APUNTES DE INTELIGENCIA, CONTRAINTELIGENCIA Y SEGURIDAD.

FASE CONJUNTA DEL CURSO DE ACTUALIZACIÓN DE ASCENSO A COMANDANTE .

DEPARTAMENTO DE INTELIGENCIA Y SEGURIDAD

16 de octubre de 2014

ESCUELA SUPERIOR DE LAS FUERZAS ARMADAS

PAGINA INTENCIONADAMENTE EN BLANCO

APUNTES DE INTELIGENCIA, CONTRAINTELIGENCIA Y SEGURIDAD.
FASE CONJUNTA DEL CURSO DE ACTUALIZACIÓN DE ASCENSO A COMANDANTE.

Estos apuntes son un extracto de las definiciones, conceptos y principios establecidos en la publicación AJP-2(A) "Allied Doctrine for Intelligence, Counter-Intelligence and Security", ratificado por España y pendiente de implementación, con el único objetivo de ser una ayuda a la enseñanza y establecer los conocimientos que debe tener alumno antes de acceder a la fase de presente.

Son unos apuntes, por lo que no se debe considerar una publicación oficial, para resolver cualquier duda o ante cualquier necesidad de ampliar lo señalado es necesario consultar el AJP-2(A).

ÍNDICE

PAGINA INTENCIONADAMENTE EN BLANCO

1. GENERALIDADES DE INTELIGENCIA.

La unión de la inteligencia con el conocimiento de las capacidades propias, y las de nuestros aliados, proporciona el fundamento del planeamiento y la ejecución de las operaciones.

La inteligencia hoy no solo consiste en catalogar las fuerzas de un adversario y evaluar sus capacidades. También abarca el entendimiento de la cultura del adversario, su motivación, perspectiva y objetivos.

2. CONTEXTO DEL ENTORNO OPERACIONAL.

Actores clave y amenazas que definen los entornos operacionales:

- Terrorismo.
- Estados hostiles.
- Estados frágiles y fallidos.
- Amenazas híbridas.
- Globalización.
- Medioambientales y humanitarias.
- Proliferación.

La necesidad de inteligencia. La complejidad de las operaciones modernas produce una necesidad de integrar la inteligencia con otras actividades en un gran abanico de fuentes y órganos para generar el entendimiento del entorno operacional. Inteligencia contribuye a tres tareas núcleo de la OTAN: defensa colectiva, gestión de crisis y seguridad cooperativa.

3. FACTORES QUE AFECTAN A LA INTELIGENCIA.

Las tres principales áreas de impacto son:

- La complejidad de las operaciones.
- Abundancia de información.
- Difusión de las fronteras tradicionales de los niveles táctico, operacional y estratégico.

4. EL ENFOQUE INTEGRAL.

Los organismos de inteligencia deben poder producir inteligencia basada en un amplio abanico de factores. Para ello necesitarán apoyarse en expertos para apuntalar sus análisis o en el apoyo reach-back (desde fuera del área de operaciones) para apoyar a los mandos y organizaciones, incluidas las no militares y no gubernamentales.

5. ENTENDIMIENTO[1].

El entendimiento es la percepción e interpretación de una situación particular con el fin de proporcionar el contexto, punto de vista y previsión necesarios para la toma de decisión. Esto incluye contestar las cuestiones principales quién, qué, donde, cuando, por qué y cómo, que proporcionan el contexto y la narrativa de los sucesos.

La valoración de la situación es el término general utilizado cuando un decisor a cualquier nivel tiene el correcto nivel de entendimiento y la habilidad para poner nuevos datos e información dentro del contexto para tomar decisiones racionales y ejecutar acciones.

6. DATOS E INFORMACIÓN.

La información se define como datos de todo tipo sin procesar que se pueden utilizar en la producción de inteligencia.

7. EL MANDO, INTELIGENCIA Y TOMA DE DECISIÓN.

Responsabilidades de inteligencia del mando. La responsabilidad definitiva de inteligencia yace en el mando. Los mandos deben familiarizarse con el proceso de inteligencia y tener una valoración de la situación suficiente para articular sus necesidades de información crítica. Es responsabilidad del mando proporcionar dirección y guía, definir prioridades, dotar la obtención y el análisis de inteligencia efectivamente, exigir la mayor calidad de los productos y revisar los efectos de sus acciones escogidas.

El mando y la toma de decisión. Un buen mando debe saber que:

- Es inevitable una correlación y una interdependencia entre la calidad y la oportunidad.
- Los comandantes no deben delegar sus decisiones.
- Las buenas decisiones se derivan de la formación y la experiencia.
- Los organismos asesoran a la toma de decisión del mando y esto necesita mutua confianza entre unos y otros.

Visión del mando. Es la capacidad de crear una imagen mental del futuro utilizando la imaginación y sabiduría. Proporciona el contexto para el desarrollo de conocimiento a todos los niveles y para determinar el nivel del apoyo de inteligencia necesario.

