UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Centro de e-Learning

Experto Universitario en Seguridad Internacional y Servicios de Inteligencia

Centro de e-Learning SCEU UTN - BA.
Medrano 951 2do piso (1179) // Tel. +54 11 4867 7589 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

MÓDULO 2:

La Inteligencia como Catalizador de la Seguridad

Unidad 5:

Marco de actuación y funciones de los servicios de inteligencia.

Presentación:

Las organizaciones políticas humanas, desde la antigüedad, han sufrido serios desafíos a su defensa y seguridad. Constantemente, las estrategias de guerra y las amenazas a la seguridad han cambiado y generado nuevos retos a las tribus, los imperios, las naciones y los Estados.

Para ello, tanto en el marco de la seguridad internacional, así como en el nacional, los Estados deben contar con mecanismos de inteligencia que les permita tanto anticiparse a las consecuencias, así como detectar las amenazas latentes que pongan en peligro una situación determinada.

En este contexto, los Servicios de Inteligencia son organismos de los Estados que tienen como misión obtener información, no alcanzable por otros organismos, y difundir inteligencia sobre diversas amenazas, a fin de hacer posible su prevención y facilitar la toma de decisiones por los Gobiernos.

Se han constituido a lo largo del pasado y presente siglo como una pieza fundamental tanto de la seguridad nacional como de la política exterior de numerosos estados, amén de convertirse en fuente inagotable de inspiración para el mundo del cine y la literatura.

Des esto se tratan los contenidos que estudiamos en la presente unidad.

Objetivos

Que los participantes logren:

- Conocer el marco de actuación y funciones de los servicios de inteligencia.
- Profundizar en los conceptos y tipos de inteligencia.
- Comprender el concepto, alcance y objetivos de la Contrainteligencia.

Bloques temáticos:

- Concepto y Tipos.
- Ciclos.
- Fuentes y Acciones.
- Contrainteligencia.

Consignas para el aprendizaje colaborativo

En esta Unidad los participantes se encontrarán con diferentes tipos de actividades que, en el marco de los fundamentos del MEC*, los referenciarán a tres comunidades de aprendizaje, que pondremos en funcionamiento en esta instancia de formación, a los efectos de aprovecharlas pedagógicamente:

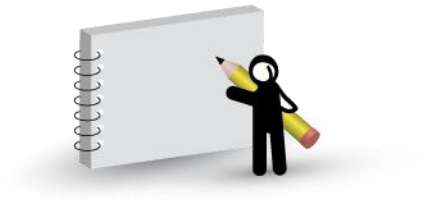
- Los foros proactivos asociados a cada una de las unidades.
- La Web 2.0.
- Los contextos de desempeño de los participantes.

Es importante que todos los participantes realicen algunas de las actividades sugeridas y compartan en los foros los resultados obtenidos.

Además, también se propondrán reflexiones, notas especiales y vinculaciones a bibliografía y sitios web.

El carácter constructivista y colaborativo del MEC nos exige que todas las actividades realizadas por los participantes sean compartidas en los foros.

**** El MEC es el modelo de E-learning colaborativo de nuestro Centro.***



Tomen nota:

Las actividades son opcionales y pueden realizarse en forma individual, pero siempre es deseable que se las realice en equipo, con la finalidad de estimular y favorecer el trabajo colaborativo y el aprendizaje entre pares. Tenga en cuenta que, si bien las actividades son opcionales, su realización es de vital importancia para el logro de los objetivos de aprendizaje de esta instancia de formación. Si su tiempo no le permite realizar todas las actividades, por lo menos realice alguna, es fundamental que lo haga. Si cada uno de los participantes realiza alguna, el foro, que es una instancia clave en este tipo de cursos, tendrá una actividad muy enriquecedora.

Asimismo, también tengan en cuenta cuando trabajen en la Web, que en ella hay de todo, cosas excelentes, muy buenas, buenas, regulares, malas y muy malas. Por eso, es necesario aplicar filtros críticos para que las investigaciones y búsquedas se encaminen a la excelencia. Si tienen dudas con alguno de los datos recolectados, no dejen de consultar al profesor-tutor. También aprovechen en el foro proactivo las opiniones de sus compañeros de curso y colegas.

Concepto y Tipos

Es muy difícil conceptualizar algo tan diversificado como la inteligencia, pero podemos decir que es todo aquello que tiene como objeto proporcionar a los gobiernos información útil, seguridad, y procedimientos no convencionales, para contribuir a que se adopte y ejecute la mejor decisión, previniendo y disminuyendo los riesgos.

A continuación, brindaremos algunas definiciones recopiladas de las leyes de algunos países:

Chile, Ley 19.974, sobre el Sistema de Inteligencia del Estado: Es el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones.

Argentina, Ley 25.520 de Inteligencia Nacional: Es la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, amenazas, riesgos y conflictos que afecten la seguridad exterior e interior de la Nación o Estado.

