepto como tal, es tan antiguo como la guerra misma. Sun Tzu, en el siglo V a.C., expresaba que "el arte de la guerra se basa en el engaño"[1]. Por otro lado, Clausewitz, en el siglo XIX, encontraba a la sorpresa no decisiva y muy desgastante. Sentenció "es muy raro que un estado sorprenda a otro (…) la sorpresa se logra más fácilmente en operaciones que requieren poco tiempo"[2], haciendo alusión al nivel táctico. Este autor consideraba que la sorpresa en el nivel operacional era difícil de lograr y por demás desgastante.

Es posible encontrar casos concretos de la historia militar en los que se obtuvo la sorpresa y, consecuentemente, una ventaja ante el enemigo. El "caballo de Troya" surgido en los relatos de Homero; la "guerra de zapa" llevada a cabo por las fuerzas del general San Martín en su campaña "Libertadora"; la operación "Guardaespaldas" en la II Guerra Mundial para proteger el desembarco aliado en Normandía; la guerra del "Yom Kippur" en 1973, entre otros.

En los ejemplos mencionados, debido a la incapacidad de un comandante para confirmar una información obtenida, normalmente la asumía como cierta. De esta manera, los usos y costumbres, la rutina, la correspondencia del enemigo obtenida al capturar un estafeta o la interceptación de cualquier otro tipo de comunicación (radioeléctrica, telefónica, etc) podía tomarse como válida. Los comandantes que supieron aprovechar esta limitación, lograron "cederle" exitosamente información falsa a su enemigo para lograr sorprenderlos.

---

[1] Sun Tzu. "El arte de la guerra", Edición Fernando Puell, 2001, p.31

[2] Clausewitz, Carl. "De la guerra", traducida al español por Celer Pawlowsky de la versión de Peter Paret. Madrid. Ministerio de Defensa de España, 1999, p 331.

Todos estos ejemplos mencionados parecerían difíciles de lograr si fuesen sometidos a los recursos tecnológicos aplicados a la vigilancia que en la actualidad se dispone. Un despliegue obtenido por una imagen satelital, una interceptación de un satélite de comunicaciones, un entrecruzamiento de datos informatizados sobre el destino de grandes volúmenes de necesidades logísticas o hasta la presencia de un espía propio infiltrado en territorio enemigo con capacidad de comunicación satelital hubieran alertado a las fuerzas sorprendidas sobre las reales intenciones del enemigo y sus acciones encubiertas.

En este sentido, se puede afirmar que en la actualidad la tecnología posibilita obtener información del enemigo de diferentes formas y empleando diferentes medios, cada vez con mayor alcance y capacidad. Esta disponibilidad permite comparar cada información obtenida con una infinidad de otras relacionadas y encontrar coherencia entre ellas o alertar cuando esto no suceda.

Pareciera, entonces, que la búsqueda de esta ventaja está reducida a la capacidad de detección que el enemigo disponga o si los propios medios tecnológicos disponibles son tan superiores que tienen la capacidad de neutralizarlos o anularlos.

El Manual de estrategia y planeamiento para la acción militar conjunta – Nivel operacional – La campaña, en su anexo 1, establece que la sorpresa puede verse favorecida por un veloz proceso de toma de decisiones, efectiva inteligencia, velo y engaño, acciones de submarinos y tropas de operaciones especiales o actuando con tácticas y métodos inesperados.

El dilema de todo comandante operacional, en este sentido, podrá ser destinar parte de los medios disponibles a la búsqueda de la sorpresa, cada vez más dificultosa de lograr y, consecuentemente, obtener un balance favorable en una relación de poder de combate o, sencillamente, destinar esa parte de los medios a conformar una mayor concentración y lograr, directamente, ese balance.

Para poder resolver este dilema, es necesario exponer a quien se desempeñe como comandante operacional las expectativas de éxito de un plan y posterior ejecución de las operaciones de velo y engaño considerando los recursos tecnológicos actualmente disponibles que pueden aplicarse a la neutralización de la sorpresa en el nivel operacional. De esta manera, dicho comandante podrá establecer si las operaciones de velo y engaño satisfacen o no el requisito de aceptabilidad en el marco de su campaña.

La obtención de la sorpresa en el nivel operacional ha sido tratada en diversos trabajos de investigación orientados a la elaboración de un adecuado plan de velo y engaño. Se puede mencionar, entre otros, al trabajo de investigación del Coronel José María Canevaro *"El velo y el engaño y la sorpresa en el nivel estratégico operacional"* del año 2004, entre otros. El trabajo más reciente en este sentido fue presentado por el Mayor de Ejército Ignacio Zubeldía bajo el título "*Los planes y operaciones de velo y engaño en el teatro de operaciones"* publicado el año 2010.

En el plano internacional, es posible mencionar el trabajo de autores estadounidenses que tratan el tema, entre ellos el Mayor Mark Johnson (USMC) y la Mayor Jessica Meyeraan (USAF) que en el ámbito de la Escuela de Guerra Conjunta y Combinada de EEUU publicaron en el año 2003 *"Military deception: hiding the real – showing the fake"* (Engaño militar: escondiendo lo real – mostrando lo falso). Asimismo, se puede incluir el trabajo de William Hutchinson, publicado en la Edith Cowan University (Australia) en el año 2006 bajo el título "Information warfare and deception" (Información de la guerra y engaño).

En el plano regional, es posible citar al Capitán de Navío de la Armada de Chile Gustavo Jordán Astaburuaga, que publicó *"La sorpresa. Multiplicador de fuerzas por excelencia"*.

Sin embargo, esos trabajos exponen las ventajas de un eficiente velo y engaño en la búsqueda de la sorpresa a la luz del análisis de exitosas operaciones históricas en la obtención de la sorpresa, pero no han sido sometidos a las capacidades de los recursos tecnológicos que actualmente están a disposición de las partes en un conflicto armado para posibilitar la seguridad en el nivel operacional.

Debe aclararse que se considera posible lograr la sorpresa en el nivel operacional a pesar de las capacidades de los actuales recursos tecnológicos aplicados a la seguridad.

De lo hasta aquí expresado, surge un interrogante que los estudios anteriores no se han planteado ¿Cómo lograr la sorpresa en el nivel operacional ante las nuevas tecnologías actualmente disponibles, aplicadas a la obtención de información? Siempre considerando a la obtención de la sorpresa en el marco de un conflicto armado con características convencionales.

Para resolver el interrogante planteado se establece, como objetivo, proponer posibles modos de obtener la sorpresa ante las nuevas tecnologías actualmente disponibles, aplicadas a la obtención de la información. Esto impone plantearse objetivos parti-

culares, el primero de ellos, establecer las capacidades y limitaciones de los recursos tecnológicos actualmente disponibles, aplicados a la neutralización de la sorpresa en el nivel operacional. Una vez cumplido éste, poder establecer las consideraciones esenciales para un exitoso velo y engaño en el nivel operacional.