Intención del mando. Es la expresión clara y concisa del mando de lo que debe hacer la fuerza y las condiciones que debe establecer para cumplir su misión.

Promoción del acceso a la inteligencia. Enfocar el esfuerzo de la inteligencia y lograr la difusión puntualmente siempre será un reto para el mando.

[1] En el AJP-2(A) se utiliza el término “Understanding”.

Los mandos deben crear una atmósfera que permita una mentalidad abierta. Análisis crítico y pensamiento creativo.

8. DEFINICIÓN DE INTELIGENCIA.

Inteligencia es el producto resultante de la obtención directa y elaboración de la información relativa al entorno y capacidades e intenciones de los actores con el fin de identificar amenazas y ofrecer oportunidades para la explotación por los decisores.

La función de combate inteligencia comprende el conjunto de actividades encaminadas a satisfacer las necesidades de conocimiento del Mando, relativas al entorno operativo, necesarias para el planeamiento y conducción de las operaciones, así como para la identificación de las amenazas contra las fuerzas propias y el cumplimiento de la misión.

Debe categorizarse basándose en su uso intencionado. En consecuencia, hay tres definiciones específicas de inteligencia a estos niveles:

- Inteligencia estratégica. Inteligencia necesaria para la formación de política, planeamiento militar y la provisión de indicios y alertas, a nivel nacional e internacional.
- Inteligencia operacional. Inteligencia necesaria para el planeamiento y conducción de campañas de nivel operacional.
- Inteligencia táctica. Inteligencia necesaria para el planeamiento y ejecución de operaciones a de nivel táctico.

9. PAPEL Y FUNCIONES DE LA INTELIGENCIA.

El papel de la inteligencia es contribuir al conocimiento continuo y coordinado en un complejo entorno global para facilitar las decisiones apropiadas que permitan a la OTAN tomar las acciones necesarias para mantener la seguridad. Es una ayuda para desarrollar el entendimiento y una herramienta crítica para la toma de decisiones.

Las funciones principales de la inteligencia son:

- Desarrollo de conocimiento y facilitar el entendimiento. Desarrolla el conocimiento sobre el entorno y los actores, incluyendo sus intenciones, capacidades y motivaciones.
- Producción de valoraciones predictivas. La inteligencia debe mirar adelante facilitando al mando mantener la iniciativa. A pesar de todo, la revisión de las actividades pasadas y actuales puede indicar intenciones futuras y deben utilizarse coherentemente.

10. CATEGORIZACIÓN DE LA INTELIGENCIA.

Inteligencia Básica. Inteligencia sobre cualquier asunto, que puede ser utilizada como referencia material para el planeamiento y como una base para elaborar información o inteligencia subsecuente. La inteligencia básica proporciona el contexto y telón de fondo sobre que revisar la inteligencia actual.

Inteligencia Actual. Esla que refleja la situación actual a cualquier nivel, estratégico o táctico. Los informes y sumarios de inteligencia proporcionan inteligencia actual para la Representación Común Operacional (Common Operational Picture – COP) y predicciones para posibles desarrollos.

11. PRINCIPIOS DE INTELIGENCIA.

Accesibilidad. La inteligencia no tiene valor si no se difunde, o es accesible, a aquellos que la necesitan.

Compartir. Hay mecanismos necesarios por los que la inteligencia pueda ser compartida, de forma puntual, dentro de la OTAN y con entidades no OTAN guiados por la idea de necesidad de compartir de acuerdo con la política de seguridad OTAN en vigor. La fuente de la información debe protegerse y la propia información debe filtrarse para proteger a la fuente con el fin de compartir información con otros.

Capacidad de respuesta. Los organismos de inteligencia deben poder analizar, fusionar, elaborar y presentar productos rápidamente para decisores militares y no militares.

Flexibilidad. Los organismos de inteligencia deben establecer una representación que proporciona inteligencia puntualmente, relevante y enfocada, diseñada para evolucionar con los retos de seguridad.

Interoperabilidad. Procesos, redes y sistemas comunes o interoperables son necesarios para apoyar la dirección, obtención, elaboración y difusión de la inteligencia, y la gestión de la organización de la inteligencia.

Integridad. La inteligencia debe ser integral en su naturaleza y debe explicar los elementos interrelacionados de un entorno operacional complejo de manera imparcial sin distorsiones. Para conseguir una inteligencia integral la OTAN utiliza el modelo PMESII, Político, Militar, Económico, Social, Infraestructura e Información.

12. ATRIBUTOS DE INTELIGENCIA.

La inteligencia es dirigida por el mando. La inteligencia es una responsabilidad fundamental del mando.

La inteligencia es colaborativa. La inteligencia tiene la capacidad de extraer las habilidades de un amplio espectro de expertos y especialistas en una variedad de organizaciones.

La inteligencia es oportuna. La inteligencia debe entregarse a tiempo.

La inteligencia es fusión. Un enfoque de múltiples fuentes utiliza el concepto de fusión de inteligencia para optimizar el valor de varias fuentes de información.

