

# Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información

Artículo

Por Miguel Ángel Esteban Navarro y Diego Navarro Bonilla



Miguel Ángel Esteban Navarro. Doctor en historia, profesor titular de biblioteconomía y documentación en la Universidad de Zaragoza. Especialista en gestión de la información en las organizaciones.

**Resumen:** Se muestra en qué medida la gestión del conocimiento puede ayudar a la mejora de los servicios de inteligencia. Una vez definido lo que se entiende por gestión del conocimiento, se describen cuáles son los rasgos de los recursos de información de una organización y de los sistemas integrados de gestión de la información que permiten su implantación. Posteriormente se analiza el fin y el proceso de creación de conocimiento por los servicios de inteligencia para la seguridad y la defensa, mediante la descripción de sus etapas (planificación, toma de datos, procesamiento, análisis y producción, comunicación y evaluación) y los principales medios tecnológicos, humanos y documentales de obtención de información. Finalmente, se destaca la importancia de la auditoría de información como necesario punto de partida y se exponen sus actividades.

## Palabras clave:

Gestión del conocimiento, Servicios de inteligencia, Seguridad, Defensa, Recursos de información, Ciclo de inteligencia, Auditoría de información, Fuentes de información, Infoguerra.

## Title: Knowledge management and intelligence services: the strategic dimension of information

**Abstract:** Discussion of the importance of knowledge management for improving intelligence services. Having first defined knowledge management, the article goes on to discuss the characteristics of information resources within an organisation and of the integrated information management systems that allow KM to be implemented. The aims and processes of knowledge creation by intelligence services—for security and defence—are analysed by way of the description of the stages involved (planning, data collection, processing, analysis and production, dissemination and evaluation) and of the principal technical, human and bibliographic means needed for information gathering. Lastly, the article highlights the importance of the information audit as a starting point, together with related activities.

**Keywords:** Knowledge management, Intelligence services, Security, Defence, Information resources, Intelligence cycle, Information audit, Information sources, Information warfare.

**Esteban Navarro, Miguel Ángel; Navarro Bonilla, Diego.** “Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información”. En: *El profesional de la información*, 2003, julio-agosto, v. 12, n. 5, pp. 269-281.

Diego Navarro Bonilla. Licdo. y doctor en documentación por la Univ. Carlos III de Madrid. Profesor ayudante del Depto. de Biblioteconomía y Documentación de dicha universidad. Autor de diversos trabajos sobre archivística y gestión de documentos administrativos. Premio Defensa 2003 en la categoría “Investigación histórica”, otorgado por el M<sup>o</sup> de Defensa.



## 1. Introducción

El año 2001 marcará posiblemente un punto de inflexión en los servicios de inteligencia para la seguridad y defensa nacional. En la reiterada sociedad de la información fueron precisamente la falta de ésta o la no integración de los datos disponibles por una deficiente gestión, algunas de las causas que permitieron los atentados del 11 de septiembre en Washington y Nueva York.

Se necesitan soluciones concretas capaces de controlar y convertir en conocimiento útil las ingentes cantidades de información que deben procesar los organismos responsables de la inteligencia de un país. Y en su búsqueda se encuentra con la gestión del conocimiento, para permitir que los servicios de inteligencia se transformen, en palabras del director del *Plan maestro de la inteligencia militar* de los EUA **Keith Masback**, en “una fuerza basada en el conocimiento, rápi-



damente desplegable y globalmente enfocada” (2002). Sólo esto permitirá que la inteligencia nacional cumpla el objetivo de “ver primero, comprender primero, actuar primero y terminar con decisión”.

En este contexto se debe situar la creación en España del *Centro Nacional de Inteligencia*, aprobada el 6 de mayo de 2002 por el *Congreso de los Diputados* a partir de la remodelación del *Centro Superior de Información para la Defensa (Cesid)*, fundado en 1977. El *CNI*, adscrito orgánicamente al *Ministerio de Defensa*, tiene como fin “facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del estado de derecho y sus instituciones”<sup>1</sup>. Corresponde al Gobierno

