Los medios de producción de inteligencia, en el análisis actual de los conflictos[1]

CLAUDIO PAYÁ SANTOS[2]

JUAN JOSÉ DELGADO MORAN[3]

JUAN CARLOS FERNÁNDEZ RODRÍGUEZ[4]

Resumen

La inteligencia y el método de obtención de esta, suponen un valor fundamental en las agendas de los Estados para determinar mejores y más eficientes formas del desarrollo, aportando con sus hallazgos, justificación a las políticas militares de defensa y de seguridad interior o exterior de los Estados pero que actualmente, debido a los adelantos tecnológicos, los sistemas de inteligencia, están evolucionando para adaptarse a los escenarios cambiantes, dando lugar a una mayor complejidad en la producción de inteligencia que ya no obedece a un escenario convencional. La noción de guerra digital y la ingeniería armamentista basada en la computación, las potencialidades de Internet y las fuentes abiertas de información en línea, son el desafío actual de los modelos globalizados de la fuerza y la acción bélica del presente siglo, convirtiéndose el avance de la tecnología en una suerte de actor en el escenario internacional en el marco de la era de la información que precisa de una inteligencia apropiada y capaz.

Recibido:
22 de agosto de 2015

Aprobado:
30 de noviembre de 2015

The means of production of intelligence in the current analysis of conflicts

Abstract

The intelligence and the method of obtaining this, represent a fundamental value in the agendas of states to find better and more efficient ways of development, contributing with their findings, justification for military

Palabras claves:
Ciclo de Inteligencia, Big Data, OSINT, fuentes abiertas, SOCMINT

Keywords:
Intelligence Cycle, Big Data, OSINT, open source, SOCMINT

1. Artículo de reflexión vinculado al grupo de investigación "Cátedra Nebrija – Santander de análisis y resolución de conflictos" de la Universidad de Nebrija, España.
2. Doctorando en Ciencias Humanas, Sociales y Jurídicas de la Universitat International de Catalunya, España, y de la Universita Luiss Guido Carli, Italia. Magíster en Inteligencia de la Universita della Calabria, Italia. Magíster en Grafoanálisis Europeo, peritaciones y análisis de la Universidad Autónoma de Barcelona, España. Magíster en Seguridad e Inteligencia de la Libera Universita Hugo Grotius, Italia. Licenciado en Criminología de la Universidad de Alicante, España. Coordinador de Área de Seguridad y Defensa de la Universidad Nebrija y Coordinador de la Cátedra de Análisis y resolución de Conflictos Nebrija-Santander. Contacto: cpaya@nebrija.es
3. Candidato a doctor en Derecho de la Universidad de Murcia, España. Magíster en Derecho Penitenciario de la Universidad de Murcia, España. Magíster en Prevención de Riesgos de la Universidad Camilo José Cela de Madrid, España. Magíster en Análisis y Prevención del Terrorismo de la Universidad Rey Juan Carlos de Madrid, España. Licenciado en Criminología por la Universidad de Alicante, España. Miembro del grupo de investigación de la Cátedra Nebrija sobre "Conflictos territoriales en América Latina". Docente del área de Seguridad y Defensa de la Universidad Nebrija. Contacto: jdelgado@nebrija.es
4. Doctor en Psicología de la Universidad Complutense de Madrid, España. Licenciado en Psicología de la Universidad de Oviedo, España. Director de Postgrados en el área de Prevención de Riesgos Laborales de la Universidad Nebrija. Docente de la Universidad de Nebrija en el área de Psicología. Contacto: jfernanr@nebrija.es

defense policies and internal or external security of the states but now, due to technological advances, intelligence systems are evolving to adapt to changing scenarios, leading to greater complexity in the production of intelligence that no longer obeys a conventional stage. The notion of digital warfare and the arms based engineering computing, the potential of the Internet and open sources of information online, are the current challenges of the globalized models of force and military action of this century, becoming advance technology in a kind of actor on the international stage within the framework of the information age that requires an appropriate and capable intelligence.

Fundamento y justificación del estudio

La información en materia de inteligencia, desde el final de la Guerra Fría ha sido profusamente objeto de estudio y fundamentación, que en opinión de Díaz & Navarro (2015), durante la Guerra Fría, los servicios de inteligencia[5] de cada lado del telón de acero debían prestar gran atención al desarrollo de capacidades militares del enemigo, dadas las amenazas y riesgos que caracterizan el entorno globalizado, pero actualmente resulta más complejo, dado que el final de la Guerra Fría supuso un incremento de los conflictos violentos a escala mundial, en donde los arraigados criterios ideológicos que alimentaban esa amenaza convencional de un bloque enemigo orgánicamente identificado y con un orden de batalla determinado, se ha trasladado hacia amenazas que desarrollan una estructura no convencional, ramificada, inestable y flexible, pero dotada de una gran voluntad de actuación, que hacen de esta volatilidad estructural su principal medio de ocultación, y que podríamos encuadrar dentro del grupo de "amenazas asimétricas".[6]

En este sentido destaca Navarro (2012), la inteligencia y el método de obtención de esta, proporcionan un ámbito compartido con otros "agentes de conocimiento", aportando un valor fundamental para determinar mejores o más eficientes formas del desarrollo de la vida social, ideológica del Estado, aportando motivación y justificación a las políticas de seguridad interior o exterior y en la política militar de defensa, que actualmente debido a los adelantos tecnológicos y a la globalización, han precipitado que los Sistemas Militares de Inteligencia estén evolucionando para adaptarse a los escenarios cambiantes que han trasformado la organización y procedimientos, dando lugar a una mayor complejidad en la producción de inteligencia que ya no obedece a un escenario convencional donde los Estados se enfrentaban en el teatro de la contienda motivados por intereses diversos.

Ahora, el conflicto se ha extendido con nuevos actores que no necesariamente son Estados, como las Organizaciones Internacionales, los grupos terroristas o subversivos, las milicias paramilitares de grupos políticos, conflictos de baja intensidad o los nuevos desafíos no militares a la seguridad nacional -competitividad económica, terrorismo y corrupción, blanqueo de capitales, tendencias en materia poblacional, migraciones, economía internacional, etc-.

Esta nueva situación ha dado lugar a la "Guerra Asimétrica" en la que no necesariamente participan Estados.

Aun así, la Guerra Asimétrica, como todo tipo de guerra o conflicto, precisa de una Inteligencia apropiada y de órganos encargados de producirla. Es aquí donde entra el ciclo de inteligencia convencional adaptándose a las necesidades del propio conflicto arrojando información que se transforma en datos concretos a disposición usualmente del mando, o de decisores políticos u organizaciones diversas.

El ciclo de inteligencia representa un proceso que consta de varias fases denominadas indistintamente por autores u organizaciones, distinguiéndose según Vignettes (2010), en las seis fases siguientes:

Desde este ámbito, la elaboración de inteligencia presenta un claro rigor conceptual en la ejecu-

5. Desde esta perspectiva, podemos definir por tanto la inteligencia, en la obtención de información procesada, analizada, valorada, contrastada e interpretada, destinada a fundamentar la toma de decisiones para hacer frente a riesgos u amenazas presentes o futuras que afecten tanto a los estados como a sus ciudadanos.