México, Ley de Seguridad Nacional: Se entiende por inteligencia el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información, para la toma de decisiones en materia de Seguridad Nacional. Procesar la información recolectada, determinar su tendencia, valor, significado e interpretación específica y formular las conclusiones que se deriven de las evaluaciones correspondientes, con el propósito de salvaguardar la seguridad del país.

Perú, **Ley 27.479 del Sistema de Inteligencia Nacional**: La Inteligencia como actividad es el conocimiento anticipado logrado a través del procesamiento de las informaciones. La difusión de la Inteligencia debe ser oportuna para contribuir a la toma de decisiones y así poder alcanzar objetivos de seguridad y bienestar.

La creación de la inteligencia para la seguridad y la defensa se debe regir por seis principios:

- ✓ **Primero:** las actividades de inteligencia derivan del estado de conflicto o de rivalidad en el que se encuentran las potencias, por lo que la intensidad de las operaciones de inteligencia desarrolladas por un país respecto de otro ha de

ser inversamente proporcional al grado de entendimiento y amistad que se profesen dichos países.

✓ **Segundo**: este principio fija el carácter secreto de la inteligencia, lo cual significa que en algún momento la información elaborada debe ser calificada como secreta y enviada por canales exclusivos. Lo importante de este principio es la afirmación implícita de que la información, sea abierta u obtenida por métodos clandestinos, no es en sí misma inteligencia, sino solamente su materia prima.

✓ **Tercero:** principio deriva del anterior e indica que la recogida clandestina de la información es la actividad fundamental de los servicios.

✓ **Cuarto:** Este principio es que la verdad es la base de una buena inteligencia: la certeza de los datos, la fiabilidad de su procedencia y la objetividad de los analistas, dejando al margen sus perjuicios, son condiciones imprescindibles para que el producto de inteligencia que se obtenga sea pertinente, válido y eficaz.

✓ **Quinto:** Este principio consiste en que la inteligencia es una actividad inútil y costosa si no tiene una aplicación que justifique la inversión realizada: la inteligencia debe servir para algo, lo cual depende de su relevancia.

✓ **Sexto:** principio afirma que las actividades encubiertas deben incluir el conocimiento proporcionado por grupos nativos, ya que sólo éstos pueden dar e interpretar un buen cúmulo de información sobre la región o el país en el que se opera.

Según su finalidad, se debe distinguir entre:

- La información estratégica para la seguridad y la defensa -es decir, para proteger la independencia, la integridad territorial y los intereses nacionales y;
- La estabilidad de las instituciones del Estado e Inteligencia Militar, orientada a la organización de la defensa para las fuerzas armadas, a la vigilancia del ejército de un enemigo potencial o real y a la preparación y desarrollo de operaciones bélicas.

La inteligencia no se construye mediante una suma de datos, sino a partir de un determinado modo de analizar los datos sobre hechos.

La generación de inteligencia no es un proceso lineal, sino un ciclo donde se combinan actividades sintéticas de discriminación, evaluación, y construcción de información a partir de la representación y análisis de datos obtenidos por múltiples medios, identificados como necesarios a partir del estudio de las necesidades y las demandas de información de los usuarios y la evaluación de los resultados de la aplicación de inteligencia elaborada en momentos anteriores.

Lo que distingue a la información de la inteligencia, es la pirámide informacional

Fuente: http://www.seguridadinternacional.es/?q=es/content/introducci%C3%B3n-la-inteligencia-en-el-%C3%A1mbito-de-seguridad-y-defensa

⇒ **Datos**. Representaciones básicas de la realidad que por sí solos no tienen significado (por ejemplo, cifras o nombres de personas). Lo adquieren gracias a la capacidad humana de establecer relaciones.

⇒ **Información**. Se genera mediante la recopilación de datos, añadiéndoles contexto, significado y propósito. Siguiendo con el ejemplo anterior: cifras, nombres de personas y detalles concretos de personas detenidas en algún país determinado.

⇒ **Conocimiento**. Es el resultado de una estructura de conceptos, teorías y explicaciones de la realidad que permiten comprenderla. Los conocimientos previos permiten evaluar e integrar nuevas informaciones. El conocimiento no sólo se encuentra en las personas, también está presente en las organizaciones, imbuido en sus procesos y estructuras. Cuando se combina con recursos

tangibles es capaz de generar ventaja competitiva respecto a otras organizaciones, y por eso tiene un especial valor. Puede ser tácito y explícito. El tácito está formado por el capital humano (miembros) y relacional (red externa de la organización). El explícito se plasma en soportes físicos. El conocimiento es de difícil captura, y se produce y difunde mediante la espiral del conocimiento.

⇒ **Inteligencia**. Es el resultado de la aplicación del conocimiento tácito y explícito para integrar, interpretar, analizar y evaluar información relevante sobre un determinado asunto que representa una amenaza o una oportunidad para una organización o un Estado. Con él se atiende a una demanda específica por parte del consumidor de inteligencia orientada a la toma de decisiones y a la acción. La inteligencia permite comprender el entorno con más profundidad y por ello sitúa en una posición ventajosa a la hora de interactuar con él.