### Inteligencia, vigilancia y reconocimiento

La noche del 20 de noviembre de 2001, un avión de reconocimiento por control remoto UAV (*unmanned aerial vehicle*) RQ-1A “*Predator*”, equipado con una cámara infrarroja con transmisión de imágenes por satélite, detectó un grupo de vehículos que llegaba a un hotel de la ciudad afgana de Gardez. Se trataba de una reunión de miembros de *Al Qaeda* en la que se encontraba **Mohamed Atef**, cerebro de los atentados contra las embajadas estadounidenses de Kenia y Tanzania en 1998. Todos ellos resultaron muertos tras la localización precisa por los sensores del avión y el posterior ataque aéreo con bombas “inteligentes” lanzadas por 3 aviones *F-15*. Las imágenes captadas se transmitían en tiempo real al centro de procesamiento en tierra de la *CIA* y simultáneamente al comandante en jefe del *Comando Central*, general **Tommy Franks**, en Florida. Desde allí, la información se transmitía al cuartel general de la *CIA* en Langley (Virginia) y al *Pentágono*. El mismo tipo de avión, a lo largo de numerosas misiones de búsqueda y destrucción, guió hasta el objetivo con sus imágenes de alta resolución obtenidas y transmitidas en tiempo real a los aviones *AC-130 “Spectre”* durante la operación *Libertad Duradera* dirigida por el ejército de *EUA* en Afganistán.

Las actuaciones de este pequeño pero costoso aparato confirmaron en una campaña bélica real el éxito de un nuevo concepto de guerra aérea conocida bajo las siglas *ISR* (*intelligence, surveillance and reconnaissance*) (**Grier**, 2002). El desarrollo de la *ISR* se debe enmarcar en el éxito de la doctrina del “ataque preventivo”, elaborada por el *Secretario de Defensa* de *EUA* **Donald Rumsfeld**, por la que se considera legítimo el desarrollo y la aplicación efectiva de todos los medios defensivos y ofensivos para cortar de raíz una posible o probable amenaza de cualquier naturaleza y origen, antes incluso de que se produzca.

La *ISR* es el inicio de la ciberguerra: la guerra de robots contra hombres o entre ellos. En la *Primera Guerra del Golfo*, 40 soldados iraquíes aislados en una trinchera en medio del desierto vieron llegar un avión teledirigido espía no tripulado, destinado a marcar la posición del enemigo a la artillería. Rápidamente salieron de la trinchera, tiraron sus armas, alzaron las manos y se rindieron ante la máquina (**Virilio**, 1997, p. 99).



Biblioteca de la Agencia Central de Inteligencia (EUA)

determinar y aprobar anualmente los objetivos del *CNI* mediante la *Directiva de Inteligencia*, que tendrá carácter secreto.

El cambio de nombre de la versión española de este organismo clave en el sistema de seguridad y defensa de los estados actuales, que se produce aprovechando un proceso de redefinición del marco legal y el control parlamentario de sus actividades, no es accidental. Es el reconocimiento de que su objetivo principal es la producción de inteligencia por encima de la obtención de información que, aun siendo una tarea imprescindible para lograr aquella, está a su servicio<sup>2</sup>. El estudio, análisis del entorno y de sus actores así como las propuestas de medidas a partir de esos trabajos son actividades fundamentales del *CNI*, como lo son de la *Agencia Central de Inteligencia* de los *EUA*, cuyo nombre manifiesta desde su fundación la materia que debe producir, y de otros servicios de inteligencia como el *MI 6* británico o el *Mossad* israelí.

Si atendemos a la naturaleza y el fin de esas actividades y al hecho de que la información obtenida por diversas fuentes es el elemento con el que se trabaja, descubrimos que estamos ante lo que se denomina en la actualidad un proceso de gestión del conocimiento. Sin embargo, la tradicional mutua ignorancia entre el cerrado y reservado mundo de los servicios de inteligencia para la seguridad y la defensa, así como el abierto universo de la gestión de la información documental, dificulta la necesaria ósmosis de conocimientos y habilidades que enriquecería a ambas esferas. Su origen se encuentra, principalmente, en el diverso ámbito de aplicación de sus trabajos, los diferentes valores culturales que están detrás de los modos de adquisición, selección, tratamiento, difusión y uso de la información e incluso la procedencia y el estatus profesional de sus miembros.

## 2. De la gestión de la información a la gestión del conocimiento

El uso del término gestión del conocimiento se ha generalizado en los últimos 5 años en áreas tan diver-



sas como la administración y organización de empresas, la documentación, la informática y la ciencia de la administración. Pero no existe una definición precisa y universalmente aceptada sobre su significado, ni siquiera dentro de cada área. Esto se debe a que su campo de acción no está delimitado con nitidez, su fin no está trazado con precisión, su método de análisis de la realidad sobre la que opera y de diseño y guía de sus actividades está en elaboración, sus técnicas no están suficientemente contrastadas y sus resultados todavía están por llegar. De momento la gestión del conocimiento en las organizaciones es más un proyecto y un deseo que una realidad.