La inteligencia es objetiva. La inteligencia siempre debe evitar la parcialidad, necesitando organismos con mentes abiertas.

13. LIMITACIONES DE LA INTELIGENCIA.

Gestión de las expectaciones. Los organismos de inteligencia deben ser realistas sobre que puede conseguirse a través de la actividad de inteligencia, especialmente cuando los recursos son limitados.

Inteligencia Incompleta. La inteligencia puede no satisfacer las necesidades del mando exactamente y puede no ser completamente apropiada, completa o corroborada fácilmente.

Medios de obtención. Todos los medios de obtención, explotación y elaboración tienen limitaciones.

Capacidades e intenciones. En los entornos operacionales contemporáneos y futuros, los organismos de inteligencia deben asegurar que los mandos entienden el incremento de dificultad de determinar las capacidades adversarias, centros de gravedad, redes e intenciones.

Restricciones nacionales. Bajo ninguna circunstancia los mandos o sus organizaciones deben asignar a las naciones contribuyentes llevar a cabo actividades que sean contrarias a sus legislaciones.

Legislación Internacional. Toda actividad de inteligencia debe conducirse dentro de este marco legal.

14. ORGANOS, FUENTES Y SENSORES.

Una fuente es una persona o cosa de la que puede obtenerse información. Las fuentes pueden dividirse en controladas, incontroladas o casuales:

- Controladas. Las fuentes controladas están bajo el control de un órgano de inteligencia.
- Incontroladas. Las fuentes incontroladas son aquellas que no están bajo el control formal de una agencia de inteligencia u organización.
- Fuentes casuales. Las fuentes casuales proporcionan información no solicitada.

Protección de la fuente. La protección de la fuente es crítica donde están involucradas capacidades de obtención encubiertas. Sin embargo, la protección de fuentes no debe ser una razón para retener inteligencia..

Órganos. Un órgano es una organización involucrada en la obtención o elaboración de la información. Un órgano debe ser capaz de obtener y elaborar información o simplemente puede tener la capacidad de obtener información y pasar esa información a otro órgano para su elaboración.

Sensores. Son entidades o partes de equipos que detectan, y pueden indicar y/o grabar objetos y actividades por medio de la energía o partículas emitidas, reflejadas o modificadas por objetos.

Inteligencia de Fuentes simple y múltiple. La mayoría de la inteligencia se deriva de una sola fuente. Sin embargo hay significantes ventajas en que se derive de la utilización de inteligencia de fuentes múltiples (MULTI-INT).

Célula Nacional de Inteligencia (NIC). Una NIC es una capacidad que está equipada y organizada por una nación para proporcionar apoyo nacional de inteligencia dentro de un mando OTAN. También puede ser añadida a un cuartel general OTAN desplegado o permanente.

15. GESTIÓN DE LA INFORMACIÓN.

Gestión de la información. Es la supervisión, administración, regulación y difusión puntual de la información. Todo el personal dentro del proceso de gestión debe entender el contexto de la información que está manejando con el fin de gestionarlo efectivamente.

Efecto de la tecnología. La tecnología moderna ha revolucionado el flujo de la información. Esto proporciona al mando nuevas y significativas capacidades que pueden entregar una ventaja operativa potenciando el alcance, velocidad y volumen de los soportes, proporcionando nuevos formatos para la información e incrementando la capacidad de manipular la información.

16. INTELIGENCIA, VIGILANCIA Y RECONOCIMIENTO CONJUNTO.

La inteligencia, vigilancia y reconocimiento conjunto (JISR). Es un paquete integrado de capacidades de inteligencia y operaciones que sincroniza e integra el planeamiento y operaciones de todas las capacidades de obtención con la elaboración y difusión de la información resultante en apoyo directo al planeamiento, preparación y ejecución de las operaciones.

Hay tres tipos de capacidad de obtención:

- Inteligencia. Los medios de inteligencia tienen la capacidad de obtener y analizar la información.
- Vigilancia. Se define como la observación sistemática del espacio aéreo, áreas de superficie o debajo de la misma, lugares, personas o cosas, por medios visuales, electrónicos, fotográficos o de otro tipo. La vigilancia se lleva a cabo contra adversarios potenciales y conocidos y amenazas así como en apoyo de operaciones en áreas de crisis actuales y potenciales.
- Reconocimiento. Se define como una misión llevada a cabo para obtener, por observación visual u otros métodos de obtención, información sobre las actividades y recursos de un enemigo o

enemigo potencial, o para asegurarse de datos relativos a las características meteorológicas, hidrográficas o geográficas de un área en particular.

Arquitectura JISR. La arquitectura JISR de la OTAN consiste en las organizaciones, procesos y sistemas que conectan las unidades de obtención, bases de datos, aplicaciones, generadores y consumidores de inteligencia y datos operacionales en un entorno conjunto.