De esta manera, es necesario determinar si es posible vulnerar las capacidades de obtención de información de los medios tecnológicos de seguridad en el nivel operacional y cómo lograrlo para poder aprovecharlas en favor propio y lograr sorprender al enemigo. Esto impone realizar un estudio técnico de los medios, que materializa la primera parte de este trabajo y, posteriormente, considerar las ventajas obtenidas en la elaboración del plan de velo y engaño, cuyo contenido se desarrolla en la segunda y última parte.

## *CAPÍTULO 1.*
## *"DISPOSITIVOS TECNOLÓGICOS EN LA SEGURIDAD OPERACIONAL"*

La búsqueda de las debilidades de los diferentes sensores demanda la explicación del principio de funcionamiento de cada uno de ellos para detectar, de esa manera, sus potenciales vulnerabilidades.

En un sentido genérico, es posible identificar a todos aquellos sistemas o componentes, independientemente el grado de sofisticación, como sensores. La Real Academia española define al sensor como *"dispositivo que detecta (siente) una determinada acción externa, temperatura, presión, etcétera y la transmite adecuadamente"*. Existen dos tipos de sensores. Los sensores directos son aquellos que actúan por contacto directo, termómetro por ejemplo, y los sensores remotos, aquellos que actúan alejados del elemento o medio cuya información captan, por ejemplo cámara fotográfica, barredores multiespectrales, etcétera. Este último grupo, de interés para el presente trabajo.

Como principio básico de la captación de imágenes se puede establecer un proceso. Todo objeto emite energía en diferentes formas, generándola o reflejándola. Ésta es captada por sistemas creados por el ser humano, dando lugar a una imagen.

Los parámetros que caracterizan la energía electromagnética son la dirección de propagación, que indica hacia donde se dirige; la amplitud, que indica la intensidad del pulso y la frecuencia que indica la cantidad de crestas que pasan por un punto en un segundo. Un sistema capta la energía emanada en un determinado rango de parámetros.

Los sensores remotos se clasifican en pasivos y activos. Los primeros son aquellos que utilizan la energía electromagnética emitida o reflejada por los cuerpos para la captación de datos o imágenes. Por su parte, los sensores activos son aquellos en que un generador especial emite, desde la misma ubicación que el sensor, una radiación de energía electromagnética hacia un área de interés. Parte de esa energía será reflejada hacia los órganos de recepción que detectarán y registrarán la onda. Asimismo existen sensores remotos que no captan imágenes.

Esquemáticamente, la clasificación de los sensores remotos podría sintetizarse según el Cuadro N° 1:

Cuadro N° 1: Clasificación de los sensores remotos

| | |
|---|---|
| Sensores Pasivos | - Sensores (cámaras) fotográficos de primera generación.<br>- Sensores optrónicos (opticoelectrónicos y opticomecáni- |

| | |
|---|---|
| | cos).<br>- Sensores electrónicos. |
| Sensores Activos | - Sensores opticoelectrónicos.<br>- Sensores electrónicos. |
| Sensores remotos que no captan imágenes | - Micrófonos, detectores acústicos y el sonar.<br>- Detectores sísmicos y magnéticos.<br>- Sensores térmicos y volumétricos.<br>- El radar y el lidar (en otra modalidad, por ejemplo para mediciones o para adquirir blancos). |

**Fuente:** Elaboración propia[3]

## *SECCIÓN 1.*

## *"SENSORES PASIVOS"*

Los sensores pasivos son aquellos que utilizan como fuente de energía la captación de información de la radiación electromagnética emitida y/o reflejada por los cuerpos. Por ejemplo, una cámara fotográfica capta el reflejo de la luz en el objeto o un sensor térmico capta las imágenes de un objeto por las emisiones de calor de éste.

Los sensores pasivos se dividen en tres grupos. Éstos, a su vez, presentan una subdivisión. Esquemáticamente, se puede representar con el siguiente cuadro:

Cuadro N° 2: Clasificación de los sensores remotos pasivos

| | |
|---|---|
| Sensores fotográficos de primera generación | - Cámara métrica.<br>- Cámara de reconocimiento convencional.<br>- Cámara panorámica.<br>- Cámara continua.<br>- Cámara multiespectral. |
| Sensores opticoelectrónicos | - Cámara fotográfica de segunda generación.<br>- Cámara de video.<br>- Intensificadores de luz residual.<br>- Barredores multiespectrales de estado sólido.<br>- Barredores hiperespectrales de estado sólido. |
| Sensores opticomecánicos | - Sensores térmicos<br>- Barredores multiespectrales de barrido mecánico. |
| Sensores electrónicos | - Radiómetro de microondas.<br>- Sonar pasivo. |

**Fuente:** Elaboración propia[4]

[3] En base a información extraída de Aguilar Huergo, Pablo *"Inteligencia de imágenes"* Instituto de Inteligencia de las FFAA Argentinas, Buenos Aires, 2007. pp. 3 a 9.

[4] En base a información extraída de Aguilar Huergo, Pablo *"Inteligencia de imágenes"* Instituto de Inteligencia de las FFAA Argentinas, Buenos Aires, 2007. pp. 3 a 9.

La cámara métrica es una cámara fotográfica que se emplea para relevamiento cartográfico, agrimensura o trabajos donde se necesiten imágenes que sean una fiel representación del terreno pero no en operaciones bélicas. Por ello debe reunir algunos requisitos indispensables como objetivos luminosos de alto rendimiento, prácticamente libres de distorsión; determinación exacta de la relación geométrica objetivo – plano focal; aplanamiento seguro de la película en el plano focal; obturadores de alta velocidad para eliminar el desplazamiento de la imagen; algunos requisitos auxiliares como reloj, altímetro; dispositivo de compensación universal para asegurar la estabilidad de la cámara y absorber las vibraciones y los movimientos del avión y un dispositivo regulador de la cadencia de toma.

Los requisitos mencionados, hacen que las cámaras métricas sean voluminosas y por ello, para su empleo, deben ser incorporadas a la estructura de un avión.

La cámara de reconocimiento convencional, al no cumplir los requisitos de las cámaras métricas, son de tamaño más reducido, lo que permite su instalación en el fuselaje de un avión y puede ser operada directamente por el piloto.

La cámara panorámica, para evitar la reducción de la resolución espacial hacia los bordes de la imagen, recurre a un barrido que la zona paraxial del objetivo debe cumplir para cubrir la superficie total del formato a exponer. El resultado final es una fotografía rectangular en la que el área del terreno abarcado llega, en dirección transversal al avión. Este procedimiento genera una deformación de imágenes.