No obstante, de entre las múltiples y variadas aproximaciones a este concepto destacan 3 rasgos comunes: la convicción de la existencia de información y conocimiento en las organizaciones que se deben identificar y procesar; la incidencia en su carácter dinámico (relación con otros procesos) y utilitario (mejora de procesos); y la consideración del conocimiento como un factor estratégico clave en una organización para el logro de sus objetivos, de modo que una gestión eficaz lo convierte en un activo que aumenta el valor de la empresa.

**«Conocimiento e información no son sinónimos, porque acumular información no supone tener más conocimiento y procesar información no es lo mismo que aprovechar el conocimiento»**

La gestión del conocimiento es, por tanto, la disciplina que se ocupa de la investigación, el desarrollo, la aplicación y la innovación de los procedimientos y los instrumentos necesarios para la creación de conocimiento en las organizaciones, con el fin de aumentar su valor y ventaja competitiva. El objeto de su práctica es la construcción de un sistema de producción de conocimiento útil en una organización para la toma de decisiones y la resolución de sus procesos estratégicos



Sede de la Agencia Central de Inteligencia en Langley (Virginia)

### Infoguerra y dominio informacional

La aplicación de las tecnologías de la información para la toma y el proceso de datos sobre el entorno de amenaza o en el que se planifica una operación constituye una de las señas de identidad de la denominada *Revolución en los asuntos militares* (Mackrell, 1997; Ortiz, 2000; Latham, 2002). Los Estados financian con generosidad numerosos proyectos de investigación y desarrollo a empresas, universidades e institutos de investigación públicos y privados, participados en mayor o menor medida, como la empresa filial de la CIA, *In-Q-Tel* (Ackerman, 2002).

<http://www.in-q-tel.com>

El control de las tecnologías de la información y la protección del espacio telemático se convertirán en un futuro próximo en los principales caballos de batalla, ya que de ellos dependen la operatividad de los sistemas de seguridad y los ejércitos actuales (Rapetto; Di Nuncio, 2001). Hasta tal punto se prevé que su importancia será decisiva que ha dado lugar al nacimiento de una utopía bélica donde la guerra del futuro se limitará a una lucha incruenta entre sistemas informáticos y de telecomunicaciones destinada a colapsar los ordenadores del enemigo, provocando la neutralización de sus armas, la parálisis de su actividad económica y el caos en la vida cotidiana, hasta conseguir su rendición sin apenas bajas humanas, ni con las desastrosas consecuencias de las guerras actuales. La infoguerra no se dirigirá a la ocupación del país enemigo, sino al dominio o destrucción de sus redes de información y flujos electrónicos, provocando la desaparición progresiva de las guerras de conquista (Echeverría, 1999, pp. 197-198). Perry Smith (1991), analista militar de la CNN en la *Primera Guerra del Golfo* es uno de sus principales teóricos.

La guerra de Irak muestra cuán lejos se está de este horizonte. Pero nadie puede negar que el ciberespacio es un nuevo frente, también con terribles efectos, sobre todo cuando afecta al control y manejo de armas de destrucción, que surge junto a los frentes clásicos de campos, ciudades y economía. La defensa y los combates militares ya se producen en el entorno telemático por el dominio de los códigos secretos, las conexiones, los servidores, los programas y los datos. Esto provoca un aumento espectacular de la importancia de la información, ya que la lucha misma se produce con información por el dominio de información.

El dominio informacional se convierte en un objetivo estratégico clave, más cercano al análisis y uso inteligente de la información que a una mera superioridad tecnológica, aunque ésta sea un elemento necesario. El concepto fue acuñado por el director de la DIA (*Defense Intelligence Agency de la Usaf*) general Minihyan: "no consiste en que mi pila de información sea mayor que la tuya. Es un modo de aumentar nuestras capacidades utilizando la información para tomar decisiones correctas y ponerlas en práctica más rápidamente que el enemigo. Es un modo de alterar la entera percepción que pueda tener el enemigo de la realidad. Es un método para usar toda la información de que disponemos y predecir e influir en lo que sucederá mañana, antes de que el enemigo se haya levantado siquiera de la cama para pensar sobre lo que hará hoy" (citado por Johnson, 1994, en: Guisnel, 1997, p. 179).