6. Podemos encuadrar tales amenazas asimétricas las que se basan en la proliferación de actores no estatales en la esfera internacional y el consecuente aumento de distintos intereses contrapuestos como la lucha por los recursos escasos en donde los conflictos por los recursos naturales como el agua, petróleo, minerales estratégicos, escasez de alimento, las fuentes de energía, los conflictos separatistas o nacionalistas, las intenciones de grupos étnicos que pretenden tener su propio Estado, los conflictos entre naciones que tratan de extender sus fronteras para abarcar territorios donde habitan comunidades afines, luchas religiosas o fundamentalistas que tratan de ganar influencia y poder dentro de un mismo Estado o incluso en toda una zona geográfica, ampliando a zonas externas su poder de disuasión mediante la estrategia del terrorismo, o las guerras revolucionarias que tratan de imponer su ideología política en su propio país o en otros países de la misma región; luchas a favor de la democracia, el anticolonialismo, y las reivindicaciones indígenas; y un largo etc.

ción de su ciclo, e independientemente del ámbito en que se obtenga. El ciclo de inteligencia si bien es un modelo único, este, se adapta a cada situación particular. En este caso hablaremos del ámbito militar, y caracterizado como hemos indicado en las seis etapas enumeradas y que resumiremos como coincide la doctrina (Navarro, 2004), en cuatro episodios (1) dirección, (2) obtención, (3) elaboración, (4) difusión.

Gráfico 1: Ciclo de Inteligencia.

Fuente: Navarro, 2004.

El primer episodio "Dirección", será el conocimiento a alcanzar en materia de seguridad por un ente u gobierno, determinándose las necesidades de inteligencia y sus prioridades, planificándose la obtención de información a través de los órganos de inteligencia propios donde la subsidiariedad y la eficacia, determinarán el modo más eficaz de obtenerlo. Todo el trabajo de la fase de Dirección se vierte en documentos en los que, a partir de las "necesidades" de inteligencia identificadas, se seleccionan los "indicios" que puedan responder a aquellas y, en función de estos, se determinan las "misiones" que, finalmente, se asignan a las "fuentes". A nivel táctico, el documento gráfico se conoce como INTE (Integración Terreno Enemigo) y también como IPB -*Intelligence Preparation of the Battlefield*- adaptándose a cada caso concreto que lo ha solicitado.

El siguiente episodio, el de "Obtención" redunda en la consulta de las fuentes directas o indirectas disponibles, esto es recopilación de información, tanto de fuentes secundarias –más accesibles aunque menos fiables– como de fuentes primarias –con mayor dificultad de acceso pero con información de calidad, entregando la información obtenida a los órganos encargados de su procesamiento. Las fuentes son desde personas, a cosas o acciones de las que se obtienen noticias del enemigo, del terreno, de la meteorología y del ambiente, pudiendo ser obtenidas de variadas formas, ya sea mediante sensores terrestres, aéreos o navales, acciones de vigilancia o de reconocimiento, interceptaciones de comunicaciones y escuchas del espectro radioeléctrico, interrogatorios y entrevistas, examen de documentos. Cualquiera que sea la función del agente en una unidad en la Unidad Táctica, debe tener conciencia de la necesidad de participar en la recogida de información.

Los sistemas de obtención de inteligencia se pueden clasificar por su origen, principalmente, en los siguientes tipos: a) HUMINT o Inteligencia clásica, obtenida por medios humanos, pudiendo utilizar éstos medios auxiliares; b) IMINT o Inteligencia de Imágenes obtenida por sensores diversos, fotográficos, térmicos, infrarrojos, radares, etc.; c) SIGINT o Inteligencia de Señales que engloba a COMINT y ELINT; d) COMINT o Inteligencia de Comunicaciones obtenida de escuchas o interceptaciones; e) ELINT o Inteligencia Electrónica obtenida de las radiaciones electromagnéticas, distintas de las usadas en transmisiones; f) OSINT *Open-source Intelligence* Inteligencia proveniente de recursos abiertos que en los últimos años, a causa del desarrollo tecnológico en la era de la información, amplía su rango de acción a una clase de Inteligencia que tiene por objeto la realización de productos de valor añadido a partir de información procedente de fuentes abiertas residenciadas en páginas web, contribuyendo así a ampliar el rango de necesidades actuales de información, como producto de inteligencia, que en su defecto, o sin dedicarle la atención oportuna, esta corre el riesgo de estar permanentemente desactualizada. Este tipo de

fuente representa hasta el 85% de la información bruta que recibe un servicio de inteligencia y por tanto será la finalidad de este artículo abundando sobre ella y direccionando el interés sobre el fenómeno para observar el estado de la cuestión.

En el tercer episodio "Elaboración" se procesa la inteligencia por una serie de expertos, que denominados analistas de inteligencia, trabajarán con esta hasta condensarla en una información procesada, distinguiéndose diferentes etapas: a) La primera etapa es la "Compilación", es una actividad de registro y organización de todo lo recibido que facilita el resto del proceso; a veces también se lleva a cabo una primera transcripción de la información bruta recibida, para hacerla más fácilmente procesable; b) En la siguiente etapa, la "Valoración", se valoran los datos por su utilidad y por su posible fiabilidad -según su valor asignado- y se sigue en el proceso, archivándose para una utilización futura, destruyéndola o bien enviándola un escalón superior o lateral; c) Después, en la etapa de "Análisis", se analizan los datos, y se sacan deducciones, comparando éstas con otras informaciones ya existentes; d) Finalmente, la etapa siguiente es la de "Interpretación", en la que la información se transforma en inteligencia, extrayéndose conclusiones y formulando hipótesis al respecto.

En la fase de Elaboración y a un nivel táctico, las etapas descritas no necesariamente deben regir con el citado rigor lineal de la explicación, pudiéndose generalmente simultanearse o solaparse entre ellas, originando nuevas necesidades de inteligencia que confirmen o invaliden anteriores conclusiones o hallazgos provisionales. La finalidad de esta etapa es que el mando finalmente disponga conclusiones.

El cuarto episodio, "Difusión" esta pueda ser ofrecida bajo los parámetros que la dirección hubiere marcado, para realizar las acciones más correctas posibles al tener información fiable y completa, aplicable al contexto del mundo globalizado en el que vivimos donde las rápidas transformaciones geopolíticas están caracterizando nuestra época, que inciden particularmente en que la Inteligencia tenga una importancia crucial y creciente como apoyo al proceso decisional, que reduzca incertidumbres en cualquier proceso o toma de decisiones.

Una correcta difusión debe diversificar los riesgos y las amenazas para la seguridad y la estabilidad no solo nacional sino también internacional, como instrumento y método de recogida de información de importancia vital en el ciclo biológico de un país u organización, reduciendo los riesgos y aumentando considerablemente el grado de certeza sobre determinados eventos de carácter puntual, proporcionando al analista una variedad de datos que facilitan la obtención de un panorama más cercano a la realidad, en tiempo real, y a su vez, una mejor calidad del conocimiento obtenido.