En esta instancia, vale la pena distinguir entre:

Inteligencia como proceso: La inteligencia es un proceso que se inicia a partir de unas determinadas demandas por parte de los decisores políticos que ponen en marcha lo que se conoce como ciclo de inteligencia, concepto que trataremos de manera más detalla en el próximo documento. La inteligencia como proceso explica que en ocasiones se confunda inteligencia con espionaje, cuando en realidad este último es una actividad que forma parte del ciclo (en la fase de obtención), y que por tanto alude a un aspecto muy puntual en el conjunto del proceso.

Inteligencia como resultado: La inteligencia también se puede entender como el producto resultante de la fase de análisis del ciclo de inteligencia. Puede ser de diversos tipos y difundirse a través de presentaciones orales o por escrito, en diversos formatos en función del tipo de inteligencia. Cuestión ésta última que abordaremos en el próximo documento sobre el ciclo de inteligencia. La inteligencia como resultado es el objeto habitual de las definiciones de inteligencia. El Glosario de Inteligencia la define como el producto que resulta de la evaluación, la integración, el análisis y la interpretación de la información reunida por un servicio de inteligencia. Pero además de esta acepción, se pueden entender como resultados de la inteligencia las operaciones que de ella se derivan, entre ellas las acciones encubiertas (Lowenthal, 2012).

Ciclos

De acuerdo a lo que hemos estado estudiando en el punto anterior, es fundamental poder distinguir cuándo y mediante qué medio la información se convierte en inteligencia.

La respuesta se halla en el denominado “ciclo de la inteligencia”, por el que el quehacer diario de un servicio de inteligencia consiste en elaborar la información obtenida por diversos medios, a lo largo de varias fases, divididas a su vez en varias subfases, hasta conseguir inteligencia.

Se entiende por Ciclo de Inteligencia la secuencia mediante la cual se obtiene información, se transforma en inteligencia y se pone a disposición de los usuarios.

El Ciclo de Inteligencia consta de las siguientes fases o etapas:

Fuente: https://www.gob.mx/cms/uploads/attachment/file/233665/ciclo-inteligencia.pdf

- **Planeación:** Durante la fase se determinan las necesidades de inteligencia, se prepara un plan para su obtención, se organizan los medios y se efectúa el mando, coordinación y control de todos ellos. Aquí cobran especial relevancia las denominadas funciones directivas, que son las siguientes: planificación, organización, motivación, mando, coordinación y control, manteniéndose las cuatro últimas durante el desarrollo de todo el ciclo.

- **Recolección** Durante esta etapa se ponen en marcha las actividades de recolección de información a partir de diversas fuentes con base en las solicitudes formuladas durante la fase de planeación.

- **Procesamiento Y Análisis** La información obtenida en la etapa de recolección se depura, estandariza y, en su caso, se decodifica con el objeto de presentarla en un formato útil para las labores de análisis, cuyo propósito consiste en transformar la información en bruto en productos de inteligencia estratégica, táctica u operativa destinados a satisfacer necesidades de información específica. Desde un enfoque multidisciplinario, el proceso de análisis recurre al uso de una gran variedad de disciplinas y metodologías especializadas que van desde la sociología, antropología, psicología, demografía, lingüística, economía, derecho, ciencias políticas y relaciones internacionales, geología, estadística, matemáticas, informática, biología, física, química, entre otras. Un aspecto de especial importancia en la elaboración de los productos de inteligencia consiste en la claridad con la que se exponen los aspectos más relevantes de la información, así como detectar sus alcances y limitaciones.

- **Difusión Y Explotación** El carácter confidencial de la información de inteligencia, así como la importancia de remitirla oportunamente a las personas indicadas, hacen que esta etapa sea de especial relevancia. Con el fin de garantizar la seguridad de la información y evitar que caiga en manos equivocadas, los productos de inteligencia son objeto de una serie de procesos y medidas de seguridad con el propósito de evitar riesgos durante su traslado y entrega. Asimismo, durante esta etapa, se pone especial atención en hacer llegar la información con oportunidad a las personas indicadas antes de que sea demasiado tarde para los procesos de toma de decisiones.

- **Retroalimentación** Un aspecto de gran relevancia para el ciclo de inteligencia consiste en determinar el grado en que la información de inteligencia proporcionada atendió las necesidades de los procesos de toma de decisiones, o, en su caso, si las personas a las que se les entregó la información requieren precisar o ampliar la información sobre un tema en especial. Lo que, en consecuencia, da inicio a las actividades de planeación y a comenzar nuevamente en la primera fase del ciclo de inteligencia.

Fuentes y Acciones

De algún sitio hay que obtener la información, al margen de las denominaciones técnicas y subcategorías las fuentes de inteligencia son cuatro: HUMINT (fuentes humanas), IMINT (Imagenes), SIGINT (señales y comunicaciones) y OSINT (análisis de recursos abiertos), en definitiva, todo tipo de medio que permita la recogida de información: desde los lectores de labios, hasta satélites de espionaje. Recientemente, en respuesta a los conflictos asimétricos se ha agregado la Inteligencia Cultural.