El JISR es multidisciplinar y su intención es extraer inteligencia, vigilancia y reconocimiento de las capacidades de obtención en un total coherente, proporcionando un marco de trabajo para la coordinación y asignación de tareas a estos medios. El JISR debe ser interoperable con otros dominios y funciones, incluyendo sus respectivos sistemas.

La organización, a todos los niveles de mando, debe tener la capacidad de:

- Definir la arquitectura necesaria para ejecutar eficientemente JISR.
- Articular el apoyo CIS necesario para el intercambio de datos requerido.
- Asesorar y encontrar las capacidades y limitaciones de los medios JISR disponibles contra las capacidades necesarias.
- Coordinar entre las divisiones de inteligencia, operaciones, planes y CIS y otras divisiones relevantes.
- Gestionar sucesos críticos en el tiempo.

17. DISCIPLINAS DE OBTENCIÓN Y PRODUCTOS DE INTELIGENCIA.

Disciplinas de obtención son los medios o sistemas utilizados para observar, sensorizar y grabar o reunir información de condiciones, situaciones, amenazas y eventos. Las principales disciplinas de obtención son:

- Inteligencia Acústica (ACINT) es la inteligencia derivada de la obtención y elaboración del fenómeno acústico. La ACINT está principalmente relacionada con el movimiento y la inteligencia que se puede derivar de su detección.
- Inteligencia Humana (HUMINT) es una categoría de inteligencia obtenida y proporcionada por fuentes humanas. Las actividades HUMINT abarcan la obtención, informe y análisis integrado dentro de la inteligencia general para proporcionar a los decisores de la información puntual y adecuada necesaria para llevar a cabo con éxito operaciones militares.
- Inteligencia de Imágenes (IMINT) es la inteligencia derivada de las imágenes adquiridas con sensores que pueden estar basados en tierra, embarcados o llevados en plataformas aéreas o espaciales. La información reunida en una imagen o en un video es clara y concisa. A menudo servirá para apoyar o confirmar la inteligencia derivada de otras fuentes.
- Inteligencia de medidas y firmas (MASINT) es inteligencia e información científica y técnica obtenida por el análisis cuantitativo y cualitativo de datos obtenidos de instrumentos de detección con el propósito de identificar cualquier característica distintiva asociada a la fuente emisora o remitente para facilitar la posterior medición e identificación. MASINT se deriva de la obtención y

comparación de un amplio abanico de emisiones con una base de datos científicos y técnicos conocidos con el fin de identificar el equipamiento o fuente de las emisiones.

- Inteligencia de Fuentes Abiertas (OSINT) es la inteligencia derivada de información pública disponible, así como otra información no clasificada que tenga limitada el acceso o distribución pública.
- Inteligencia de Señales (SIGINT) es la inteligencia derivada de la obtención y explotación de señales o emisiones extranjeras., se utiliza este término cuando no es necesario diferenciar entre inteligencia de comunicaciones (COMINT) e inteligencia electrónica (ELINT) que se definen como:
    - COMINT es la inteligencia derivada de comunicaciones electromagnéticas y sistemas de comunicaciones por los no usuarios o receptores destinatarios.
    - ELINT es la inteligencia derivada de transmisiones electromagnéticas que no son comunicaciones por los no usuarios o receptores destinatarios.

Productos de inteligencia. Los productos especializados de inteligencia incluyen, pero no se limitan a:

- Inteligencia de Fuerzas Armadas.
- Inteligencia relativa a CBRN (Química, Biológica, Radiológica y Nuclear).
- Inteligencia forense y biométrica.
- Inteligencia Geoespacial.
- Inteligencia Médica.
- Inteligencia Científica y técnica (STI).
- Inteligencia Técnica (TECHINT)
- Inteligencia de Seguridad (SI).
- Inteligencia de objetivos.

Información Geoespacial sobre los hechos georeferenciados por la posición geográfica y dispuesta en una estructura coherente. Puede estar disponible en formato digital o analógico.

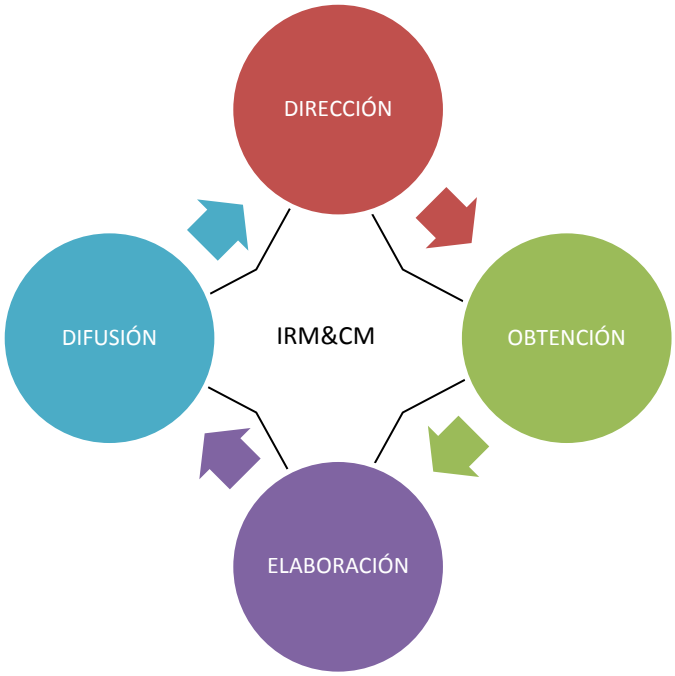
Información sociológica y cultural relativa a los factores de geografía humana, social y cultural. Estos factores incluyen población, político, económico, étnico, estratificación social, estabilidad, opinión pública, educación, religión, salud, historia, lenguaje, valores, percepciones y conducta.