Las cámaras continuas surgieron ante la necesidad de obtener imágenes nítidas en vuelos de reconocimiento a baja altura, desde aviones rápidos. Actualmente, estas cámaras pueden ser operadas en forma automática y producir imágenes excelentes aún en condiciones adversas de vuelo y de iluminación. La cámara continua térmica posibilita obtener imágenes tanto de día como de noche y a través de humo permitiendo, incluso, la observación estereoscópica.

La cámara multiespectral, de empleo similar a la cámara métrica, permite dividir la respuesta del terreno en bandas de espectros. Esto permite obtener información sobre los diferentes porcentajes de energía reflejada por los distintos elementos del terreno.

Los sensores opticoelectrónicos funcionan, básicamente, como el ojo humano. A partir de una imagen inicial hay un proceso de transformación de las variaciones lu-

minosas de los "píxeles"[5] en variaciones eléctricas que tienen su intensidad proporcional a los valores de luz de cada punto. La señal de video es amplificada, procesada y transmitida por cable hasta el monitor.

La cámara fotográfica de segunda generación carece de material sensible. La imagen captada por la lente es proyectada sobre un dispositivo de acople de carga (CCD) en vez de hacerlo sobre una película convirtiendo la imagen en impulsos eléctricos, los cuales pueden ser grabados en forma analógica o convertidos a formato digital. Para su interpretación, se requiere computadoras potentes.

La cámara de video se diferencia con la cámara fotográfica de segunda generación en que, mientras la última capta una imagen fija, la de video capta imágenes en movimiento. Las imágenes también son convertidas en impulsos eléctricos y transmitidas al monitor para su visualización y pueden ser almacenadas en cintas de video, primera generación, o digitalizadas.

Un intensificador de luz residual (ILR) contiene un sistema multiplicador de electrones con un dispositivo de observación en un extremo y una lente en el otro. Como la imagen obtenida por este sensor es transitoria, deberá añadirse una cámara de video o cámara fotográfica para su registro. Asimismo, los ILR presentan algunos inconvenientes como ser una mínima iluminación ambiental; pueden provocar deslumbramiento ante una fuente lumínica de importancia y sus capacidades se reducen ante precipitaciones, niebla, viento blanco y humo generado por agentes fumígenos.

Los barredores multiespectrales de estado sólido captan una imagen, por similitud al ojo humano. La imagen captada se basa en la reflexión parcial de la luz. La información contenida en esa imagen es de dos tipos. Por un lado "espacial", en la medida que permite identificar de donde viene cada contribución a la imagen. Por otro lado "espectral", en la medida que se pueden identificar diferentes colores. Estos sistemas operan en varias bandas del espectro electromagnético y se pueden encontrar en sistemas de reconocimiento satelital.

Los barredores hiperespectrales de estado sólido mejoran las prestaciones del grupo anterior en tanto que la imagen obtenida de los multiespectrales podía presentar "a ojos del sensor" diferentes materiales del mismo color y, por ende indistinguibles. La

[5] Se denomina píxeles a los puntos que componen una imagen. Su expresión deriva de la abreviatura de "picture element" expresión en inglés que significa elemento de imagen en castellano. Aguilar Huergo, Pablo "Inteligencia de imágenes" Op cit, p. 24

información contenida en la imagen es mucho más que la contenida en una imagen visible. Es por eso que su interpretación demanda mayor tiempo.

Los sensores opticomecánicos utilizan un objetivo normal para producir una imagen óptica sobre un detector. Este detector, que ocupa un área no mayor que la cabeza de un alfiler, está conectado a un conductor eléctrico que, por su reducido tamaño, puede ser enfriado sin dificultad para mejorar su capacidad de captación.

El problema de cubrir con ese reducido "campo visual" un campo angular mucho más amplio, encuentra solución en un barrido sistemático. Estas señales son amplificadas y transmitidas a un monitor para la observación de las imágenes y almacenadas en formato analógico o digital.

Los sensores térmicos captan la energía (térmica) emitida por los cuerpos que se distribuye casi enteramente en las regiones del infrarrojo medio y lejano. La fotografía infrarroja convencional puede registrar imágenes en el infrarrojo cercano, por lo que está limitada en este aspecto.

La formación de imágenes térmicas presenta diversas ventajas con respecto a los ILR: pueden ser utilizados en la oscuridad completa, puede obtener imágenes a través de todo tipo de humo, polvo y niebla; no enceguecen; puede operar durante el día y permiten detectar objetos a mayor distancia. También tienen desventajas: son más costosos; consumen mucha energía; son muy grandes y frágiles. Esto lo limita a ser empleados en sistemas de vuelo nocturno de aeronaves, sistema de puntería de tanques y a reconocimiento aéreo. Actualmente, existen algunos elementos (redes, uniformes y/o sistemas) de enmascaramiento térmico.

Los barredores multiespectrales de barrido mecánico no se limitan al infrarrojo térmico. Pueden proveer, también, imágenes multibanda en cualquier banda de espectro. Si embargo, el proceso de transmisión de la información resulta algo complejo para evitar la degradación de la calidad y la consecuente pérdida de información. Varios sistemas satelitales de reconocimiento de recursos terrestres y meteorológicos poseen este tipo de barredor multiespectral.

En el análisis multiespectral de imágenes satelitales, el intérprete pasa por los filtros la información que no es captada por el ojo humano para que sean perceptibles dando preponderancia a aquellos aspectos que se desee destacar.

Los sensores electrónicos son sensores que carecen de parte óptica y reciben la radiación emitida y/o reflejada por los cuerpos a través de una antena y transferida a una computadora que la convierte en una imagen.

El radiómetro de microondas capta la radiación electromagnética generada por todo objeto que tenga una temperatura termodinámica superior a los 0°C permitiendo diferenciar un cuerpo del medio que lo rodea. Debido a la longitud de onda que operan, pueden ser considerados sensores para casi todo tipo de clima afectado solamente por el agua líquida en forma de precipitación. Estos sensores se encuentran emplazados en la mayoría de los satélites meteorológicos y de estudio para el medioambiente.

## *SECCIÓN 2.*
## *"SENSORES ACTIVOS"*

Los sensores activos son aquellos sensores que contienen en su estructura una fuente emisora de energía electromagnética que irradiada sobre una zona determinada, parte de esa energía será reflejada hacia la fuente y los órganos de recepción, detección y registro.

Los sensores opticoelectrónicos activos, la fuente emisora de radiación electromagnética del sensor emite una radiación reflejada por el blanco que es enfocada por el objetivo del sensor hacia un material fotosensible (primera generación) que la registra o hacia un dispositivo electrónico que la convierte en impulsos eléctricos. Ejemplos militares de éstos son el visor nocturno de primera generación y el lidar.