❖ **Inteligencia Humana, Human Intelligence (HUMINT):** Es la recolección de información por personal especialmente entrenado, usando una variedad de tácticas y métodos tanto activos como pasivos, cuyo objeto son otras personas de las cuales se puede extraer información o colaboración para obtenerla.
La Inteligencia de fuente humana, es la más antigua y tradicional. Se refiere a los espías, infiltrados, agentes secretos, informadores, entrevistas, interrogatorios. Si bien con el fin de la guerra fría este tipo de inteligencia quedo desplazada, tras los atentados del 11S han vuelto a adquirir importancia y relevancia. Encontramos los siguientes tipos:

- Oficial de Enlace: Es un miembro del servicio secreto acreditado en una embajada. Su misión es relacionarse y recibir o aportar información, con sus homólogos de ese país. En ocasiones puede ejercer de Jefe de inteligencia de las actividades de esas embajadas en ese país.

- Agente Operativo: Es el sujeto encargado de hacer seguimientos, introducciones en edificios para colocar escuchas, acciones operativas, dependiendo de los escrúpulos del servicio puede encargarse de asesinatos selectivos.

- Infiltrado o Topo: Es el agente que se introduce en organizaciones terroristas, criminales o en otros servicios de inteligencia, empresas con el objetivo de obtener información, desestabilizar, o llegar a otro tipo de acciones asesinatos, sabotajes.
- Agente de Campo: Es el espía que se introduce en un país o determinada zona con el objeto de recoger información, de determinados objetivos o crear una red propia de colaboradores e informadores.

- Informador o colaborador: No es un miembro del servicio de inteligencia pero desde su posición, o puesto de responsabilidad dentro de una organización, transmite información.

También se suelen conocer por “blancos” (los agentes en el exterior), y “negros” los agentes infiltrados en organizaciones.

❖ **Inteligencia de Imágenes (**IMINT: Imagery Intelligence): Constituye una categoría de inteligencia derivada de la información obtenida y proporcionada por imágenes obtenidas a través de satélites o medios aéreos:

- Inteligencia de Imágenes (Optin Optical Intelligence) en la región visible del espectro.

- Espionaje fotográfico (PHOTINT: Photoraphic Intelligence) desde la típica cámara hasta los satélites.

- Electro-óptico (EOPINT: Electro-Optical Intelligence): Los fenómenos electro ópticos serán aquellos en los que las propiedades ópticas de un medio son modificables por la presencia de un campo eléctrico, láser (Se han utilizado láseres en la longitud de onda azul-verde, capaz de traspasar el agua, para las comunicaciones entre satélites y submarinos), cables de fibra óptica, televisiones.

- Infrarrojos (IRIN: Infra Red Intelligence): Las emulsiones fotográficas pueden hacerse sensibles a los rayos infrarrojos de la parte invisible del espectro con tintes especiales. La luz infrarroja atraviesa la neblina atmosférica y permite realizar fotografías claras desde largas distancias o grandes altitudes (satélites). Debido a que todos los objetos reflejan la luz infrarroja, pueden ser fotografiados en total oscuridad. Las técnicas de fotografía infrarroja se emplean siempre que tengan que detectarse pequeñas diferencias de temperatura, capacidad de absorción o reflexión de la luz infrarroja. La película infrarroja tiene muchas aplicaciones militares y técnicas, como por ejemplo la detección de camuflajes.

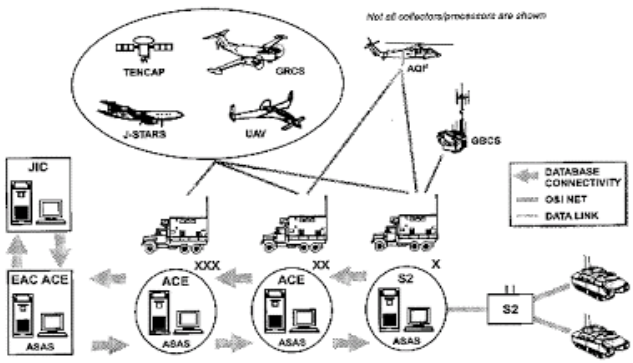


Figure 2–4. Intelligence flow

Fuente: http://desarrolloydefensa.blogspot.com/2008/09/cules-son-las-fuentes-de-inteligencia.html

❖ **Inteligencia de Señales (SIGINT: Signals Intelligence):** con redes como ECHELON, engloba una serie de recursos:

- Comunicaciones Inteligentes (COMINT: Communications Intelligence) Se trata de las comunicaciones que todos conocemos; es decir: teléfono móvil y fijo, radio, transmisores, internet.