18. EL CICLO DE INTELIGENCIA.

El ciclo de inteligencia es la secuencia de actividades por las que se obtiene información, se reúne, se convierte en inteligencia y se pone a disposición de los usuarios. Se focalizan en cuatro fases fundamentales: dirección, obtención, elaboración y difusión. En realidad es un paquete complejo de actividades que comprenden varios ciclos operando a diferentes niveles y velocidades. Algunas tareas se solapan y coinciden de forma que se llevan a cabo concurrentemente más que secuencialmente.

El ciclo consiste en cuatro fases:

- Dirección. Se define como la determinación de las necesidades de obtención, planeamiento del esfuerzo de obtención, el uso de órdenes y solicitudes a los órganos de obtención y el mantenimiento de una revisión continua de la productividad de esos órganos. La dirección es la clave del proceso de inteligencia. Hay dos tipos diferentes de dirección necesarios para que el proceso funcione: la dirección interna y la externa. La dirección externa proviene de los mandos de cada nivel y asienta los parámetros de las necesidades de inteligencia y objetivos. La dirección interna proviene del oficial superior de inteligencia a cada elemento especializado del organismo de inteligencia.
- Obtención. Se define como la explotación de fuentes por los órganos de obtención y la entrega de información obtenida la unidad de elaboración apropiada para la producción de inteligencia. Los medios ISR también pueden contribuir. La actividad de obtención necesita estrecha colaboración entre la inteligencia y la organización del mando para optimizar la utilización de los medios de obtención.



- Elaboración. Se define como la conversión de información en inteligencia a través de la compilación, evaluación, análisis, integración e interpretación. La elaboración es iterativa y puede generar posteriores solicitudes de obtención antes de la difusión de inteligencia.
- Difusión. Se define como la entrega puntual de la inteligencia en la forma apropiada, y por cualquier medio adecuado, a aquellos que la necesitan. También requiere seguridad, conformidad con las necesidades del demandante y un mecanismo de retroalimentación.

Como se muestra en el diagrama, la gestión efectiva del ciclo de inteligencia y la coordinación de las cuatro fases se lleva a cabo a través del proceso de Gestión de las Necesidades de Inteligencia y Gestión de la Obtención (IRM&CM). Es necesario señalar que las necesidades de inteligencia (IR) proporcionan la racionalización y priorización de cualquier actividad de inteligencia así como proporcionar el detalle para permitir al organismo de inteligencia responder a la necesidad de la forma más efectiva. Las necesidades de inteligencia deben cubrir todo el abanico de información del espectro PMESII. Los tipos de necesidades de inteligencia militares son:

- Necesidades Críticas de Información del Mando (CCIR – Commander`s Critical Information Requirements). Es la información relativa a las áreas críticas para el éxito de la misión o representan una amenaza crítica. Las CCIRs cubren todos los aspectos que atañen al mando, incluyendo las necesidades de Información de las Fuerzas propias (FFIR), Elementos Esenciales de Información Propia (EEFI) y las Necesidades Prioritarias de Inteligencia (PIR).

- Necesidades Prioritarias de Inteligencia (PIR – Priority Intelligence Requirements). Son una parte vital de las CCIRs y normalmente se formulan por los organismos de inteligencia en estrecha colaboración con el mando. Las PIR abarcan aquellas necesidades de inteligencia por las que un mando tiene una prioridad establecida.
- Necesidades específicas de Inteligencia (SIR – Specific Intelligence Requirements). Apoyan y complementan cada PIR proporcionando una descripción más detallada de la necesidad. Se utilizan por el organismo de inteligencia para determinar qué medio de inteligencia, fuente o disciplina que puede satisfacer de la mejor manera la necesidad e identificar la coordinación necesaria para asegurar el apoyo de los medios apropiados.
- Elementos Esenciales de Información (EEI – Essential Elements of Information). Las SIR se descomponen en preguntas más detalladas conocidas como EEIs. Los EEIs añaden los detalles a las SIR y permiten la producción de una lista de asignación de tareas de obtención basada en el plan de obtención de inteligencia.

19. ÁREAS DE INTELIGENCIA CONJUNTA.