Veamos por tanto las interrelaciones compartidas desde los diferentes productores de inteligencia.

La producción de inteligencia en los conflictos a nivel estratégico, táctico y operativo

Tanto táctica como estrategia suelen utilizarse erróneamente como sinónimos, pues aunque la estrategia representa el esquema implementado para alcanzar los objetivos, la táctica será el método previsto para alcanzar dichos objetivos, mientras que el adjetivo operacional, todavía resulta más complejo de delimitar por el amplio espectro que abarca dentro del léxico militar, utilizándose a pesar de la diferencia gramatical indistintamente operacional y operativo, aumentando la confusión terminológica. En este artículo conceptualizaremos la táctica como el sistema o método militar que se desarrolla para ejecutar un plan y obtener un objetivo en particular, resultando el plan que supone la puesta en marcha de lo establecido previamente por la estrategia, desarrollando aquello que ya se practicó y se entrenó.

La producción de Inteligencia[7] a nivel táctico se diferencia desde el punto de vista teórico, de los niveles estratégico y operativo ya que cuenta con

7. Una breve y concisa definición de Inteligencia puede definirse como "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 ventaja de producirse en contacto directo durante el conflicto[8] o la gestión de la crisis, trabajando con la información en bruto, pero que tiene en su contra la urgente necesidad de ser administrada al momento de obtenerse, sin capacidad de discernir la sobreinformación resultante o la propia fragilidad de los productos obtenidos.

Para este articulo definiremos por tanto Inteligencia Operativa como el despliegue suficiente de Inteligencia para llevar a cabo operaciones y en todo caso Inteligencia Operacional será el nexo entre los campos de la estrategia y de la táctica necesarios para la concepción y desarrollo de las operaciones, estableciendo posibilidades operativas o tácticas según corresponda, determinando características, limitaciones y vulnerabilidades del enemigo y proporcionando los antecedentes necesarios para realizar operaciones de Inteligencia en apoyo a la Conducción Operativa o táctica.

Para abordar la definición de Estrategia desde un punto de vista militar y seguidamente trasladar el término al ámbito de la inteligencia, es preciso previamente delimitarlo con exactitud, pues como hemos visto se solapan fácilmente las definiciones y cometidos propuestos a la hora de determinar el campo de actuación de cada fenómeno. Alonso Baquer (2000) la define así, "La Estrategia es tanto el arte de concebir planes de operaciones coherentes con los fines legítimos de una comunidad política, como el arte de conducir los ejércitos hacia objetivos decisivos" mientras que Clausewitz (1978) refiere que "la teoría de la gran guerra o la llamada Estrategia tiene extraordinarias dificultades y se puede afirmar que muy pocos hombres alcanzan conceptos claros" por su parte Sun-Tzu (1993, p. 21), elabora el concepto *"bing-fa"*, que podemos sin ser técnicamente concretos traducirlo por Estrategia, Sun Tzu mantiene que la guerra está basada principalmente en el engaño, "Una operación militar implica engaño. Aunque seas competente aparenta ser incompetente. Aunque seas efectivo, muéstrate ineficaz" y como ultima definición concisa si cabe a pesar de la época la tomamos de Von Bülow:

> El arte de la guerra tiene dos ramas, la Estrategia y la Táctica, la primera es la ciencia de los ejércitos fuera del campo visual; comprende todas las operaciones en la guerra y es parte de la ciencia militar cuyas relaciones se encuadran con la política y la administración; el estratega es el arquitecto, el albañil, el táctico. (Heinrich, 1806).

Esta última definición ha sido traída a colación para definir la labor de la inteligencia como una labor que se puede asemejar en alusión a Von Bülow como la propia de un albañil que se basa principalmente en los conocimientos teóricos aprendidos y trasladados mediante la experiencia a cada caso real en donde el ingenio del estratega, esto es en nuestro caso, como se desarrolle la inteligencia y la efectividad de esta, tiene la capacidad de anticipar situaciones o anticipar conocimiento sobre estas.

Características de la Inteligencia Operacional en los conflictos

Muy brevemente al objeto de esta revisión conceptual y ya aglutinando la suma de los diversos conceptos brevemente analizados, podemos definir a la Inteligencia Operacional como, el conocimiento obtenido con un fin práctico, mediante la observación, investigación, interpretación y predicción de los fenómenos necesarios que puedan imponer nuestra voluntad en el campo operacional, brindándonos la táctica oportuna para desarrollar la estrategia adecuada a cada fenómeno en particular, de modo que el nivel de Inteligencia Operacional, se situara entre la propia Inteligencia Estratégica y la Inteligencia Táctica no pudiendo delimitarse claramente los límites de cada particular proceso, dado la particular superposición que puede sucederse en el proceso de adquisición de Inteligencia en sus diferentes estadios, al cubrirse áreas atribuidas a otros productores de Inteligencia, dado que cada "espacio" de Inteligencia, dispone de su zona "táctica" de responsabilidad o interés.

A pesar de su denominación, la prognosis de Inteligencia desde el ámbito operacional enfoca su

8. Freund, define el conflicto del siguiente modo: "El conflicto consiste en un enfrentamiento por choque intencionado, entre dos seres o grupos de la misma especie que manifiestan, los unos respecto a los otros, una intención hostil, en general a propósito de un derecho, y que para mantener, afirmar o restablecer el derecho, tratan de romper la resistencia del otro eventualmente por el recurso de la violencia, la que puede, llegado el caso, tender al aniquilamiento físico del otro" (Freund, 1983, p. 65). Mientras que desde un ámbito social, pero con perfecta cabida en nuestro análisis, Dahrendorf señala que el conflicto es el motor de la historia, es lo que mantiene el desarrollo de la sociedad. Este conflicto, para ser socialmente relevante se manifiesta más allá de las relaciones individuales. Encuentra su ámbito de desarrollo entre los roles sociales, entre grupos sociales, entre sectores de la sociedad, entre sociedades y entre organizaciones supranacionales (Dahrendorf, 1959).

trabajo tanto a largo a medio o corto plazo, esto es acometiendo la obtención de inteligencia durante el tiempo de paz, el tiempo de conflicto o en la propia escalada y materialización del conflicto, mientras que la Inteligencia Estratégica elabora su presupuesto y frutos de inteligencia a largo plazo fundamentalmente y la Inteligencia Táctica se centra en la producción de inteligencia durante el propio conflicto y a muy corto plazo.

Es por ello que la Inteligencia Operacional no se considera un sistema independiente, más bien se trata de un subsistema dentro de un ecosistema de interrelaciones tácticas que coordina los niveles subordinados trabajando en conjunto para difundir inteligencia a sistemas superiores con capacidad de ejecutar en conjunto una estrategia, basada en los juegos de hipótesis y previsiones que la Inteligencia Operacional ha especulado y propuesto sobre escenarios probables de ayuda y decisión al mando. Es probable la discusión en que algunas agencias de inteligencia inciden sobre los modelos matemáticos basados en teoría de juegos que fundamenten si cabe, el menor margen especulativo posible. Veamos seguidamente la concepción que mantienen las Naciones Unidas respecto a cómo debe obtenerse, tratarse y difundirse la Inteligencia por los Estados.