El visor nocturno de primera generación implica el uso de un reflector infrarrojo, que emite energía no visible para el ojo humano, cuya intensidad y condiciones meteorológicas afecta su alcance. La principal desventaja de estos equipos es que la fuente puede ser detectada por cualquiera que tenga un sensor de estas características.

El lidar, acrónimo de Light Detection and Ranging – Detección y Medición de Luz, es una tecnología que permite determinar la distancia desde un emisor láser a un objeto o superficie utilizando un haz láser pulsado. La distancia se mide a partir del tiempo de retraso entre la emisión del pulso y la detección de la señal reflejada. Si bien es un sensor de aplicación en el medio civil, tiene su utilidad en el ámbito militar.

El lidar utiliza ondas entre diez y cien veces más cortas que las ondas de radar. Esto implica una mayor capacidad para obtener datos. Una ventaja de esta tecnología en comparación con otras, es que puede ser adquirido en condiciones atmosféricas en que la fotografía aérea convencional no puede hacerlo. Un ejemplo de ello, la toma de datos puede lograrse desde un avión en vuelo nocturno o en condiciones de visibilidad reducida por nubosidad o bruma.

Los sensores electrónicos activos carecen de un elemento óptico para captar y concentrar la radiación recibida hacia un material sensible o dispositivo electrónico, estos sensores emiten y reciben la radiación electromagnética a través de una antena o transductor. Entre los sensores que producen imágenes, se encuentran el radar y el radar lateral.

El radar, Radio Detection and Ranging – Detección y Medición de Distancia por Radio, posee su propia "iluminación", constituida por una emisión de pulsos de energía electromagnética de frecuencia bien definida. Estos pulsos son emitidos por la antena mientras gira haciendo un barrido. Entre dos paquetes de pulsos sucesivos hay un intervalo durante el cual no se emite. A través de la misma antena se conecta el receptor que capta el débil reflejo. El proceso alternado entre emisor y receptor se repite cíclicamente y en forma continua por un período.

Los ecos recibidos son amplificado y evaluados según su retardo de señal, que ubica en posición el punto, y su intensidad, que se traducirá en la imagen del punto. Este dispositivo es afectado en su rendimiento por los diferentes tipos de terreno pudiendo generarse, áreas sin retorno conocidos como "sombra de radar", señales difusas o, incluso, retorno fluctuante. En realidad, el radar no es una "herramienta todo tiempo". Otra desventaja del radar es que, al ser un sistema activo, puede ser detectado y, por ende, vulnerable a las contramedidas electrónicas del enemigo.

El radar lateral busca incrementar la longitud de la antena para lograr, con ello, mejor resolución de la imagen. Desde una detección aire – tierra, una buena calidad de resolución es indispensable para identificar los objetivos. Con una antena montada paralela al eje de un avión se denomina "Radar de Visión Lateral Aerotransportado" o SLAR, por sus iniciales en inglés. La exploración de pantalla está condicionada por el barrido de antena.

El problema de la longitud de la antena en el avión fue resuelto con el Radar de Abertura Sintética, o SAR, con el empleo del "Efecto Doppler". Esta mejora fue evidenciada durante la Guerra del Golfo, en 1991, cuando los aviones Mohawk OV-1D norteamericanos dotado con SLAR fueron superados por los aviones Jaguar franceses dotados de radar SAR en el reconocimiento del campo de batalla y la localización de blancos.

Actualmente, el sistema SAR tiene gran aplicación en el campo militar en misiones de reconocimiento y vigilancia aérea, inclusive en áreas urbanas. Por sus dimen-

siones, puede ser montado sobre una aeronave no tripulada y sus capacidades permiten obtener información con cielo cubierto y llovizna tenue, tanto de día como de noche.

Existen, asimismo, una serie de otros sensores activos que, hasta el momento, no se ha encontrado utilidad en el ámbito militar propio del nivel operacional. Entre los que podemos mencionar, se encuentra la radiografía, los visores de rayos T, la tomografía axial computada, la resonancia magnética nuclear, la ecografía.

El sonar lateral es un sensor activo que puede tener una utilidad militar aunque, hasta el momento, implica una exposición y consecuente vulnerabilidad a la acción enemiga. Constituye un sensor acústico utilizado para la búsqueda de objetos en el fondo marino empleando un torpedo remolcado que emite una señal ultrasónica y recibe su eco.

## *CONCLUSIONES PARCIALES.*

De lo expuesto surge como primera conclusión que un adecuado sistema de seguridad y vigilancia de nivel estratégico tiende a la integración de la mayor cantidad de tipos de sensores remotos en cantidad acorde a los espacios a ser asegurados. Esta disponibilidad, conforme a las capacidades económicas del estado, debido a los costos, y al acceso a dicha tecnología.

Las técnicas de enmascaramiento tendientes a disimular colores, brillos y formas, tan empleados en conflictos armados anteriores no son efectivos al momento de intentar ocultar información ante la totalidad de los sensores remotos actualmente disponibles. No obstante ello, su empleo efectivo es un recurso válido a ser considerado en todos los niveles para reducir al máximo posible la coincidencia de información producida por los distintos sensores dificultando, de esta manera, la producción de inteligencia.

Gran cantidad de los actuales sensores requieren ser operados desde aeronaves en vuelo, tripuladas o no. Por esta razón una adecuada capacidad de defensa antiaérea que posibilite una rápida detección y destrucción del medio aéreo reducirá sensiblemente la capacidad de obtener información incrementando las posibilidades de obtener la sorpresa en el nivel operacional.

Las capacidades de los actuales medios hacen muy escasa la posibilidad de ocultar información a la vigilancia del enemigo. Por otro lado, se puede incrementar las medidas de confundir al enemigo a través de la exposición de blancos simulados que

provoquen confusión y demora en el análisis de la información obtenida, sobrecargando y saturando los órganos de dirección de inteligencia. Para ello, es necesario conocer los tipos de sensores a disposición del enemigo e identificar la forma en que los blancos falsos deberán exponerse.

La información obtenida desde plataformas satelitales es muy detallada y precisa, pero no está al acceso de todos los países. Otra desventaja que presenta radica en los tiempos, relativamente prolongados, de transmisión y el procesamiento de esa información en el grado de detalle que ella ofrece. Si bien las experiencias de su producto son aplicadas en tareas de las ciencias, es posible que el producto resultante no sea oportuno para evitar la sorpresa.

Existe un grupo de sensores que son de empleo en el nivel táctico, incluso individual. No obstante ello, son de interés en este análisis ante la necesidad de considerar a todo elemento como medio de obtención de información. Una reducida fracción puede estar ejecutando una misión para obtener de información que responda al más alto nivel de un teatro de operaciones.