El área operacional conjunta se divide en tres áreas:

- Área de Operaciones (AOO). Es un área definida por el jefe de la fuerza conjunta dentro de un área de operaciones conjunta para la conducción de actividades militares específicas.
- Área de responsabilidad de Inteligencia. Es un área asignada a un comandante, en la que es responsable de proporcionar inteligencia con los medios a su disposición.
- Ciberespacio. Dentro del Entorno Operacional general, el ciberespacio trasciende de nuestros conceptos de fronteras políticas o geográficas. Por lo tanto, los mandos deben considerar el ciberespacio como un área por sí misma.

20. LA AMENAZA A LA SEGURIDAD.

Seguridad es la condición conseguida cuando información designada, materia, personal, actividades e instalaciones están protegidos contra el espionaje, el sabotaje, la subversión y el terrorismo, así como contra la pérdida o publicitación no autorizada. Incluye las medidas implementadas para protegerse contra la amenaza a la seguridad.

Puede originarse desde fuentes internas o externas. Los organismos de seguridad deben prestar atención en particular a las amenazas internas.

Las amenazas se categorizan en:

- Terrorismo. Es el uso ilegal, o la amenaza del uso, de la fuerza o la violencia contra individuos o propiedades en un intento de coaccionar o intimidar a gobiernos o sociedades para lograr objetivos políticos, étnicos, religiosos o ideológicos.
- Espionaje. Actividad de inteligencia dirigida hacia la adquisición de información por medio de métodos clandestinos y proscritos por la ley del país contra el que se comete el espionaje.
- Sabotaje. Cualquier acto incumplido de una operación militar, o cualquier omisión, que intente causar daño físico con el fin de ayudar a un adversario o alcanzar un objetivo político de subversión.
- Subversión. Acciones diseñadas para debilitar la fortaleza militar, económica o política de una nación minando la moral, lealtad o fiabilidad de sus ciudadanos. Los métodos de subversión pueden incluir:
    - Propaganda y agitación, manifestaciones y disturbios, distribución de panfletos.
    - Uso de organizaciones encubiertas para encubrir actividades reales.
    - Reclutamiento de adeptos que operen consciente o inconscientemente en nombre de sus reclutadores.
    - La creación de un clima de desconfianza y desilusión, que se dirige para desacreditar al gobierno o individuos.
    - La diseminación de falsos rumores o distorsión de la verdad (desinformación) con el fin de destruir la confianza en los líderes o aliados.
- Crimen Organizado. Cualquier empresa, o grupo de personas, inmersas en actividades ilegales continuas que tienen el propósito principal de generar beneficios, sin respeto a las fronteras nacionales.
- Ataques a las redes de ordenadores. Acciones llevadas a cabo utilizando las redes de ordenadores para irrumpir, negar, degradar o destruir la información residente en las redes de computadores y computadores, o las propias redes y computadores

21. NEUTRALIZACIÓN DE LA AMENAZA A LA SEGURIDAD.

Responsabilidad de neutralizar la amenaza. La Contra Inteligencia (CI) de la Alianza es responsable de neutralizar la amenaza a la seguridad que representan servicios de inteligencia hostiles y grupos o individuos terroristas, criminales o subversivos. La seguridad a todos los niveles será dirigida por el mando.

Dentro de la OTAN, los organismos de seguridad están establecidos a todos los niveles del mando. Las naciones anfitrionas son las principales responsables de la protección externa de las instalaciones de la OTAN localizadas en su territorio. Los planes nacionales, por tanto, deben desarrollarse entre los organismos nacionales y los mandos OTAN y mantenerse un estrecho enlace entre los mismos.

Responsabilidades del organismo de seguridad.

- Asesorar al mando sobre todas las amenazas a la seguridad.
- Gestionar y apoyar a las operaciones para neutralizar las amenazas a la seguridad.
- Obtener, elaborar y difundir información relativa a las necesidades de CI y producir y difundir valoraciones de la amenaza actual.
- Contribuir al proceso de seguridad operacional, incluyendo el planeamiento, coordinación y aplicación de medidas de seguridad de protección en toda la formación.
- Establecer y mantener contacto con las fuerzas de seguridad civiles y las autoridades de Contra Inteligencia.

Necesidad de saber. El principio fundamental de seguridad es que el conocimiento o la posesión de la información clasificada deben estar estrictamente limitada a aquellos, con la autorización de seguridad con el nivel apropiado, que tienen claramente la necesidad de saber con el fin de llevar a cabo sus cometidos. Ninguna persona está autorizada en virtud de su rango o posición para tener acceso a información clasificada. El refuerzo del principio de necesidad de saber limita el daño que puede ser hecho por una amenaza interior, mientras que fallar en este principio dañar a la seguridad gravemente.

Principios que gobiernan las operaciones de seguridad.