Los principios de la inteligencia según la Organización del Tratado del Atlántico Norte -OTAN-

Como indicábamos anteriormente, la Inteligencia Operacional basa sus características propias bajo el condicionamiento y existencia de una necesidad concreta del mando operacional que requiere conocimiento sobre las debilidades del adversario, las intenciones de este a medio y largo plazo y la identificación de sus objetivos clave, tanto militares como sociopolíticos, adaptando los flujos de inteligencia a la particular necesidad solicitada, sin obviar como indicamos, los factores políticos nacionales e internacionales, que puedan someternos a la legalidad subyacente que básicamente son los principios básicos admitidos por la OTAN, tales como, la defensa colectiva, la gestión de crisis y la seguridad cooperativa.

Los países miembros de la OTAN contemplan ocho principios en los que deben basarse los niveles y escalones de la inteligencia militar. Los "Principios" son: Control Centralizado, Oportunidad, Explotación Sistemática de las Fuentes, Objetividad, Accesibilidad, Capacidad de Respuesta, Protección de las Fuentes, Revisión Continua y Comunicación. De estos ocho Principios, algunos son genéricos y válidos para todos los tipos de inteligencia, como, por ejemplo, la Objetividad, la Protección de las Fuentes o la Revisión Continua.

El Control Centralizado pretende evitar duplicaciones e interferencias entre los distintos órganos de Inteligencia, proporcionar apoyo mutuo entre los mismos y asegurar un uso económico y eficaz de los recursos. Por ello, el Mando Táctico no sólo asigna misiones a los órganos de Inteligencia sino que también centraliza medios y puede prohibir determinados esfuerzos.

Oportunidad la información o Inteligencia más precisa y fiable no tiene ningún valor si se dispone de ella demasiado tarde. Por la misma razón, el procedimiento de asignación de misiones de obtención debe ser capaz de responder, sin retraso, a cualquier cambio significativo en la situación.

La Explotación Sistemática de las Fuentes significa no sólo la asignación metódica de misiones a aquellas, sino también que las fuentes puedan utilizarse por los distintos órganos de inteligencia sin que haya barreras entre ellos.

Objetividad debe ser rechazada toda tendencia o intento de distorsionar la información, tratando de adaptarla a ideas preconcebidas. Hay que distinguir claramente los hechos probados de la conclusión e hipótesis a las que da lugar la interpretación de los mismos.

La Accesibilidad implica que la información bruta y la Inteligencia elaborada deben ser accesibles a los órganos de Inteligencia de todos los escalones. Por ello, los órganos de Inteligencia tienen que poder entrar en los archivos de los demás, lo que supone, hoy día, el acceso a sus sistemas informáticos. Como la cantidad de información obtenida de las fuentes va disminuyendo como consecuencia de las sucesivas redacciones de los encargados de

su gestión, en ocasiones, es preciso llegar a la información original.

Capacidad de Respuesta el órgano de Inteligencia debe estar organizada y disponer de los medios necesarios para dar respuesta, en cualquier momento, a las necesidades de Inteligencia.

Protección de la Fuente todas las fuentes de información estarán protegidas adecuadamente para asegurar la continuidad de su explotación en el tiempo.

Revisión Continua la Inteligencia ha de ser actualizada continuamente, corrigiéndola cuando sea necesario, considerando toda nueva información y comparándola con la ya conocida. De esta forma se garantizará su validez y capacidad para confirmar o rechazar hipótesis.

La Comunicación se refiere a que el flujo de información e Inteligencia entre los distintos escalones tácticos necesita ser ascendente, descendente y lateral, lo que obliga a disponer de un sistema de transmisiones rápido, fiable y redundante. a) Ascendente: todo mando tiene la obligación de hacer llegar a su inmediato superior toda información/Inteligencia o noticia que haya adquirido y que pueda ser de interés, aun sin orden expresa para ello; b) Descendente: obliga a poner en conocimiento de las Unidades subordinadas todas las informaciones/Inteligencia o noticias que puedan interesar a aquéllas; y c) Lateral: todo mando tiene que comunicar a los de su mismo nivel la información/Inteligencia o noticias obtenidas directamente que puedan ser explotadas por aquéllos.

En este ámbito, la Inteligencia no tiene valor sino se difunde, o no es accesible, a aquellos que la necesitan, debiendo llegar con facilidad a los diferentes órganos que la demanden. Existe el sesgo durante la compartición de Inteligencia que esta vaya disminuyéndose en las sucesivas transacciones, redacciones y elaboraciones para las diferentes cadenas de mando, por lo que será necesario intentar basarse siempre en las fuentes o brutos originales y durante estas elaboraciones, proteger la propia información para proteger a la fuente con el fin de compartir información ya sea mediante los mecanismos dentro de la OTAN y con entidades no OTAN y con los organismos y cadenas de mando que tengan capacidad de respuesta, de acuerdo con la política de seguridad OTAN en vigor.[9] Estos organismos deben poder analizar, fusionar, elaborar y presentar productos de Inteligencia del modo más rápido posible para decisores militares y no militares, y que además esta Inteligencia sea relevante, enfocada y diseñada para evolucionar con los retos de seguridad que se estén planteando.

Hemos descrito en líneas anteriores, diferentes conceptos que la doctrina militar ha mantenido inalterados durante décadas recurriendo a tradicionales consideraciones a la hora de definir o explicar los diversos procesos de Inteligencia, pero en la actualidad, el ámbito de la Inteligencia se ha ampliado, sometiéndose a una nueva redefinición, que comprenda una reelaboración de los programas de investigación y desarrollo de los ejércitos, referenciados a la consecución de los objetivos y la aplicación de los medios tecnológicos de organización y actuación militar de las fuerzas del siglo XXI. Esta redefinición que aludimos, no necesariamente debe implicar una reelaboración desde el punto de vista teórico, pues consideramos que los métodos tradicionales utilizados para la obtención de Inteligencia permanecerán, aunque lógicamente tenderán hacia un alcance más global, coexistiendo con los nuevos campos de obtención de Inteligencia que a nivel práctico suponen una necesaria revisión, lógicamente adecuada a los múltiples desafíos que plantean tanto la nueva realidad internacional, como los conflictos globales, estando en posición de proveer a los gobiernos la alerta temprana necesaria para enfrentar los desafíos emergentes.

En el siguiente epígrafe nos ocuparemos de este nuevo campo de obtención de Inteligencia, particularmente el que basa su estructura y producción en el análisis de las tecnologías residenciadas en la web habiendo adquirido la consideración de la información web, como un eje fundamental en los procesos de toma de decisiones en cualquier ámbito de la actividad humana, ya sea mediante el

9. Siguiendo estos parámetros OTAN, los organismos de inteligencia deben establecer una representación que proporcione inteligencia puntualmente, mediante una explotación sistemática de las fuentes y asignación metódica de tareas sin que haya barreras entre la interoperabilidad de los distintos órganos de inteligencia, donde la producción de inteligencia por estos, deberá 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 modelos Políticos, Militares, Económicos y Sociales.

cribado de sus datos estructurados o no estructurados, permitiendo al productor de Inteligencia, identificar tendencias, patrones, perfiles, establecer relaciones de significación a partir de grandes volúmenes de datos almacenados.