En este marco se debe entender la presentación de la infoguerra, con una perspectiva más amplia y menos militarista, como el conjunto de operaciones de obtención, proceso y uso de información desarrolladas en un entorno real o virtual destinadas a que un país, una organización o un individuo logren sus objetivos y consigan una situación de predominio sobre sus posibles competidores (Jones; Kovacich; Luzwick, 2002). Evidentemente, la posesión de un servicio de inteligencia eficaz es indispensable para el logro de ese dominio informacional, tanto para prevenir como para actuar.

de negocio, vinculado con sus objetivos y valores corporativos y su plan estratégico mediante el diseño, la implantación, el mantenimiento y la evaluación de un programa de identificación, conservación, organización, integración, análisis, valoración, protección, compartición y uso eficaz de los recursos de información de que dispone y del capital intelectual de sus miembros, con el apoyo de las tecnologías de la información y las comunicaciones.

La gestión del conocimiento es el resultado de la reunión en un programa de gestión común de los recursos de información y los conocimientos, capacidades y habilidades de los recursos humanos existentes en una organización en un entorno tecnológico. Su nacimiento es resultado de la evolución, por ampliación de su ámbito de acción, de la gestión de los recursos de información, cuya práctica está en su base.

### 3. Recursos de información y capital intelectual

Los recursos de información de una organización están formados por todos los componentes de la escala ascendente que va desde el dato hasta el conocimiento pasando por la información en bruto, los flujos de información, los documentos, la información documental y la información evaluada producidos, reunidos o adquiridos por esa organización (**Davenport; Prusak**, 1998, pp. 1-6); así como las tecnologías y las personas que participan en su elaboración, gestión, almacenamiento, análisis y difusión.

El dato es la unidad de información básica no procesada asociada a un objeto o hecho concreto como por ejemplo el contenido del campo de una base de datos. La información en bruto es la reunión de datos con una forma y una estructura que les dan significado, asociada a un contexto que facilita su interpretación; por ejemplo, el registro de una base de datos. El flujo de información es la transmisión de datos presentados bajo la forma de un mensaje dentro de un proceso de comunicación. El documento es el conjunto de datos elaborados y estructurados como una unidad de significado mediante la codificación de signos escritos, orales, icónicos o audiovisuales fijados en un soporte material para su conservación y transmisión; por ejemplo, una base de datos con información financiera. La información documental es la comunicación de un mensaje documental de carácter exhaustivo, específico, relevante y pertinente a una demanda de información que se presenta en un proceso comunicativo con el fin de generar en el receptor nuevo conocimiento que le permita comprender un hecho, adoptar una decisión y realizar un acto.

Por conocimiento se entiende en este contexto la comprensión de la realidad a partir de la obtención y el

análisis de información orientada a la toma de decisiones y la acción. Conocimiento e información no son sinónimos, porque acumular información no supone tener más conocimiento y procesar información no es lo mismo que aprovechar el conocimiento. En realidad, estamos saciados de información pero hambrientos de conocimiento. La información se encuentra en el origen del conocimiento, que es una creación individual y social a partir de la búsqueda e interpretación de información que, a su vez, es guiada por el conocimiento previo que poseemos.

El capital intelectual de una organización es la reunión de todos los conocimientos que posee. Reúne las competencias, las capacidades y el saber de sus miembros, las estructuras, los procesos y las rutinas creadas por éstos durante su trabajo, que permanecen incluso sin su presencia, y los datos e indicadores de las relaciones que la organización mantiene con su entorno. El capital intelectual es intangible y dinámico. Se construye mediante la interacción de las personas en el seno de una organización durante el ejercicio de sus funciones.

El conocimiento se produce y comunica en una organización mediante un ciclo que comienza y finaliza con la creación de conocimiento tácito por los diferentes individuos que la componen. El conocimiento tácito es de posesión personal, difícil de formalizar y de compartir, sólo accesible a los otros de modo indirecto. Tiene dos dimensiones: una técnica formada por el conjunto del saber y las habilidades obtenido mediante la experiencia y el estudio a partir del procesamiento de información; y otra cognoscitiva, compuesta por valores, ideales y emociones. Este conocimiento se comparte con otros durante la interacción mediante diversos medios: mensajes verbales y no verbales, actos y mensajes documentales que, una vez recibidos, procesados e interiorizados permiten la creación de nuevo conocimiento tácito y el inicio, de nuevo, del proceso descrito generando un ciclo continuo.