- Los mandos a todos los niveles son responsables de la seguridad.
- Las operaciones de seguridad deben coordinarse con el organismo de inteligencia, y consultarse con los de operaciones y otros, y deben integrarse con el esfuerzo general de inteligencia.
- Ellas deben ser un enfoque individual a cada nivel de mando para la política de seguridad.
- Los equipos de seguridad deben establecerse para enfrentarse a las amenazas y dar asesoramiento de seguridad a los mandos a cada nivel de mando.
- La amenaza a la información debe producirse por el personal de inteligencia y seguridad como avisos, valoraciones de la amenaza y establecimientos del nivel de amenaza. Estos deben de ser entregados con el grado de clasificación de seguridad más bajo y difundirse tan ampliamente como sea posible.
- La obtención de la seguridad relativa a la información debe coordinarse a cada nivel de mando e integrarse en el esfuerzo general de inteligencia.
- La responsabilidad para el establecimiento y mantenimiento de las bases de datos de inteligencia de seguridad debe estar definida claramente y, siempre que sea posible, integrarse con el esfuerzo general de inteligencia.

Formación en seguridad. El mantenimiento de altos estándares de formación en seguridad es de una importancia particular en todas las naciones de la OTAN para neutralizar el terrorismo, espionaje, sabotaje, subversión, crimen organizado y ataques contra redes de ordenadores.

22. SEGURIDAD DE PROTECCIÓN.

La seguridad de protección se define como el sistema organizado de medidas defensivas instituidos y mantenidos a todos los niveles de mando con el fin de lograr y mantener seguridad. Hay cuatro categorías de medidas de seguridad de protección:

- Seguridad del Personal. Aquellas medidas tomadas para excluir o restringir el acceso para proteger información o material de personas cuya lealtad, fiabilidad o confianza en ellas puede ser dudosa.
- Seguridad Física. La parte de la seguridad relativa a las medidas físicas de seguridad diseñadas para salvaguardar al personal, prevenir el acceso no autorizado a los equipos, instalaciones, material y documentos y salvaguardarlos contra el espionaje, sabotaje, daño y robo.
- Seguridad en las operaciones. Proceso que da a una operación u ejercicio militar la seguridad apropiada utilizando medios activos o pasivos para negar a un enemigo el conocimiento de las disposiciones, capacidades o intenciones de las fuerzas propias.
- Seguridad de la información (INFOSEC). Se define como las medidas necesarias para preservar la confidencialidad, integridad y disponibilidad de la información en documentos, grabaciones o formatos digitales.

Los objetivos de la seguridad de protección son:

- Revelar cualquier intento de penetrar a los controles por personal no autorizado.
- Prevenir a los servicios de inteligencia hostiles o a las organizaciones, grupos o individuos, subversivas, terroristas o criminales, la adquisición de información, causando disrupción o subvirtiendo al personal civil o militar.
- Proporcionar un mínimo de estándares comunes de seguridad que puedan aplicarse en todas las formaciones o unidades.
- Prevenir la posibilidad del acceso no autorizado a información digital y la destrucción o alteración de información en los sistemas de comunicación o información o en ordenadores personales.
- Asistir en la investigación especializada de fugas de seguridad.

Ninguna medida de seguridad será efectiva por sí sola, por lo tanto, la seguridad e protección debe consistir en un número de medidas interrelacionadas y que se apoyen mutuamente y que juntas consigan un grado de seguridad aceptable.

La aplicación de medidas de seguridad de protección es principalmente una responsabilidad nacional.

Desarrollo de una valoración de la amenaza. Una valoración de la amenaza es vital para neutralizarla y debe preparase exhaustivamente…

- Estudiando las fortalezas, capacidades, métodos e intenciones probables de todas las organizaciones, grupos, individuos y medios respectivos como se han mencionado antes.
- Definiendo los posibles objetivos y los más probables de ser atacados.
- Considerando la amenaza a, y la vulnerabilidad de, objetivos críticos.

23. PROTECCIÓN A LA FUERZA.

Protección a la Fuerza son las medidas y medios para minimizar la vulnerabilidad del personal, instalaciones, material, operaciones y actividades, a las amenazas y daños con el fin de preservar la libertad de acción y la efectividad operacional y así contribuir al éxito de la misión.

24. CONTRA INTELIGENCIA.

La contrainteligencia son aquellas actividades relacionadas con la identificación y neutralización de la amenaza a la seguridad planteada por las organizaciones o servicios de inteligencia hostiles o por individuos relacionados con el espionaje, sabotaje, subversión o terrorismo.

La idea central del esfuerzo de inteligencia es proteger al personal, información, planes y recursos, en la nación y desplegados. Su fin es proporcionar conocimiento y entendimiento de la situación prevalente para mantener la información privilegiada en secreto, los equipos seguros y el personal a salvo. La contrainteligencia debe ser proactiva y preventiva en su enfoque.

La contrainteligencia es una función de inteligencia que proporciona a los mandos de todos los niveles de un detallado conocimiento de las amenazas, vulnerabilidades y riesgos para permitirles tomar decisiones bien razonadas sobre las medidas de seguridad.