Las nuevas amenazas basadas en las fuentes y recursos informáticos

La concepción cibernética, la noción de guerra digital, la Inteligencia artificial y las armas autónomas, la ingeniería armamentista basada en la computación y los sistemas de información en línea son el desafío actual de los modelos globalizados de la fuerza y la acción bélica del presente siglo, donde los marcos de la doctrina nacional e internacional suponen un cuestionamiento de los límites entre la guerra y la paz, y los límites entre las fronteras regionales y el concepto de soberanía.

La conciencia bélica de la opinión pública internacional, legitima igualmente un cambio de estrategia y táctica militar en donde la concepción de los ejércitos actuales ilustra un escenario en el que la estrategia militar reorienta sus esfuerzos hacia el desarrollo y control de los sistemas de información, y los medios y tecnologías de la comunicación basados en web requieren una intervención propiamente como estrategia, ampliándose los conceptos tradicionales de la guerra y *per-se* de la Inteligencia que a esta se subordinaba, dado que las nuevas amenazas basadas en los recursos informáticos, obligan necesariamente a proveer la sofisticación electrónica de capacidad de respuesta y defensa necesaria, haciendo que la balanza de los objetivos de la Inteligencia se incline hacia las intenciones, más que a las capacidades, sin que, se menosprecie la importancia de ambos factores en la balanza (Díaz, 2009, p. 184).

El problema de la ciberguerra continuamente amenazado por los *hackers* y enemigos virtuales que intentan introducirse en los sistemas de seguridad nacionales, poniendo en peligro la estabilidad mundial, o desestabilizando los flujos financieros mundiales mediante el sabotaje económico. La victoria ante estas amenazas pasa obligatoriamente por el dominio de los sistemas de información que deben integrarse a la esfera militar, así como las estrategias de Inteligencia deben añadir al elenco de producción, las propiamente obtenidas a través de las nuevas tecnologías y comunicaciones electrónicas, reformulándose las bases metodológicas del pensamiento militar, concernientes a la seguridad pública y Defensa del Estado.

Por tanto, frente a una cultura militar operativamente mecanizada y de intervención masiva, la organización bélica del presente milenio, establece un modelo de organización militar descentralizado, fluido, dinámico y virtual y desterritorializado en donde la ONU, la OTAN, el Comando Norteamericano de Defensa Aeroespacial (Canadá y EE.UU.), el Sistema Interamericano de Defensa se coordinan y supervisan en la explotación e interceptación de las redes desde sus sistemas de inteligencia, donde insistimos, la concepción estratégico-militar debe direccionarse hacia el dominio sobre las nuevas tecnologías, las telecomunicaciones, y el control de las fuentes abiertas residenciadas en Internet como nuevo centro emergente, que provean sistemas de seguridad y técnicas de registro criptográfico para el control centralizado de la información considerada sensible.

Si a principios del presente siglo, los gobiernos se han afanado en una carrera tecnológico-armamentística, dotando a sus ejércitos de sistemas de inteligencia artificial, y de teledetección satelital para posibilitar mejoras en el espionaje y rastreo de objetivos, en los últimos años se ha venido implementando una carrera por parte de la Inteligencia de los países para tener presencia y tomar parte del control de las comunicaciones electrónicas, esto es las acometidas tanto por web como por telefonía móvil. En este artículo no nos adentraremos en las categorías y posibilidades de la inteligencia obtenida mediante la captación de redes móviles, pues requeriría desbordar el ámbito y objeto de la obtención de inteligencia mediante el cribado de datos en *BIG DATA.*[10]

10 IBM, considera que hay *"Big Data"*, si el conjunto de información supera el *terabyte* de información, es sensible al tiempo, y mezcla información estructurada con no estructurada. Así, su enfoque trata de buscar la forma mejor de aprovechar estos datos, su gestión, su combinación (datos estructurados con los que no lo son), la aplicación de algoritmos predictivos de comportamiento, y con todo ello, permitir la toma de decisiones que añadan valor al negocio.

Big data como herramienta de la seguridad y la defensa

Para el ámbito de interés de este artículo, el ámbito de la seguridad y la defensa resulta interesante analizar cómo el análisis del *Big Data* puede ser aplicado y ofrecer beneficios al objeto de extraer Inteligencia. En el ámbito que referimos de la seguridad y la defensa requiere tomar decisiones complejas a muy corto plazo dados los conflictos y/o crisis recientes y actuales han visto crecer su grado de complejidad, con líneas divisorias muy difusas entre lo civil y lo militar; entornos intensivos en información con creciente mezcla de escenarios reales o virtuales resultando un desafío.

De manera genérica podemos decir que la aplicación de *"Big Data"* a defensa y seguridad persigue capturar y utilizar grandes cantidades de datos para poder aunar sensores, percepción y decisión en sistemas autónomos, y para incrementar significativamente el que el entendimiento de la situación y contexto del analista y el combatiente o el agente del orden (Carrillo, Marco De Lucas, Dueñas, Cases, Fernández, González, & Pereda, 2013, p. 44).[11] Para poder trabajar con la creciente complejidad y abundancia de datos, es necesario un mayor enfoque en la comprensión de la situación, especialmente en aquellos ámbitos donde los objetivos (blancos, enemigos, criminales, etc.) son en apariencia de pequeña escala y/o de carácter ambiguo. En este sentido, para un mayor cribado direccionado a la creación de Inteligencia de las fuentes abiertas que trataremos, aludiremos la Inteligencia denominada OSINT, acrónimo derivado de su nombre en inglés *Open-source Intelligence.*[12]

Aunque *OSINT* ya hemos abundado no es un término nuevo, si cabe, igualmente ve necesaria su redefinición dado que la consideración que se le prestaba radicaba principalmente en que desde antaño, mantenía un concepto tradicional de recopilación de información, igualmente de fuentes abiertas, pero basado fundamentalmente en el estudio de televisión y prensa extranjera, entrevistas con los hombres de negocio o turistas a la vuelta de un viaje o colaboraciones con expertos académicos, pero que actualmente, dado el aumento de la capacidad de almacenamiento de información residenciado en las fuentes abiertas web, y que exponencialmente ha crecido en los últimos años, genera cada día una enorme cantidad de información consciente o inconscientemente[13], evidenciándose las potencialidades de Internet y sus alcances globales, convirtiéndolo en una suerte de actor en el escenario internacional en el marco de la era de la información.