- Campos eléctricos y magnéticos: (ELINT: Electromagnetic Intelligence) Se trata de las cargas y corrientes eléctricas. El radar o radio de detección y medición de distancia, es un sistema electrónico mediante el cual se puede detectar la presencia de objetos o superficies, y también su posición exacta y movimiento a distancia, gracias a la propiedad que tienen de reflejar en su totalidad o en parte las ondas electromagnéticas.

- Detección por telemetría (TELINT: Telemetry Intelligence) Se trata del medio a través del cual se obtienen imágenes, medidas, radiaciones tanto en el espacio como en la superficie con imágenes ópticas, en los espectros visible e infrarrojo normalmente. En ocasiones cuentan con detectores radar.

❖ **La Inteligencia de Reconocimiento y Signatura** (MASINT: Measurement and Signature Intelligence) ocupa aquel espacio de la inteligencia no atribuido a la Inteligencia de Imágenes (IMINT), de Señales (SIGINT), la Humana (HUMINT), y la de Fuentes Abiertas (OSINT), y agrupa varios subtipos:

- Inteligencia Acústica (ACINT o ACOUSTINT), de Radar (RADINT), de Infrarrojos (IRINT), la Láser (LASINT), Nuclear (NUCLINT), Óptica (OPINT), y la de radiación no intencionada (URINT), también incluye las siguientes:

- Inteligencia de Radar (RADINT): La RADINT o Inteligencia de Radar es aquella información obtenida a través de los datos recolectados por radares.

- Inteligencia Acústica (ACOUSTINT): En principio la inteligencia acústica se refiere a aquella obtenida mediante el "Sonar". Hay dos grandes tipos de sonar: ***Sonar Activo**: es el que emplea para detectar objetos bajo el agua. El eco que devuelve dicho objeto al incidir sobre él las ondas acústicas emitidas por un transmisor: es similar al radar. Empleando el Sonar Activo se emite un tren de ondas acústicas con una determinada potencia al agua. Un objeto sumergido sobre el que incidan estas ondas, reflejará parte de ellas que volverán hacia el foco emisor. ***El Sonar Pasivo:** se limita a escuchar el sonido que proviene de los objetos que se encuentran sumergidos. Estos dispositivos reciben directamente el ruido producido por el objeto y el camino que recorre la onda es la distancia existente entre el objeto y el receptor del ruido. Esto permite el análisis del ruido radiado por los barcos, obteniendo así la denominada "firma acústica" que permite identificar cada unidad de forma unívoca al igual que una huella dactilar identifica a una persona; pero a diferencia de las huellas dactilares que son invariables, las firmas acústicas cambian con el tiempo. Esto obliga a mantener una información actualizada de inteligencia de unidades navales. Existen varios tipos de equipos para obtenerla: -SOSUS (Sound Surveillance System): consiste en gigantescas "orejas" sonar pasivas sumergidas en el fondo del mar; -TACTAS (Tactical Towed Array Sonar): es un sonar pasivo remolcado, consiste en un tubo muy fino, de flotabilidad neutra, de 1,8 km o más, lleno de hidrófonos (sonares pasivos); -SURTASS (Surveillande Towed Array Sensos System), son una variante del SOSUS aplicada utilizando los TACTASS. Consiste en un pequeño catamarán de unos 50 metros y motores eléctricos, que está dotado de un modelo muy refinado del TACTASS, del sonar remolcado, Disponen de comunicaciones vía satélite y comunican a una base en la costa la información que recogen.
- Inteligencia Nuclear (NUCINT): Esta derivada de la información aportada de la recolección y análisis de radiaciones y otros recursos radioactivos.

- Inteligencia de Infrarrojos (IRINT): Las emulsiones fotográficas pueden hacerse sensibles a los rayos infrarrojos de la parte invisible del espectro con tintes especiales. La luz infrarroja atraviesa la neblina atmosférica y permite realizar fotografías claras desde largas distancias o grandes altitudes (satélites). Debido a que todos los objetos reflejan la luz infrarroja, pueden ser fotografiados en total oscuridad. Las técnicas de fotografía infrarroja se emplean siempre que tengan que detectarse pequeñas diferencias de temperatura, capacidad de absorción o reflexión de la luz infrarroja. La película infrarroja tiene muchas aplicaciones militares y técnicas, como por ejemplo la detección de camuflajes
- Inteligencia Laser (LASINT): Usando la tecnología láser, se busca obtener monitorizaciones de audio, es decir aplicando el Laser sobre un entorno cerrado, se podría obtener información, de las vibraciones producidas por el sonido. Se le considera una categoría dentro de la inteligencia electro-óptica.

- Inteligencia de Radiaciones Involuntarias (URINT): Se dedica a la monitorización del espectro electromagnético, requiere equipos muy costosos y complejos, por ejemplo puede capturar datos de la pantalla de un ordenador que emite este tipo de radiaciones, esto exige equipos muy complejos y costosos, equipos se han de proteger para que no las emitan: es la denominada protección frente a TEMPEST.

Hay otra clasificación de las fuentes que las agrupa en fuentes abiertas y fuentes cerradas.