Archivo del Centro Nacional de Inteligencia

El éxito del ciclo de producción y comunicación del conocimiento exige dos medidas complementarias: lograr el pleno control de todos los datos y documentos existentes en una organización; y explicitar el conocimiento tácito mediante su transformación en información fijada en un documento, porque no se puede identificar, almacenar, tratar y transmitir lo que previamente no se ha codificado. Únicamente esto hace posible integrar en los mensajes que se emitan como respuestas a demandas de información, datos de todo tipo y origen, estructurados o no en documentos.

#### 4. Sistema integrado de gestión de la información

Conseguir lo descrito exige implantar un sistema integrado de gestión de la información. Es un conjunto de elementos organizados y en interacción dinámica en función de un objetivo y de acuerdo con unos principios y unas normas estables que contribuyen a la obtención de ese fin mediante el establecimiento de relaciones en el marco de un proceso regulado y finalista.

**«El capital intelectual se construye mediante la interacción de las personas en el seno de una organización durante el ejercicio de sus funciones»**

Por consiguiente, consiste en la integración y organización de una serie de elementos (personas, tecnologías de la información y las comunicaciones, normas, procedimientos e instrumentos de tratamiento y recuperación de la información) que permite desarrollar un proceso de comunicación de conocimiento mediante la reunión, selección, autenticación, conservación, transformación (representación y organización de su contenido), evaluación, recuperación y transferencia de datos adecuados a las necesidades y las demandas de sus usuarios. Estos datos (las evidencias de conocimiento), que pueden ser generados por el organismo que mantiene el sistema o captados de fuentes externas, se estructuran y conservan en la más amplia variedad de objetos y soportes y se transmiten bajo la forma de flujos de información o de documentos estables. Un sistema de información es, por tanto, el producto de la reunión de un proceso y los entes físicos que lo soportan y dirigen.

El sistema de información se compone a su vez de 3 subsistemas con sus elementos y procesos peculiares: de captura y creación de datos, de transmisión de datos y de regulación de los flujos de información y el de gestión de la información documental. El primero trabaja con datos brutos, el tercero con datos estructu-



*Biblioteca del Centro Nacional de Inteligencia*

rados en documentos y el segundo con ambas clases de material.

La integración de todos los recursos de información es un requisito imprescindible para el éxito del sistema. Se trata de superar la disgregación de la información en diversos almacenes y unidades de gestión separadas y sin comunicación, ya que se constata que dificulta una conservación, un tratamiento y una recuperación eficientes, obstaculiza la adopción de los avances tecnológicos e impide el suministro y la utilización de toda la información disponible durante las consultas.

El fin es dotar a la organización de un sistema de información que sea capaz de efectuar un control completo de toda la información, formal o informal que captura, conserva, crea o fluye por su seno y que intercambia con su entorno. Por tanto, el horizonte se debe situar en el diseño y puesta en marcha de un plan de gestión que atienda de modo conjunto a todos los aspectos involucrados en el funcionamiento de los 3 subsistemas básicos de información, ya que todos tienen el mismo fin: suministrar información que ayude a la organización a la que pertenecen al diseño y el cumplimiento de sus objetivos. De la unidad de la organización se deduce el principio de que el sistema de información también ha de ser único.

#### 5. Inteligencia para la seguridad y la defensa

El uso de información por parte de los estados para tomar sus decisiones sobre una base firme es una constante histórica. Su aplicación para la protección contra amenazas internas o externas no es una excepción. Precisamente la obtención y el análisis de información para su transformación en conocimiento aplicado para la defensa y el ataque, mediante la diplomacia o el espionaje, nació con las primeras civilizaciones. En la actualidad el conocimiento creado para actuar en este ámbito coincide en sus caracteres, medios de comunicación y aplicación con el descrito anterior-

mente, si bien se denomina desde hace varias décadas inteligencia.