El principal documento[14] de la OTAN sobre OSINT[15] identificaba cuatro categorías en las fuentes abiertas (Davara, s.f., pp. 69-71): a) OSD *(Open Source Data;* Datos de fuentes abiertas): impresión en bruto, radiodifusión, informe oral u otra forma de información de una fuente primaria, como una fotografía, una grabación, una imagen de satélite comercial, etc.; b) OSIF *(Open Source Information;* Información de fuentes abiertas): integrada por datos que se agrupan generalmente por medio de un proceso de edición que proporciona algún tipo de filtrado y validación, así como una gestión de su presentación; c) OSINT *(Open Source Intelligence;* Inteligencia de fuentes abiertas): información que deliberadamente ha sido obtenida, discriminada, extraída y desimanada a personas seleccionadas, todo ello con objeto de responder a una pregunta o tema específico; d) OSINT Validada (OSINT-V): información a la que se puede atribuir un muy alto grado de certidumbre. Puede ser producida por un

11. En el citado Manual, los autores identifican hasta 12 aplicaciones en donde el *BIG DATA* puede arrojar ventajas frente a otras soluciones tecnológicas. Las diferentes aplicaciones son las siguientes: Detección de intrusión física en grandes espacios o infraestructuras abiertas, Computación sobre información encriptada, Análisis automático de vulnerabilidades de red (máquinas-tráfico de datos), Criminología computacional, Uso fraudulento de recursos corporativos y/o sensibles, Análisis de video en tiempo real/Búsqueda y recuperación rápida en librerías de video, Inteligencia visual en máquinas, Identificación de anomalías, patrones y comportamiento en grandes volúmenes de datos, Análisis de texto (estructurado y no estructurado) como apoyo a la toma de decisión en tiempo real en entornos intensivos en datos, Consciencia situacional, Traducción automática a gran escala (en número de idiomas y en volumen), Predicción de eventos

12. Tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público, comprendiendo cualquier tipo de contenido, fijado en cualquier clase de soporte, papel, fotográfico, magnético, óptico, etc. que se transmita por el medio y que se puede acceder en modo digital o no, y a disposición pública, difundido por canales restringidos o gratuitos. Podemos considerar fuentes abiertas de ámbito OSINT: a) Datos extraíbles de la Internet abierta, frecuentemente de la web abierta; b) Estudios e informes, white papers, revistas especializadas y otras fuentes de literatura gris; c) Repositorios abiertos, tanto públicos como privados; d) Registros administrativos públicamente accesibles.

13. Como por ejemplo cuando se reserva un billete de avión, se paga con una tarjeta de crédito, se entra en un servidor para ingresar el e-mail, se participa o es participado en una red social, blogs, foros de Internet o sencillamente se interactúa ante la infinidad de sensores de las ciudades inteligentes (Smart Cities).

14. En ; http://www.nato.int/cps/en/natohq/topics_68372.htm?selectedLocale=en
OTAN Open Source Inteligencia Manual,
OTAN Open Source Inteligencia Reader
OTAN Inteligencia explotación de la Guía de Internet.

15. El concepto OSINT, tiene su origen en los Estados Unidos como método de inteligencia analítica estandarizado y diseñado para cumplir tareas específicas o toma de decisiones de apoyo. No debe ser confundido con el OSIF, que representa toda la información a disposición del público de código abierto que se basa los análisis OSINT.

profesional de inteligencia de todo tipo de fuente, con acceso a las clasificadas, trabajando para una nación o como personal de una coalición.

En este sentido, la creciente importancia de las fuentes abiertas ha llevado a la creación de organismos específicos como el estadounidense *Open Sources Center,* (OSC),[16] mientras que en la Unión Europea, se han llevado a cabo iniciativas como el Eurosint,[17] orientado a la cooperación europea en materia de Inteligencia y al uso intensivo de las fuentes abiertas para elaborar Inteligencia en la prevención de amenazas para la paz y la seguridad. O, por ejemplo, uno de los *think tanks* más importantes del mundo. *Stockholm International Peace Research Institute* -SIPRI-[18] es un instituto de estudios estratégicos dedicado a la investigación de los conflictos, a la producción, comercio y control del armamento, al gasto militar, la prevención, los conflictos, y la seguridad internacional. En el caso británico, podemos dar relevancia al NEC,[19] que es una red que engloba 10 redes especializadas. Sin olvidar igualmente el potencial de la NSA[20] para abarcar también este campo de estrategia. La OTAN dispone del sistema se NNEC,[21] similar en la teoría al sistema británico.

La adquisición de Inteligencia a partir de las nuevas tecnologías y su encuadre dentro de la estrategia

Actualmente, los sistemas de ayuda al mando en la toma de decisiones, formados fundamental por los órganos de inteligencia, están evolucionando hacia un "sistema de sistemas", en el que se integran en una única red sensores, decisores, plataformas varias e Inteligencia, con la finalidad de aumentar la capacidad de acción de las fuerzas por una mejor explotación de la información, mediante la superioridad que supone la obtención de información relevante y decisiva para el combate, a través de la explotación oportuna de inteligencia, siendo válido tanto para la batalla convencional como para el enfrentamiento asimétrico.

El desarrollo de la tecnología ha desatado una explosión de información que tiene la virtud de difundirse muy rápidamente, conociéndose las noticias prácticamente al momento de producirse e incluso durante o antes de sucederse, difundiéndose de manera global. En este contexto de sobreabundancia de información el papel del profesional de inteligencia cobra relevancia, en la gestión del conocimiento, y donde la capacidad de anticipación y de respuesta ante los diferentes eventos supera cualquier otra concepción anterior de producción de inteligencia, dado que el enorme flujo de información recibida a través de las redes digitales, puede, por una parte, saturar el sistema y, por otra, producir indecisión en el Mando ante el cúmulo de noticias y su rápida variación.

El impacto de las nuevas tecnologías en el campo de la Inteligencia ha sido de tal repercusión que se puede decir que en la producción de Inteligencia se ha pasado de un estadio artesanal a otro industrial (Sainz de la Peña, 2012, p. 227), en donde proliferan organizaciones y entidades de todo tipo generando información de calidad, universidades, memorias, anuarios, papeles de trabajo, literatura gris, bases de datos, documentación electrónica, organismos públicos, y privados, *think tank* de toda clase.

En la Inteligencia de código abierto, la recopilación de información difiere generalmente de las diferentes disciplinas de la Inteligencia que hemos referenciado, consolidándose en las agencias de inteligencia una nueva conceptualización de la estrategia operacional basada en estos recursos, básicamente porque la obtención de información en bruto a analizar puede ser un desafío importante, especialmente si son objetivos no cooperativos, independientemente esté residenciada en fuentes

16. Véase;https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

17. Véase; https://www.eurosint.eu/

18. Ver en: http://www.sipri.org/

19. En el NEC británico hay un enlace directo entre el nivel Estratégico y el Táctico, lo que abunda en la idea de que en las situaciones actuales de "asimetría", el nivel Táctico se convierte, muchas veces, en Operativo y que los medios tecnológicos del nivel Estratégico pueden trabajar directamente para el Táctico.

20. La (NSA) National Security Agency es responsable de la protección, desarrollo y control de las comunicaciones militares y administrativas, el desarrollo de las tecnologías de la información, la seguridad de las redes informáticas, el espionaje vía satélite y la coordinación de la guerra en el espacio, entre los Estados Unidos y los servicios de información de Reino Unido, Canadá, Australia y Nueva Zelanda, entre otros. En todo el mundo, todas las comunicaciones por correo electrónico, teléfono y fax son regularmente interceptadas por Echelon, cuyos ordenadores extraen de la masa de informaciones los mensajes que contengan palabras-clave sensibles".