- **Las fuentes abiertas** (OSINT: Open Source Intelligence) se refieren a la recolección de información de una persona o empresa utilizando fuentes de acceso público como internet, redes sociales, buscadores, foros, fotografías, wikis, bibliotecas online, conferencias, metadatos entre otros. Son una eficaz herramienta para recopilar todo tipo de información, la cual puede ser utilizada para tareas como realización de perfiles de seguridad, estudios psicológicos, evaluar tendencias de mercado, auditorias en temas de seguridad de la información o conocer sobre la identidad digital y reputación online de personas, entre otras.

Su uso se estructura a partir de la recolección y procesamiento de información. Entre más información se encuentra, mayores conclusiones se pueden establecer en diferentes procesos. Un ejemplo de inteligencia con fuentes abiertas es la técnica utilizada denominada Google Hacking, la cual permite encontrar información en Google mediante la utilización de filtros. Tal es

la importancia que han adquirido los profesionales en OSINT que las empresas en la actualidad están vinculando a sus procesos a profesionales que sepan buscar información y que tengan conocimiento estadístico y predictivo del análisis de altos volúmenes de información.

- **Las fuentes cerradas**: son las conocidas como secretas o para cuya obtención se requieren procedimientos de carácter especial.

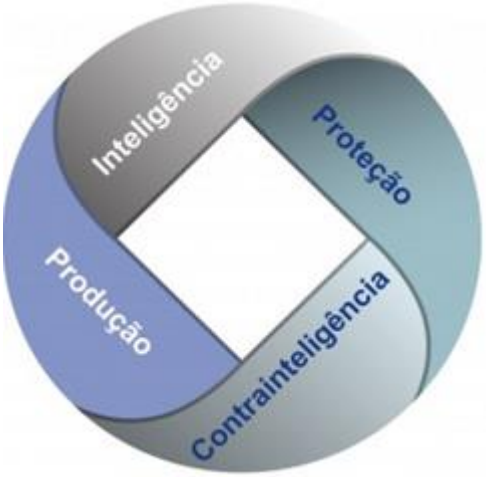
Fuente: https://www.coettc.info/2018/06/22/iii-congres-internacional-de-seguretat-i-telecomunicacions/

Contrainteligencia

La contrainteligencia es el conjunto de acciones orientadas a prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población.

Esta forma parte de una de las funciones de la Inteligencia y tiene como finalidad proteger informaciones importantes y sensibles para el Estado y neutralizar acciones de Inteligencia realizadas en beneficio de instituciones, empresas, grupos o gobiernos extranjeros.

Su actuación se extiende a la protección de los conocimientos que la propia área de Inteligencia produce, así como otros conocimientos e informaciones considerados sensibles a la seguridad del Estado.



Fuente: http://www.abin.gov.br/es/atividadeinteligencia/inteligenciaecontrainteligencia/contrainteligencia/

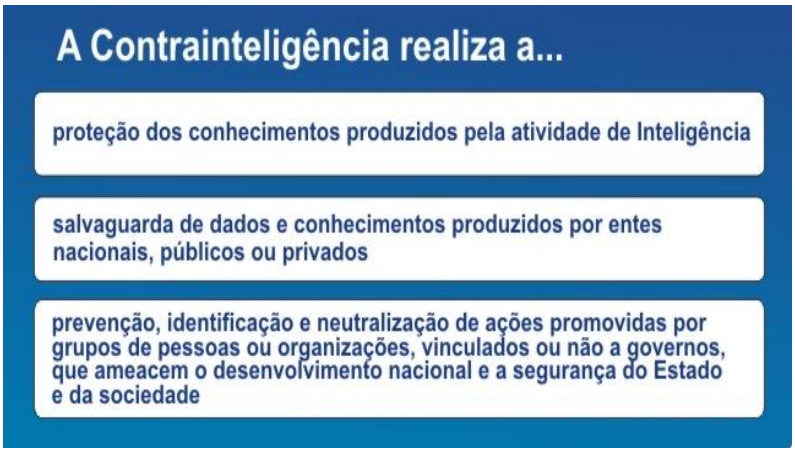
La Contrainteligencia también utiliza metodología específica, así como en el área de producción de conocimientos de Inteligencia, con foco en la detección e identificación de las amenazas existentes a las informaciones del Estado. Puede emplear acciones de obstrucción y neutralización con el propósito de frustrar los esfuerzos de agentes adversos y evitar la filtración de informaciones sensibles y sigilosas.

Las atribuciones de la Contrainteligencia, en general, se dividen en dos áreas de actuación: la protección de conocimientos y el contraespionaje.

✓ **El área de protección del conocimiento**: actúa para prevenir la filtración de informaciones sensibles. Ese segmento opera en órganos e instituciones nacionales de investigación, con la promoción de la cultura de protección de las informaciones y con el fomento de la adopción de medidas preventivas. El área desarrolla evaluaciones de riesgos que analizan el nivel de exposición de las informaciones y de los sistemas, de instituciones nacionales, de protección a las acciones de la Inteligencia adversa.