En ocasiones, otra vulnerabilidad de estos sistemas no se encuentra en los sensores sino en los dispositivos de transmisión de la información. Mediante operaciones de Guerra Electrónica puede lograr impedirse la disponibilidad de la información resultante en oportunidad.

## *CAPÍTULO 2.*
## *"VELO Y ENGAÑO"*

Como se pudo determinar en el capítulo anterior, cada vez resulta más dificultoso, sustraer de la detección del enemigo medios o fuerzas con capacidad de influir decisivamente en la campaña o en una parte de ella. Una adecuada integración de los medios disponibles aplicados a la seguridad operacional materializa ese desafío. No obstante, no se puede expresar taxativamente que sea imposible. Puesto que la evolución es permanente, la experiencia demuestra que, a cada avance tecnológico, lo sucede una posibilidad de neutralizarlo.

La búsqueda de la sorpresa en el nivel operacional, entonces, no puede estar basada únicamente en el intento de negar al enemigo la detección. Ese intento sería altamente costoso y tendría muy pocas expectativas de éxito, al punto que muy pocos comandantes aceptarían los riesgos.

Ante esta encrucijada, es conveniente destacar que el engaño no se efectúa a los medios tecnológicos que el enemigo emplea para la obtención de información, sino a las personas que la analizan, interpretan y valoran dicha información para producir inteligencia.

A partir del análisis de casos históricos, se pudo observar que el enemigo engañado tuvo a su disposición indicios que, si hubieran sido adecuadamente analizados, el engaño habría fracasado.

Por supuesto, condicionar la interpretación del enemigo implica la afectación en alguna medida de sus medios tecnológicos que alimentan el análisis.

Como se expresara al final del capítulo anterior, se puede limitar parcial y temporalmente la capacidad de la tecnología enemiga. Esa limitación provocada es la ventana de oportunidad para "sembrar" el engaño o, al menos, la duda de cómo se emplearán los propios medios.

Francisco A Marín en "*Engaños de la guerra – Las acciones de decepción en los conflictos bélicos*" ha establecido algunos principios de aplicación general para las operaciones de velo y engaño. Éstos constituyen axiomas de fundamental importancia al momento de planificar operaciones de velo y engaño, ellos son: objetivo, credibilidad, seguridad, conocimiento del adversario, preparación, coordinación, oportunidad y flexibilidad.

Cuando se habla de objetivo, se establece que estas operaciones no tienen una finalidad en sí misma sino que se utilizan para apoyar operaciones principales. Se vela y se engaña para que el enemigo no pueda identificar las acciones principales propias hasta que sea demasiado tarde para contrarrestarlas.

Por credibilidad, se entiende que aquello que se procura hacer concluir al enemigo sólo tendrá posibilidades de éxito si la información suministrada deliberadamente al adversario tiene un mínimo de realismo.

El principio de seguridad hace referencia, por un lado, a evitar que el enemigo no descubra las verdaderas intenciones propias. Por otro, requerirá disponer de información del enemigo necesaria para permitirle obtener la información que lo induzca a conclusiones falsas.

El principio de conocimiento del adversario establece la importancia, en todo conflicto bélico, de tener el mayor y más profundo conocimiento del oponente para poder anticipar cómo reaccionará con la información falsa que se le permitirá obtener. De esta manera, se procura evitar efectos adversos a las operaciones propias.

El concepto de preparación implica la necesidad de inclusión de las medidas de velo y engaño desde las primeras intenciones del comandante, como máximo decisor. Inicialmente, podrá ser una consideración general profundizándose conforme avance el planeamiento. Por otro lado, este principio establece que los responsables de planificar las acciones de velo y engaño necesitan tener acceso irrestricto al trabajo de todos los integrantes del Estado Mayor a los efectos de no considerar previsiones que atenten o afecten al plan principal, o parte de él.

El principio de coordinación permite establecer la idea de la relación necesaria entre el plan de velo y engaño y el plan esquemático de campaña. Esta necesidad radica en que el plan de velo y engaño constituye un plan complementario que apoya al principal. Esta coordinación de todos los planes será una responsabilidad del área de operaciones dentro del trabajo del Estado Mayor.

La idea de flexibilidad en el plan de velo y engaño hace referencia a la necesidad de una constante adaptación a los cambios de situación que se podrán presentar con la evolución del conflicto. Sin un adecuado grado de flexibilidad, se corre el riesgo que este plan fracase ante una situación no prevista o anticipada.

Finalmente, el principio de oportunidad da una idea del tiempo previo que las operaciones de velo y engaño requieren. La información falsa que deliberadamente es cedida el enemigo debe permitir que éste la incorpore como cierta, la pueda procesar y

obtener con ella, las conclusiones erróneas que facilitarán las propias acciones. La reducción en los tiempos que este proceso demanda puede llegar a provocar un efecto contrario al pretendido.

Estos principios hasta aquí mencionados, son el producto del estudio de casos históricos que han sido exitosos aplicando el velo y el engaño. Es posible, sin embargo, que esta enunciación de principios deba ser ampliada en la actualidad. Esta incorporación puede darse a través de la inclusión de nuevos principios o a la ampliación de los ya existentes.

De lo expresado, el principio de seguridad parecería quedar incompleto. Existe una necesidad de seguridad no contemplada en el enunciado anterior y que guarda relación directa con el seguimiento del accionar enemigo a los efectos de monitorear que las acciones de velo y engaño estén teniendo el resultado pretendido o no. No considerar este seguimiento implica la posibilidad de un riesgo superlativo de asumir que las acciones resultan exitosas convirtiéndose en una situación totalmente adversa ante el hecho que así no suceda.

Es pertinente considerar que el enemigo buscará obtener para sí, los mismos beneficios de la sorpresa. Por ello, no es de descartar que su plan de velo y engaño sea inducir a la propia fuerza que están actuando conforme a sus previsiones. Este caso sería el más exitoso de todos los relacionados con la sorpresa porque logrará concretar todos los principios anteriormente enumerados.

Para concretar este seguimiento, es indispensable orientar y dirigir esfuerzos de obtención de información hacia el accionar del enemigo. Lograr determinar con un relativo grado de certeza permite confirmar el éxito de las operaciones de velo y engaño y optimiza el principio de flexibilidad, puesto que genera más tiempo para la adaptación que demande un cambio en la situación.

Este concepto de seguimiento requiere una interacción con el órgano de dirección de inteligencia, reforzando el principio de coordinación.