21. Para la OTAN, el NNEC representa el enfoque y la política común para armonizar el uso de las nuevas tecnologías, con la finalidad de usarlas en futuras misiones. El problema que se planteará es que la OTAN no tiene órganos propios de Inteligencia y que depende de los de las naciones aliadas.

abiertas[22] o en la minería de datos.[23] En este mismo contexto de fuentes abiertas, se está produciendo un gran movimiento alrededor de lo que se conoce como *Open Data,* implicando que los datos puedan ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen, siendo sus características fundamentales las siguientes: a) Disponibilidad y acceso: la información debe estar disponible como un todo y a un costo razonable de reproducción, preferiblemente descargándola de internet. Además, la información debe estar disponible en una forma conveniente y modificable; b) Reutilización y redistribución: los datos deben ser provistos bajo términos que permitan reutilizarlos y redistribuirlos, e incluso integrarlos con otros conjuntos de datos; y c) Participación universal: todos deben poder utilizar, reutilizar y redistribuir la información.

El termino recientemente acuñado en el diccionario LID de Inteligencia y Seguridad[24] de -SOCMINT- y definido como la "actividad de inteligencia referida a las redes sociales y medios sociales de comunicación de plataforma digital y los datos que las mismas generan" y que podríamos esquematizarlo según Álvarez & Perdomo (2002), como la interacción entre las funciones y roles de las redes sociales, vuelcan la Inteligencia de Fuentes Abiertas (OSINT), creándose la Inteligencia en Redes Sociales (SOCMINT), las interrelaciones entre los medios de comunicación tradicionales y los medios con soportes en redes sociales y web 2.0 (social media + más media), las operaciones de activismo en la red *(hactivism)* y la ingeniería social.

La web 2.0 supuso un cambio en el modo de comunicación de los usuarios en Internet, de forma que los usuarios dejan de ser meros receptores de información y comienzan a ser generadores de la misma, como ejemplo lo supone el que hoy en día, la mayor parte de los usuarios forman parte de las redes sociales, disponen de sus propios blogs o participan en foros que provoca que el volumen de información disponible haya crecido de forma exponencial en los últimos años.

Este bruto ingente de información[25] que se puede obtener a través de la obtención, gestión, integración, análisis, filtrado, refinamiento y síntesis de la información ubicada en todo tipo de soportes y formas de transmisión y comunicación de información en las fuentes web,[26] se cimenta generalmente en el pasado, pero a los efectos de obtener inteligencia es útil para comprender el presente y hacer predicciones futuras, ya que normalmente las decisiones se basan en experiencias pasadas, siendo posible identificar tendencias, anomalías y amenazas, destacándose por tanto la importancia del papel de los profesionales que gestionen estas fuentes, aplicadas a la seguridad, la defensa nacional así como la toma de decisiones en general.

Por su parte, OSINT acrónimo derivado de su nombre en inglés *Open-source Intelligence*[27] en los últimos años, a causa del desarrollo tecnoló-

22. Por su parte Martín de Santos & Vega (2010): "Las fuentes abiertas de información incluyen tanto la Internet superficial como la profunda (también llamada invisible), el correo electrónico, así como las fuentes de los medios de comunicación tradicionales, incluyendo los medios dirigidos a un público específico y boletines especializados y de los foros de discusión en línea. Se incluye la literatura gris, expertos (o especialistas) en determinados temas y cualquier persona que tenga conocimiento de algo por haber sido testigo directo de ello o haberlo vivido" (pp. 91-112). Por otra parte Iravedra (2011) dice que: "Fuentes abiertas son las que no están clasificadas".

23. La minería de datos o *data mining* o "el arte de sacar conocimiento de grandes volúmenes de datos" es una técnica que "consiste en extraer información de los algoritmos que contienen las grandes bases de datos que acumulan la historia de las actividades de las organizaciones" (Martínez, 2011, pp. 55-63). Las redes de transmisiones digitalizadas, con su gran capacidad y velocidad de transmisión, permiten que las comunicaciones tácticas y, dentro de ellas, de las utilizadas por los órganos de Inteligencia. Como ejemplo; en la primera guerra de Irak, una fuerza de 500.000 hombres disponía de 100Mbits de banda ancha; unos 12 años más tarde, los 350.000 combatientes de la *"Operation Irak Freedom"*, en la segunda guerra de Irak se apoyaban en 3.000Mbits.

24. Ver:https://www.google.es/search?q=dicionario+LID+inteligencia&ie=utf-8&oe=utf-8&gws_rd=cr&ei=iX3UVbu8CobnUtTUr8gN#q=diccionario+lid+inteligencia+y+seguridad+pdf

25. La proliferación del uso de Internet y la facilidad de publicación de contenidos a través de diferentes medios como redes sociales o blogs ha favorecido que se almacene una ingente cantidad de información online. Las cifras más significativas son las siguientes: a) Usuarios de Internet; aproximadamente 2.500 millones de usuarios; b) Únicamente el servidor Google, almacena 30 billones de páginas web, o lo que es lo mismo, más de 1.000 terabytes de información; c) La red social Facebook tiene más de 1.000 millones de usuarios, 60 millones de páginas y 270.000 millones de fotos subidas; d) La red social Twitter tiene cerca de 240 millones de usuarios activos que escriben diariamente cerca de 600 millones de tweets; e) La red social Tumblr tiene cerca de 180 millones de blogs y alrededor de 55.000 millones de posts; f) La red social Flickr tiene casi 90 millones de usuarios y más de 10.000 millones de fotos; g) La red social Instagram cuenta con más de 350 millones de usuarios activos, que han subido 30 billones de fotos desde el 2010. Aproximadamente se suben a la red social 5 millones de fotos diariamente.

    Estos son algunos de los datos representativos más conocidos, sin mencionar la cantidad de información disponible en la *DEEP WEB*, así como también aquella información no accesible para el usuario común, pero existente dentro de la Web en capas invisibles o profundas, cuyos contenidos no son accesibles desde motores de búsqueda comunes y conocida como *WEB DATA MINING*.

26. No olvidemos que la *World Wide Web* tiene un origen como experimento y herramienta militar.

27. Tipo de Inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público, comprendiendo cualquier tipo de contenido, fijado en cualquier clase de soporte, papel, fotográfico, magnético, óptico, etc. que se transmita por el medio y que se puede acceder en modo digital o no, y a disposición pública, difundido por canales restringidos o gratuitos. Podemos considerar fuentes abiertas de ámbito OSINT: a) Datos extraíbles de la Internet abierta, frecuentemente de la web abierta; b) Estudios e informes, white papers, revistas especializadas y otras fuentes de literatura gris; c) Repositorios abiertos, tanto públicos como privados; d) Registros administrativos públicamente accesibles.

gico en la era de la información, la inteligencia OSINT amplía su rango de acción a una clase de Inteligencia que tiene por objeto la realización de productos de valor añadido a partir de información procedente igualmente de fuentes abiertas como las descritas, y particularmente las fuentes abiertas residenciadas en páginas web, contribuyendo así a ampliar el rango de necesidades actuales de información, como producto de inteligencia, que en su defecto, o sin dedicarle la atención oportuna, esta corre el riesgo de estar permanentemente desactualizada.