✓ **El área de contraespionaje** busca identificar acciones de espionaje o sabotaje en curso contra conocimientos, informaciones o tecnologías sensibles del Estado. En los casos en los que haya confirmación de las sospechas, el contraespionaje desarrolla acciones para mitigar los efectos, obstruir las acciones y neutralizar la capacidad de actuación futura de los agentes adversos.

✓



Fuente:
http://www.abin.gov.br/es/atividadeinteligencia/inteligenciaecontrainteligencia/contrainteligencia/

En definitiva, la contrainteligencia es un conjunto de actividades que son establecidas de manera colectiva por una contraparte con el propósito de entorpecer e interceptar las diversas fuentes de información inteligentes del enemigo por medio de códigos, censura, tretas, trampas o mentiras, con el fin de generar confusión.

Se trata de un conjunto de actividades destinadas a anular la eficacia de las acciones de inteligencia enemigas y a proteger la información contra el espionaje, los disturbios, la infraestructura, el sondeo o algún tipo de sabotaje. Sus desarrolladores son conscientes de que los sistemas de seguridad deben ser cada vez más fuertes e implacables y que dependen de un planeamiento que tiene que ser muy efectivo.

A lo largo de la historia de la humanidad siempre ha existido esta arriesgada forma de contrapeso. Las primeras unidades de contrainteligencia y espionaje organizadas se remontan al siglo I en la antigua Roma: los frumentarii, quienes eran básicamente soldados legionarios que ejecutaban funciones articuladoras y sistematizadoras para proteger el dominio imperial. Sus tareas se encauzaron hacia el espionaje político, hasta convertirse gradualmente en la policía secreta del imperio.

La contrainteligencia eficiente es sorpresiva. Usada enormemente en las actividades políticas, militares y electorales, es un juego estratégico que utiliza medidas defensivas y ofensivas que actúan para preocupar, desmentir y entorpecer las acciones del otro. El descontrol y la desinformación son factores que pueden cambiar el escenario de cualquier proceso. Mientras la inteligencia consiste en recopilar, organizar, proteger y transferir información, la contrainteligencia intenta privar al adversario de conocer las competencias y debilidades para no otorgar ningún tipo de ventaja.

Los movimientos de contrainteligencia son de ejecución y no excluye una planificación, proyección o programación previa de cada una de las acciones a emprender, no obstante, su tiempo de respuesta debe ser urgente y realizado de manera permanente, para imposibilitar, o al menos supeditar, que el adversario obtenga información sobre planes, operaciones y acciones, aplicando medidas de rechazo, desaprobación y, sobre todo, de seguridad.

Como ocupación tiene perspectivas que le otorgan una conducta detectivesca y un proceder policial, debido a los métodos utilizados para detectar, impedir, delatar y atrapar a los transgresores de la seguridad e inteligencia. El ciberespionaje nace como una práctica inmediata que ayuda a formar imágenes de los sistemas de defensa y logísticos, así como las capacidades militares y electorales relacionadas que pueden explotarse en una crisis.

Tiene que ser coordinada al más alto nivel y con gran responsabilidad pues depende, en gran parte, de diversos y numerosos órganos y procedimientos de averiguación, búsqueda e indagación. Se trata de un orden organizacional muy relevante y extenso, que depende de una maquinaria tecnológica, militar y electoral, que tiene que estar muy bien constituida para no ser descubierta y subyugada.

Es una actividad basada en el control, la vigilancia y la alerta constante en donde el desarrollo de la ciencia, la tecnología y la técnica obliga a una paulatina especialización de sus prácticas.

Así, la seguridad siempre será esencial para preservar el poder, porque el principio conductivo de la contrainteligencia influye en el planeamiento, coordinación y ejecución de las operaciones políticas, económicas, militares y las que están enlazadas con el juego electoral.

Su impulso destructivo aplicado a las operaciones modernas que otorgan poder exige sagacidad, para promover la ejecución de sus acciones, así como pericia para crear medidas propensas para contrarrestarlas, neutralizarlas y evitarlas.

Bibliografía utilizada y sugerida

Alonso Blanco Jesús. Contener las Redes de Amenaza. Instituto Español de Asuntos Estratégicos. Madrid 2015.

Avilés, J. ”Las amenazas globales del siglo XXI”. Arbor, Tomo CLXXX, núm. 709, pp. 247-268. Madrid. 2005.

Bataglio Jorge. Transformaciones en la seguridad internacional en la post Guerra Fría: su impacto en América del Sur. Estudios Internacionales 160, Universidad de Chile. 2008.

Brown, Chris “Understanding International Relations”: Palgrave Macmillan. Nueva York. 2005.

Bull, Hedley “Intervention in world politics” Clarendon Press. Oxford. 1984.
Calduch Cercera Rafael, Incertidumbres y Riesgos. E. G. Estrategia Global N° 5. Madrid 2004.