Otro principio que refuerza la interacción con el órgano de inteligencia es el principio del conocimiento del adversario. Potencia las posibilidades de éxito el conocimiento del enemigo con tal profundidad que permite anticipar la interpretación del enemigo a las propias acciones. Confirmarle al enemigo con información falsa sus conjeturas iniciales para producir conclusiones erróneas. Lógicamente, las conjeturas iniciales del enemigo sobre las propias acciones estarán condicionadas por su propia personalidad, de ahí la conveniencia de un conocimiento profundo.

Es también necesario, dentro del conocimiento del adversario, saber que medios tecnológicos tiene a su disposición para obtener la información para poder, así, administrar convincentemente la información falsa a ser cedida y permitir su obtención con la mayor variedad posible de medios. Esto posibilitará la confirmación y proceso de inteligencia de ese enemigo.

Es necesario, además, considerar que la información que se facilita al enemigo tenga un mensaje unívoco, pero a la vez, no sea tan evidente que despierte sospechas su fácil obtención. Es por eso que se considera conveniente incluir un principio de coherencia para asegurar un mensaje que no contenga contradicciones en sí mismo posibilitando, así, conclusiones del enemigo no deseadas.

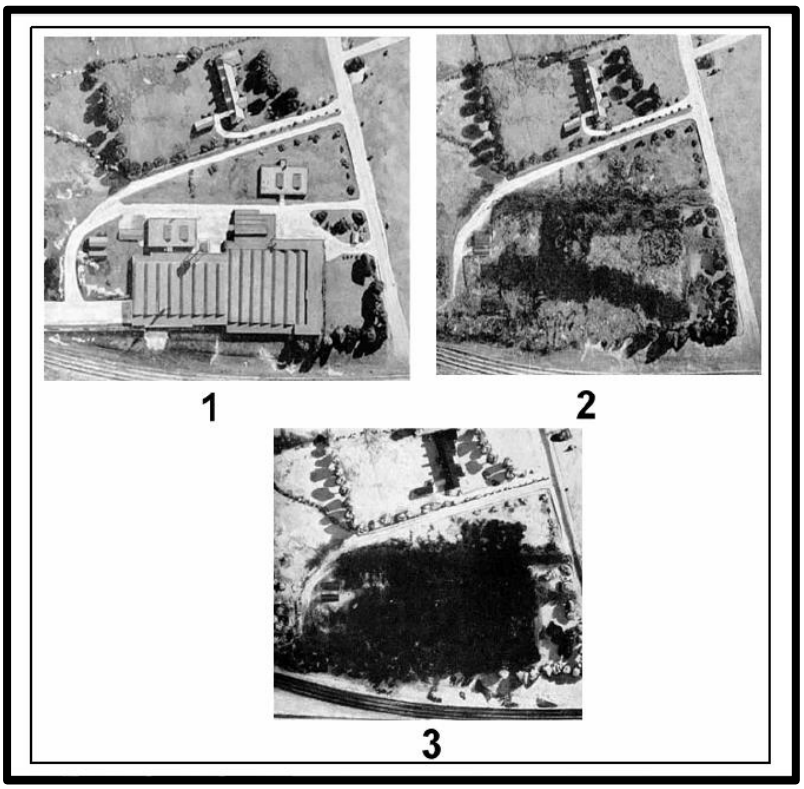
Esta necesidad de coherencia demanda que el plan de velo y engaño tenga un planeamiento dinámico y, por más que se ejecuten acciones preparatorias aún durante el planeamiento de las operaciones principales, demanda un ajuste final una vez terminado el plan de las operaciones principales. Siguiendo el principio de preparación, esos ajustes no deberían ser mayores y, por ende, mantendrían ese mensaje, aunque amplio, único.

Es conveniente entender al principio de preparación en un sentido más amplio. No solamente es indispensable considerar las medidas de velo y engaño desde la orientación del Comandante, sino que deberán prepararse las informaciones necesarias para restarle credibilidad a aquella información que, a priori, se sepa no se podrá ocultar. Este aspecto interactúa con los principios de conocimiento del enemigo y credibilidad. Así se genera un grado de incertidumbre en el enemigo tal, que éste no sabe que creer y que no.

Solamente se podrá afectar los medios tecnológicos de obtención del enemigo si se tiene un conocimiento lo más completo y actualizado de esos recursos que el enemigo dispone. Esto posibilita lograr investigar cómo burlar esos sistemas y poder determinar aquellos aspectos que no podrán ocultársele.

Un buen ejemplo de lo expresado se puede visualizar en una comparación de imágenes:

Imagen N°1: Ejemplos de velo y engaño




**Fuente:** Aguilar Huergo, Pablo *"Inteligencia de imágenes"* Op cit. p. 117.

En la foto 1 (con película pancromática) se puede observar una instalación sin que se le haya ejecutado ninguna acción de velo y engaño; en la foto 2 se puede observar, con la misma película, la instalación oculta y en la foto 3, con película infrarroja se puede detectar la vegetación empleada para ocultar el predio.

Este ejemplo, a través de las imágenes, demuestra como las acciones de enmascaramiento no son efectivas ante la integración y comparación de imágenes de distintos medios. La imagen infrarroja permite detectar fácilmente la vegetación empleada para disimular la instalación. No obstante, la imagen no permite identificar lo que en esa instalación se encuentra. La clave estará, entonces, en generar tantas imágenes como la foto N°3 que, por su número y ubicación, impidan determinar a los analistas definir con certeza cuál de todas es la verdadera.

Si estas acciones son constantes y adecuadamente planificadas, se puede lograr saturar el sistema de comando y control del enemigo, afectando de esta manera el proceso de toma de decisiones y evitando que, de esta manera, pueda anticiparse quedando condenado a reaccionar a las acciones propias.

Evidentemente, un plan de velo y engaño que cumpla con todos estos requisitos demanda una asignación de medios humanos y materiales comparables por su mag-

nitud, con las destinadas a ejecutar las operaciones principales. La diversidad de sensores actualmente disponibles incrementa aún más las fuerzas empeñadas en lograr la sorpresa.

Este concepto hace que se refuerce la sentencia de Clausewitz sobre el costo en la asignación de medios para el desarrollo de estas operaciones en el nivel operacional. No obstante, en la actualidad, un Comandante operacional está condicionado por restricciones impuestas por la Estrategia Nacional y Militar, en especial en el marco de un estado democrático. El tiempo que demande la campaña, preferentemente breve, en la búsqueda del Objetivo Operacional será normalmente una imposición cada vez más observada.

Otra restricción, cada vez más frecuente en los conflictos actuales, es la cantidad de bajas humanas como consecuencia del conflicto. Las actuales sociedades nacionales, como la República Argentina, valoran más la vida del ser humano. Involucrar al estado en una guerra indefinida en el tiempo y con una elevada expectativa de muertes, puede afectar la política interior de la Estrategia Nacional y, por ende, el nivel operacional.