Determinados los alcances e importancia de OSINT, hemos de revelar nuevamente que este no es un concepto moderno, siquiera en su actual entendimiento, pues ya desde hace más de una década, la OTAN, le concede especial relevancia, como lo evidencia el ejemplo del programa -EUSC- formado por un centro de satélites dedicado a la producción y explotación de inteligencia a partir de información de origen espacial, por medio del análisis de datos de satélites comerciales. También la Agencia Europea de Defensa -EDA- ha puesto en marcha programas de desarrollo de herramientas de prospectiva y análisis OSINF y de formación de inteligencia OSINT.

En este sentido y como impulsor, destaca principalmente los Estados Unidos, cuyos servicios de inteligencia han concedido una gran importancia a OSINT, mediante la transformación, en 2005, del Servicio de Información de Emisiones del Exterior (FBIS) en el Centro de Fuentes Abiertas -OSC-, incorporado OSIF y OSINT, en sus rutinas de Inteligencia militar implantado la red IKN *(Intelligence Knowledge Network)* proporcionando servicios de inteligencia al Ejército. Francia, por su parte está impulsando la plataforma HERISSON *(Habile Extraction du Renseignement d´intéret Stratégique a partir de Sources Ouvertes Numérisées)* de integración de información de fuentes abiertas.

Gráfico 2: Open-source Intelligence

Fuente: Elaboración propia.

a) Requisitos: en esta etapa se establecen los parametros minimos y maximos que deben satisfacerse para conseguir el objetivo que ha activado el desarrollo del sistema; b) Fuentes de información: esta etapa consiste en identificar a partir de los parametros establecidos, las fuentes de interés que serán recopiladas; c) Adquisición: en esta etapa se obtiene la información a partir de los orígenes indicados; d) Procesamiento: esta etapa consiste en dar formato a toda la información recopilada para que posteriormente pueda ser analizada discriminándola del bruto obtenido. e) Análisis: en esta etapa se genera inteligencia a partir de los datos recopilados y procesados, habiendo relacionado la información buscando los patrones que permitan llegar a conclusiones significativas; f) Inteligencia: esta etapa consiste en presentar la información potencialmente útil y comprensible, para que pueda ser correctamente explotada.

Queda abierto por tanto el debate que deberá acontecer desde el ámbito militar y el ámbito académico-legal para adelantar los parámetros que dilucidaran las respuesta de la Inteligencia sobre los fenómenos y retos de la Inteligencia que se avecinan, tales como las plataformas informáticas cuánticas, la guerra informática y digital o la ingeniería armamentista basada en la computación, las potencialidades de Internet y las fuentes abiertas de información en línea.

Referencias

Alonso, M. (2000). ¿En qué consiste la Estrategia? Madrid: Ministerio de Defensa.

Álvarez, L. & Perdomo, C. (2002). Inteligencia, Ciberseguridad y Ciberdefensa; nuevas implicaciones conceptuales en las Estrategias de Seguridad Nacional. Universidad de Las Palmas de Gran Canaria.

Carrillo, J., Marco De Lucas, J., Dueñas, J., Cases, F., Fernández, J., González, G. & Pereda, L. (2013). Big data en los entornos de defensa y seguridad. (Documento de Investigación, 03). Madrid: Centro Superior de Estudios de la Defensa Nacional -CESEDEN-. Recuperado de *http://www.ieee.es/Galerias/fichero/docs_investig/DIEEEINV03-2013_Big_Data_Entornos_DefensaSeguridad_CarrilloRuiz.pdf*

Clausewitz, C, V. (1978). De la guerra. Madrid: Ediciones Ejército.

Blanco, J. & Díaz, G. (2015). Presente y futuro de los estudios de inteligencia en España. (Documento marco, 11). Madrid: Instituto Español de Estudios Estratégicos. Recuperado de *http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM11-2015_EstudiosSeguridadEspana_JMBlanco-GustavoDiaz.pdf*

Dahrendorf, R. (1959). Clases sociales y su conflicto en la sociedad industrial. Madrid: Rialp.

Davara, F. (2009). Información de fuentes abiertas sin secretos. Revista Atenea, 12, pp. 68-71. Recuperado de *http://issuu.com/ateneadigital/docs/atenea_12_web*

Díaz, G. (2009). La inteligencia y el estudio de las relaciones internacionales. En Inteligencia teórica. Aproximaciones metodológicas al estudio de la inteligencia en España. Madrid: Ediciones Singulares.

Dietrich, F. (1757-1807). Espíritu del sistema moderno de guerra. Madrid: Eusebio Álvarez.

Freund, J. (1983). Sociología del Conflicto. París: Presses Universitaires de France.

Iravedra, J. (2011). Inteligencia de fuentes abiertas en la Unión Europea (proyecto Virtuoso. La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a amenazas. Madrid: Instituto Universitario «General Gutiérrez Mellado»- Universidad Nacional de Educación a Distancia.

Martín de Santos, I. & Vega, A. (2010). Las fuentes abiertas de información: un sistema de competencia perfecta. Inteligencia y Seguridad: revista de análisis y prospectiva, 8, pp. 91-112.

Martínez, G. L. (2011). Minería de datos: Cómo hallar una aguja en un pajar. Ingenierías, 53, pp. 55-63.

Navarro, D. (2012). Lecciones aprendidas (y por aprender): Metodologías de aprendizaje y herramientas para el análisis de inteligencia. Revista del Instituto Español de Estudios Estratégicos.

Navarro, D. (2004). El ciclo de inteligencia y sus límites. Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol, 48

Sainz de la Peña, J, A. (2012). Inteligencia Táctica. UNISCI Discussion Papers, 28, p. 227.

Sun Tzu. (1993). El arte de la guerra. Versión de Thomas Cleary. Madrid: Editorial Edaf.

Vignettes, M. (2010). El Ciclo de Inteligencia: naturaleza y alternativas. Inteligencia y Seguridad, en Revista de Análisis y Prospectiva; Jun-Nov.

ESCUELA SUPERIOR DE GUERRA
COLOMBIA

Fundada en 1909
Unión, Proyección, Liderazgo

Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados

Registro Calificado Res. MEN 10334 de 2010. Cód. SNIES 90906

Inscripciones abiertas

ISO 9001:2008
NTCGP 1000:2009
BUREAU VERITAS Certification

ESCUELA SUPERIOR DE GUERRA
Carrera 11 No. 102-50. Of. 327, Bogotá
Conmutador: 620 40 66 Extensión 21067 - 20618
Teléfono Directo 629 49 90

GESTIÓN DE LA CALIDAD NTCGP 1000:2009 SECTOR PÚBLICO
CERTIFICADO