Todavía no existe una definición de inteligencia universalmente aceptada, a pesar de que se han ensayado numerosas (Warner, 2002). Destaca la delimitación de inteligencia realizada por **Thomas F. Troy** (1991-92), a partir de la crítica del trabajo pionero de **Sherman Kent** (1966), como conocimiento del enemigo presidido por el secreto, para cuya creación se nutre de las informaciones obtenidas por agentes de información, por medios técnicos o de fuentes y recursos de información abiertos. La inteligencia no se construye mediante una suma de datos, sino a partir de un determinado modo de analizar éstos sobre hechos. En consecuencia, las claves para su logro se encuentran por igual tanto en la obtención de información como en su proceso de transformación en conocimiento estructurado, preciso y listo para ser utilizado como sostén de una decisión que adopta generalmente la forma documental de un informe, y en su protección.

De acuerdo con esta concepción, el servicio de inteligencia se puede definir como un organismo cuya razón de ser es crear un eficaz sistema de información, aplicando los procedimientos e instrumentos de la gestión del conocimiento con el fin de suministrar al estado conocimiento para la comprensión de su entorno, el ajuste de su estrategia, la adopción de medidas de intervención e influencia en la realidad, el desarrollo de operaciones tanto de información como de desinformación y de contrainteligencia en el terreno de la seguridad y la defensa nacional. A diferencia de la mayoría de los departamentos y oficinas del estado donde la gestión de la información es un mero elemento auxiliar de su acción principal, ésta es la función y el instrumento fundamental de un servicio de inteligencia. Su objetivo es generar información evaluada para los órganos de decisión política que contribuya a despejar el escenario de incertidumbre intra e interestatal donde actúa el estado (Fraguas, 1991).

La diversidad y el carácter no convencional de las nuevas amenazas del siglo XXI a la seguridad nacional: proliferación de armas de destrucción masiva, infoguerra, ciberterrorismo, guerra y terrorismo bacte-

riológico, redes mafiosas de tráfico de armas y narcóticos, etc., frente al tradicional enfrentamiento de ejércitos nacionales con grandes efectivos humanos y materiales que se despliegan sobre el territorio, refuerzan aún más si cabe tanto la necesidad como la importancia de disponer de información y conocimiento de muy diversa procedencia y naturaleza por parte de las fuerzas armadas y los cuerpos y fuerzas de seguridad del estado. La información posee una dimensión estratégica de primera magnitud, bien como medio activo de defensa: conocer para prevenir, o reactivo: conocer para atacar (Kahn, 2001).

**«Un sistema de información es, por tanto, el producto de la reunión de un proceso de comunicación de conocimiento y los entes físicos (personas, normas, tecnologías...) que lo soportan y dirigen»**

Es erróneo identificar la información estratégica producida por los servicios de inteligencia con la inteligencia militar, ya que ésta sólo es una especie de la primera. Según su finalidad, se debe distinguir entre 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 por las fuerzas armadas, a la vigilancia del ejército de un enemigo potencial o real y a la preparación y el desarrollo de operaciones bélicas. Las diferencias no radican ni en las fuentes ni en el modo de trabajo ni en el carácter civil o militar de los miembros de los servicios de inteligencia, sino en el ámbito de actuación y uso de la inteligencia.

La inteligencia para la seguridad y la defensa tampoco se debe confundir con la inteligencia económica y la inteligencia competitiva. Aunque todas tienen un fin proteccionista, y la primera también se ocupa de obtener y evaluar información económica, actúan en sectores diversos. La inteligencia económica se centra en el sector productivo, comercial y en los actores económicos, generalmente de un estado o una región, siendo una evolución de las diferentes prácticas de vigilancia científica, tecnológica, comercial, jurídica, etc., y de protección del patrimonio ensayadas desde mediados del siglo XX (Clerc, 1997). La competitiva se circunscribe aún más al mundo empresarial como una práctica destinada a recoger, seleccionar, archivar, analizar y distribuir información sobre el entorno de una empresa concreta para obtener ventaja sobre su competencia (Tena; Comai, 2001; Pollard, 1999).



Sede del Centro Nacional de Inteligencia en Madrid

Además, la inteligencia para la seguridad y la defensa emplea tecnologías más variadas para la toma de datos, no duda en recurrir a medios de obtención de información como el espionaje y todos sus productos están sometidos a uno de los 3 niveles clásicos de protección: secreto, reservado y cautela o confidencial.

## 6. Ciclo de la inteligencia

La cuestión fundamental es, como ya planteaba **Taplin** (1989), ¿cuándo y mediante qué medio la información se convierte en inteligencia? La respuesta se halla en el denominado “ciclo de la inteligencia” mediante el cual, 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 diferentes subfases, hasta conseguir inteligencia (**Montero**, 1998). Se trata de un proceso donde se debe distinguir entre el objeto (la información), los medios posibles para su obtención y el producto (la inteligencia) que se entrega a la autoridad política o militar decisoria tras evaluar la fiabilidad de los datos, analizarlos, integrarlos e interpretarlos (**Díaz**, 2001).