Una guerra prolongada, aparte de provocar muchas muertes, puede desestabilizar la economía nacional, debilitar una administración ante la opinión pública, hacer perder elecciones. Este aspecto, que condiciona al más alto nivel de la estrategia nacional, tiene repercusiones en el diseño de una campaña, propia del nivel operacional.

Estos condicionantes anteriormente mencionados, duración de la campaña y expectativa de bajas, se presentaron como determinantes en el diseño operacional en los casos de ambas "Guerras del Golfo", Afganistán y posteriores. Tanto condicionaron, que terminó siendo la Estrategia Nacional instancia de decisión al respecto.

"El general Franks se enfrentó a dos preguntas clave: ¿Había forma de ser más eficiente y concentrar una mayor fuerza militar en menos tiempo? ¿Podía usarse menos fuerzas para cumplir los objetivos?"[6] La respuesta a estos interrogantes estaba en la búsqueda de la sorpresa a través del velo y el engaño. La superioridad tecnológica de la coalición, favorecía este tipo de operaciones.

Esta circunstancia evidencia una nueva caracterización de los "costos" de la guerra estableciendo nuevos parámetros de aceptabilidad aparte de la cantidad de fuerzas empleadas en el logro del estado final deseado. En especial a partir que, por el desa-

[6] Woodward, Bob *"Plan de ataque: cómo se decidió invadir Iraq"*. Traducido por M Pino. Ed Planeta. Barcelona, 2004, p.57

rrollo tecnológico, esas fuerzas no implican mayor empleo de seres humanos. Es por eso que, actualmente, el diseño de una campaña busca afectar sus fortalezas indirectamente, actuando sobre aquellos factores que lo configuran como fortaleza de tal manera de debilitarla en sus vulnerabilidades.

## *CONCLUSIONES FINALES.*

Un adecuado sistema de seguridad en el nivel operacional presupone la integración de todos los medios tecnológicos a disposición del Comandante Operacional. Esta diversidad de medios hace que los recursos anteriormente empleados para lograr el engaño como el enmascaramiento o simulaciones no sean totalmente efectivos; no obstante, es conveniente seguir considerándolos para dificultar el análisis del enemigo en el proceso de inteligencia.

Se hace cada vez más difícil velar al enemigo información ante la nueva tecnología. Evitar la detección del enemigo, con los recursos tecnológicos actuales demanda un esfuerzo que no muchos considerarían como aceptable. A pesar de ello, parece bastante más sencillo cegar la observación del enemigo en determinados sectores. Si esta capacidad es ejercida en lugares que permita sembrar la duda sobre las previsiones de empleo propio, pueden ser un recurso válido en procura de la sorpresa.

La búsqueda de la sorpresa mediante acciones de velo y engaño implica, en todos los casos, asumir riesgos. Éstos deben ser calculados para que el Comandante tenga elementos de juicio válidos para resolverse sobre su adopción o no. Asumir esos riesgos calculados en procura de una ventaja es una decisión del Comandante. Mucho influirá, en este sentido, la personalidad del decisor y las opciones que estén a su disposición.

Asumir riesgos calculados, independientemente de las opciones disponibles, implica afrontar con audacia una situación que puede no desenlazar favorablemente. Es por eso que influye la personalidad del decisor, porque denota audacia.

Cada vez resulta más dificultoso negar información al enemigo no obstante, es posible lograrlo impidiendo el despliegue y accionar de los medios que transportan o posibilitan la operación de los sensores. De esta manera, limitando o impidiendo el vuelo de las aeronaves que portan los sensores, podrá reducirse la capacidad de obtención de información del enemigo. Un adecuado sistema de Defensa Antiaérea cobra valor en este sentido. Otra opción es afectar sus sistemas de comunicación para que la información llegue distorsionada o fuera de la oportunidad en que es necesaria.

Las actuales posibilidades de engaño se encuentran en permitir al enemigo acceder a tanta información que por su volumen, coherencia, credibilidad y oportunidad generen en el enemigo confusión y saturen su sistema de comando y control. Para que

sea efectivo, el plan de velo y engaño necesita contemplar acciones que posibiliten obtener información falsa de tal manera que resulte más convincente que la verdadera.

Como ya de demostró, ante la imposibilidad de evitar la detección, podrá procurarse el engaño generando tantos blancos falsos a la vigilancia del enemigo que desvíe esfuerzos y pierda tiempo en determinar cuál de todos son los reales. Ese esfuerzo, que demanda direccionar medios para la obtención y, fundamentalmente tiempo, generarán una demora en la confirmación que obligará al enemigo a avanzar en su planeamiento empleando suposiciones cubriendo esos "vacíos" de información. La elaboración de esas suposiciones estará condicionada por la forma de interpretar la guerra del enemigo.

Conociendo los sistemas que dispone el enemigo, es posible que, considerando la mayor diversidad posible, se permita la obtención de información de imágenes, comunicaciones, movimientos terrestres y zonas "oscurecidas" que lleven a la interpretación pretendida. Para que esta información sea creíble, debe ser dosificada de manera, aparentemente, inconexa y en oportunidades que no den lugar a sospechas sobre la falsedad que éstas contienen.

Es necesario asegurar un mensaje unívoco reduciendo el riesgo de situaciones no deseadas como resultado de interpretaciones del enemigo diferentes a las pretendidas.

El seguimiento y monitoreo de la evolución en el accionar del enemigo se presenta como un recurso de gran valor para incrementar la propia flexibilidad y reforzar la seguridad estableciendo la eficacia de las operaciones de velo y engaño en procura de la sorpresa.

Un eficiente plan de velo y engaño demanda de acciones permanentes. Aún en tiempo de paz resulta indispensable estudiar al adversario, real o potencial, para poder establecer un patrón de pensamiento del actor opuesto y elaborar un convincente mensaje que confirme sus suposiciones, pero que no refleje la realidad de las previsiones propias.

Este estudio del enemigo no implica violar ninguna frontera. Consiste en actualizar el conocimiento del material que incorpora, estudiar sus reglamentos, emplear la misma vigilancia a través de satélites de la forma en que el enemigo se entrena, cuáles son las operaciones más practicadas, que obras de preparación territorial realiza, etc. Fundamentalmente, este estudio necesita abarcar guerra electrónica. Poder identificar

rango de frecuencias en que el enemigo transmite información – en cualquiera de sus formas – es de gran valor para poder afectar su sistema cuando sea oportuno.