El mando debe negar al adversario la oportunidad de llevar a cabo terrorismo, espionaje, subversión, sabotaje, crimen organizado o ataques a las redes contra las fuerzas propias. Para conseguirlo es necesario identificar las vulnerabilidades de las fuerzas propias a las operaciones de obtención de inteligencia de un adversario. Esta información se utiliza para informar a los planes de OPSEC, contra vigilancia y decepción, incluyendo la política de Seguridad de Protección.

25. RESPONSABILIDADES.

Responsabilidades nacionales. Cada nación debe designar una organización como único punto de contacto para asuntos de CI. Dentro de cada organización nacional, se nombrará un asesor de CI nacional (NCIA). Las naciones nombrarán representantes de CI nacional (NCIRs) pasa asesorara los NCIAs o para desplegarse en los diversos niveles de mando durante ejercicios u operaciones. La función de un NCIR es coordinar las actividades CI de la OTAN con sus autoridades nacionales y apoyar a los organismo de CI en estos cuarteles generales. Cuando se han establecido en un teatro Células Nacionales de Inteligencia (NICs), los elementos de organizaciones de CI nacional deben formar parte de la NIC con el fin de asegurar un intercambio rápido

de mensajes de alerta con la Célula adecuada de CI de la OTAN. Las autoridades nacionales son las últimas en retener el control de sus órganos de CI.

Autoridad de Coordinación de CI. Cuando las fuerzas de la OTAN se despliegan en una operación, la autoridad de coordinación de CI (CICA) designada supervisará todos los aspectos de CI y será el principal asesor del mando en asuntos de CI. El CICA es responsable de coordinar y evitar conflictos entre operaciones nacionales y OTAN e investigaciones en el área de operaciones conjuntas.

J2X. Normalmente, la CI se acoplará con seguridad y HUMINT bajo la dirección de un organismo J2X determinado. En las operaciones, la dirección, coordinación y supervisión de los elementos HUMINT y CI son responsabilidad de J2X dentro de la rama de inteligencia, J2x mantendrá el registro de fuentes y evitará conflictos entre las actividades de HUMINT y CI. Además, proporcionarán asesoramiento a los mandos en operaciones HUMINT y CI. La célula CI es responsable de la coordinación de las actividades CI, incluyendo la supervisión de las actividades operacionales y reuniones. El J2X es también responsable de asegurar que los acuerdos y métodos de compartir información están en su lugar con el fin de incrementar la valoración de la situación y la eficiencia de todo el esfuerzo ce CI y HUMINT.

HUMINT y CI. Las actividades HUMINT a manudo tienen lugar entre aquellas que están relacionadas con la CI y muchos de los métodos y capacidades son comunes.

26. CONTRAMEDIDAS.

Objetivos de CI. Una vez que la valoración de CI se ha completado y las implicaciones para la seguridad están identificadas, se pueden identificar los objetivos de CI. Estos son instalaciones, organizaciones, redes de información y personal de interés de CI o inteligencia que debe ser detenido, destruido, explotado o protegido.

Implicaciones de Seguridad. Los organismos de inteligencia y seguridad pueden deducir de la valoración de CI los efectos que las amenazas identificadas dentro de la valoración pueden tener en la actividad de las fuerzas propias. Las implicaciones se categorizan en:

- Amenazas que se resuelven mediante el cumplimiento de medidas efectivas de seguridad y OPSEC.
- Amenazas (que pueden tornarse en oportunidades) para ser explotadas mediante la satisfacción de necesidades de inteligencia y la conducción de operaciones de información.

Contramedidas. Estas son:

- Disuasión. Las medidas robustas constituirán una disuasión efectiva contra un atacante potencial.
- Negación. Las actividades aplicadas a evitar que un adversario acceda a información protegida y sensible.
- Detección. La exposición y neutralización de los esfuerzos del adversario para reunir información.
- Decepción. Actividades utilizadas principalmente para inducir a error o confundir al adversario sobre las capacidades e intenciones delas fuerzas propias.

GLOSARIO

ACINT	Inteligencia acústica
AII	Área de interés de inteligencia
AIR	Área de responsabilidad de inteligencia
AOO	Área de operaciones
BDA	Valoración de daños de combate
CCIR	Necesidades críticas de información del jefe.
CIDI	Centro de integración y difusión de inteligencia
COMINT	Inteligencia de telecomunicaciones
ELINT	Inteligencia electrónica
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
GEOINT	Inteligencia geoespacial
HPT	Objetivos de alto rendimiento
HUMINT	Inteligencia de fuentes humanas
HVT	Objetivos de alto valor
IMINT	Inteligencia de imágenes
ISR	Inteligencia, vigilancia y reconocimiento
IPOE	Análisis del entorno operativo
MASINT	Inteligencia de firmas
MEDINT	Inteligencia médica
NBQ	Nuclear, biológico y químico
ORBAT	Orden de batalla
OSINT	Inteligencia de fuentes abiertas
PLIINT	Plan inicial de inteligencia
PROB	Programa de obtención
SIGINT	Inteligencia de señales
TECHINT	Inteligencia técnica
UAS	Sistema aéreo no tripulado