Cancelado Henry. La seguridad internacional frente a las amenazas globales contemporáneas. Análisis político nº 68, Bogotá, enero-abril, 2010.

Clarck, Robert. “Intelligence Analysis: A Target-Centric Approach” Washington, DC: CQ Press. 2012.

Colom Guillem “Rusia y las operaciones de información”. Publicado en GESI. España. 2017. Disponible en: http://www.seguridadinternacional.es

De La Lama Jorge. El nuevo concepto de Seguridad Hemisférica Cooperativa. FLACSO. Chile.1998 .

Davis, Michael y Wolfgang Dietrich (eds.). “International intervention in the post-cold war world: Moral responsibility and power politics” ME Sharpe. Nueva York:. 2004

Drogin, Bob Curveball “Spies, Lies, and the Con Man Who Caused a War” New York: Random House. 2007.

Esteban, Miguel Ángel y Carvalho, Andrea V. “La inteligencia y los activos informacionales”. Inteligencia. Valencia. 2012.

Feal Vázquez Javier. Amenazas transnacionales. Boletín de Información del CESEDEN núm. 295, Madrid. 2006.

Feal Vázquez Javier: “Globalización o mundialización. Tanto monta-monta tanto”. Boletín de Información del CESEDEN, núm. 274, pp. 95-110. Madrid 2002.

Fontana, Andrés. Nuevas amenazas: implicancias para la Seguridad Internacional y el empleo de las Fuerzas Armadas. Universidad de Belgrano. Buenos Aires 2003..

Franco Samantha. El estado de derecho internacional frente a las nuevas amenazas a la seguridad internacional. México. 2012.

Gaytán Jorge Antonio Ortega. Las Amenazas Asimétricas. ¿Desafíos De Seguridad Y Defensa En El Hemisferio Occidental?. Guatemala. 2011.

Gel-Rial. Discordia en la Política Económica Mundial. Buenos Aires. 1988.

Gentry, John A. “Has the ODNI Improved U.S. Intelligence Analysis?”, International Journal of Intelligence and CounterIntelligence, Vol. 28, Issue 4, pp. 637-661. Washington. 2015.

Herrero, J.L.: “Memorandum sobre la cumbre de la ONU (16-17 sep 2005). Revista Foreign Policy, pp. 51-55, Madrid.Septiembre 2005.

Hoffman Stanley. Jano y Minerva: Ensayos sobre la guerra y la paz. Grupo Editor Latinoamericano. Buenos Aires 1987.

Holzgrefe J.L. y Keohane Robert. Humanitarian intervention: Ethical, legal, and political dilemmas.: Cambridge University Press. Cambridge y Nueva York 2003.

Hulnick, Arthur S. “What's wrong with the Intelligence Cycle”, Intelligence and National Security, Volume 21, Issue 6, pp. 959-979. Washington. 2006.

Jackson, Robert “Sovereignty”. Polity Press. Cambridge. 2007
Keating, Thomas F. y Andy Knight. Building sustainable peace. University Press. United Nations.Tokio. 2005

Losada Maestre, Roberto “Análisis de riesgos y seguridad colectiva”, Sauca Cano, José María (Ed.), Aviones usados como bombas. Problemas políticos y constitucionales en la lucha contra el terrorismo, Madrid: Los Libros de la Catarata. 2015.

Lowenthal, Mark M. “Intelligence: From Secrets to Policy” Washington, DC: CQ Press. 2012.

Morgenthau Hans. Política entre las Naciones. La lucha por el poder y la paz. Editorial Sudamericana. Buenos Aires. 1960..

Morillas Bassedas, Pol. La seguridad internacional después de la guerra fría ¿Avanzando hacia una doctrina de seguridad humana? Fundación CIDOB. España .2006.

Novak Talavera Fabián “La teoría de los actos unilaterales de los estados”. Revista Agenda Internacional. Perú. 1994.

Rojas Diana Marcela “La intervención internacional: los desafíos de la conceptualización” en la tesis doctoral “Las transformaciones de la intervención

en la era de la globalización: el caso de Estados Unidos en Colombia: 1961-2010". Colombia Internacional 76, julio a diciembre de 2012.

Sánchez Gómez-Merelo Manuel "Un nuevo Código de Seguridad Global". Blog sobre convergencia y tecnología de Tendencias21. Disponible en: https://www.tendencias21.net/seguridad/Un-nuevo-Codigo-de-Seguridad-Global_a30.html

Thomas, Ann y Aron Thomas, Jr. "Non-intervention: The law and its import in the Americas" Southern Methodist University Press. Dallas, Texas1956.

Lo que vimos:

En esta unidad hemos estudiado el marco de actuación y las funciones de los servicios de inteligencia; los conceptos, tipos, ciclos, fuentes, acciones y la contrainteligencia.

Lo que viene:

En la próxima unidad estudiaremos la llamada comunidad de “La Inteligencia”, sus actuaciones en el manejo de fuentes, operaciones psicológicas y recopilación de datos.

¡Los esperamos…!