Asimismo, un conocimiento profundo de los medios del enemigo para obtener información, posibilitará facilitar la información falsa y tomar previsiones sobre lo que no se puede ocultar. Como ya se demostrara, obliga a diferentes acciones de velo y engaño la disponibilidad de diferentes tipos de sensores a ser empleados en la vigilancia del nivel operacional. Existen medidas de enmascaramiento y simulación que son efectivas para vulnerar una gama limitada de sensores. Será necesario prever medidas para aquello que, del estudio previo de sus medios, se determine que no se pueda ocultar a su detección.

Otro recurso para lograr la sorpresa es disponer de fuerzas que por su magnitud, ubicación, medios disponibles y/o movilidad estén en capacidad de ser empleados en diferentes posibles lugares. A pesar que el enemigo descubra su real existencia, deberá destinar fuerzas para neutralizar esos medios en todas las posibilidades de empleo. Difícilmente, los medios destinados por el enemigo para este fin sean suficientes debiendo establecer prioridades para su asignación. De esta manera, un elemento de magnitud considerable de fuerzas paracaidistas o de asalto aéreo; el posicionamiento de buques de desembarco próximos a una playa, puede que no se necesiten ocultar al enemigo para lograr el efecto de engaño pretendido.

Lograr planificar y conducir operaciones militares con mayor rapidez que el enemigo hace que éste pierda su libertad de acción reaccionando a la propia iniciativa. Pero esta situación es muy difícil de mantener por un tiempo prolongado.

Velo, engaño y rapidez de la acción son parte de los requisitos para lograr la sorpresa, dislocarlo previamente en todo lo que sea posible.

Los desarrollos tecnológicos son ambivalentes: por un lado proveen ventajas para aquel bando que tiene acceso a fuentes de información especiales, tales como satélites de vigilancia u otros medios especializados, pero por otra parte, el ser dependiente de las tecnologías modernas, representa nuevas vulnerabilidades que pueden ser explotadas por aquel bando inferior en estos campos. Cuando se incorpora tecnología de avanzada, normalmente, existe una tendencia de superación de lo anterior. El uso continuo de estos, como parte del adiestramiento, hace que se dejen de lado la práctica de métodos “más tradicionales” indispensable como reaseguro del sistema. De esta manera, se produce “un corte” en la cadena del conocimiento condenando todo el sistema de seguridad a un único componente – tecnológico – aplicado a la seguridad estratégica.

Esto fue una de las mayores enseñanzas de los organismos de seguridad estratégica de los EEUU después del 11-S, revalorizando nuevamente la "inteligencia humana" dejada de lado como consecuencia de una carrera tecnológica.

El obstáculo de la sorpresa, más que la tecnología, está en la capacidad de quienes la emplean, en su imaginación para desarrollar nuevos procedimientos y planes de operaciones originales. El límite está, en consecuencia, en el hombre más que en los sensores.

De todo lo expresado es posible concluir que, la sorpresa es posible lograr en el nivel operacional a pesar de las nuevas tecnologías de la información. Que la posibilidad de lograr vulnerar esos recursos tecnológicos demanda un conocimiento actualizado y permanente de las capacidades del enemigo en la seguridad operacional. Aprovechando el conocimiento de sus sensores disponibles, cederle información falsa en forma convincente que, preferentemente, confirme sus suposiciones sobre el propio actuar. Desacreditando ante sus ojos aquello que no se pueda ocultar y disponiendo fuerzas en condiciones de proyectar su accionar en tantos lugares y en oportunidad que impida al enemigo abarcar todas ellas haciendo que priorice una previsión de empleo equivocada.

## *BIBLIOGRAFÍA.*

**Libros:**


- Clausewitz, Carl, *"De la guerra"*. Dirigida por Michael Howard y Peter Paret. Traducido al español por Celer Pawlowsky. Ministerio de Defensa de España. Madrid, 1999.
- Lidell Hart, Basil Henry, *"Estrategia de la aproximación indirecta"*. Traducida por Carlos Botet. Iberia Editores SA. Barcelona, 1946.
- Marín, Francisco A "Engaños de guerra – Las acciones de decepción en los conflictos bélicos" Inéditas Editores, Barcelona, 2004.
- Marti Sempere, Carlos, *"Tecnología de la defensa"*. Instituto universitario "General Gutierrez Mellado". Madrid, 2006.
- Pertusio, Roberto *"Estrategia Operacional"* Instituto de Publicaciones Navales. Buenos Aires, 2005.
- Sun Tzu, *"El arte de la guerra"*. Edición Fernando Puell, Buenos Aires, 2001.
- Woodward, Bob *"Plan de ataque: cómo se decidió invadir Iraq"*. Traducido por M Pino. Ed Planeta. Barcelona, 2004.


**Reglamentos militares:**


- Ejército EEUU, C 300 Joint, Interagency, Intergovernmental and Multinational (JIIM) Capabilities Theme. Escuela de Guerra y Estado Mayor del Ejército EEUU, 2008.
- Ejército EEUU, C 500 Joint Functions Theme. Escuela de Guerra y Estado Mayor del Ejército EEUU, 2008.
- Ejército EEUU, F 100 Managing Army Change. Escuela de Guerra y Estado Mayor del Ejército EEUU, 2008.
- EMCFFAA Argentina, MC 20-01 Manual Estrategia y Planeamiento – Nivel Operacional. ESGC, Ed 2011.
- Ejército EEUU, Operational Combat Service Support. Escuela de Guerra y Estado Mayor del Ejército EEUU, 2006.
- Ejército Argentino, RB 00-01 Reglamento de conducción para el instrumento militar terrestre, Ed 1992.
- Ejército Argentino, RC 00-02 Diccionario para la acción militar conjunta, Ed 1999.

- Ejército Argentino, RFD 99-01 Terminología castrense de uso en el Ejército Argentino, Ed 2001.

**Otros:**

- Aguilar Huergo, Pablo *"Inteligencia de imágenes"* Instituto de Inteligencia de las FFAA Argentinas, Buenos Aires, 2007
- Canevaro, José María *"El velo y el engaño y la sorpresa en el nivel estratégico operacional"* Trabajo de investigación, Escuela Superior de Guerra. Buenos Aires, 2004.
- Castagno, Juan Domingo *"El velo y el engaño"*. La Revista. Escuela Superior de Guerra. Buenos Aires, ene-mar 2007.
- Hutchinson, William "*Information warfare and deception"* Edith Cowan University. Perth (Australia), 2006.
- Johnson, Mark – Meyeraan, Jessica *"Military deception: Hiding the real – showing the fake"* Joint Forces Staff College. Nolfolk (EEUU), 2003.
- Ley de Defensa Nacional (número 23.554) de la República Argentina. Buenos Aires, 1988.
- Zubeldía, Ignacio *"Los planes y operaciones de velo y engaño en el teatro de operaciones"* Trabajo de investigación, Escuela Superior de Guerra conjunta. Buenos Aires, 2010.