Sello del CNI

**«La obtención y el análisis de información para su transformación en conocimiento aplicado para la defensa y el ataque, mediante la diplomacia o el espionaje, nació con las primeras civilizaciones»**

El ciclo de inteligencia persigue la generación de conocimiento estratégico útil, verdadero y ajustado a los requerimientos de información preestablecidos por un destinatario final, a quien se difunde selectivamente el resultado plasmado en un documento, mediante un proceso que consta de 6 etapas: planificación; toma de datos; procesamiento; análisis, producción, difusión; comunicación; y evaluación. Sus principios, acciones y resultados son propios de la gestión del conocimiento.

**1. Planificación.** Consiste en determinar las áreas de interés estratégico del organismo para el que actúa el servicio de inteligencia y las necesidades de información concretas requeridas por sus responsables. Es una etapa crucial, ya que la inteligencia es el resultado de un proceso metódico que se origina en las necesidades de información de los usuarios (**Herman**, 2001, p. 286).

Las áreas estratégicas se fijan mediante la identificación y clasificación en niveles de prioridad de los

ámbitos de actuación del servicio y sobre qué se desea información, de modo conjunto por los responsables del servicio de inteligencia y de los órganos políticos y, en su caso, militares a los que sirven. Posteriormente el servicio traduce esas prioridades en necesidades generales de información, clasificadas en diversas áreas analizando los rasgos de los entornos informativos externo e interno de la organización. Atiende, fundamentalmente, al tipo y el contenido de la información que se puede adquirir, la disponibilidad y fiabilidad de las fuentes junto con los cauces de comunicación. Asimismo, se intenta deducir a partir de esas necesidades generales posibles demandas concretas de información con objeto de poder responder en el tiempo más breve posible cuando se produzcan e incluso de anticiparse a su formulación. Se trata de distinguir entre necesidad de información, que existe en los usuarios siempre de carácter general, y demanda de información, de carácter específico y planteada formalmente (**Sanz**, 1994, pp. 23-31).

Esta distinción permite clasificar la inteligencia que se produce al final del ciclo en 3 tipos, según el momento de su utilización:

—Básica: de naturaleza general y de relativa permanencia, obedece a las necesidades generales y estratégicas de la organización y suele almacenarse en bases de datos.

—Actual: adopta la forma de boletines periódicos sobre cuestiones más específicas de interés habitual o de respuesta precisa a demandas sobre hechos concretos, con los datos disponibles o mediante un proceso de búsqueda ad hoc con los recursos de los que se dispone.

—Estimativa (**Ford**, 1993): orientada a determinar, ante una situación concreta y a petición del usuario del servicio, la posible evolución de la situación y las posibilidades de actuación de los elementos involucrados en ella, a partir de los datos de que se dispone.

**2. Toma de datos.** Trata de la adquisición, selección, autenticación y reunión de datos e información en bruto mediante medios tecnológicos, humanos o documentales, cuya tipología y caracteres se exponen más adelante. Los datos que se obtienen son el resultado de una tensión dialéctica entre lo que se desea, lo que se puede conseguir con los medios de que se dispone y el producto de la reflexión sobre los datos que han sido de utilidad tras su proceso y análisis.

**3. Procesamiento.** Es el control y la conservación de los datos recopilados por medios diferentes para su

conversión e integración en conjuntos estructurados de información que puedan adoptar la forma de mensajes documentales tras su recuperación. La ingente cantidad de datos, información en bruto y documentos con los que se trabaja exige recurrir a los más avanzados sistemas electrónicos de gestión de datos, sistemas de apoyo para la toma de decisiones (*decision support systems*)<sup>3</sup> y a técnicas y herramientas como la minería de datos, los sistemas de indización automática, los agentes inteligentes de búsqueda y recuperación, etc., cuya investigación es un área prioritaria para los servicios de inteligencia<sup>4</sup>. La sobreabundancia de información, si no se controla eficazmente, puede originar un colapso del servicio o, cuanto menos, dificultar su necesaria compartición entre los diversos departamentos y con otros servicios de inteligencia del país o de naciones amigas.

**«Los recursos de información sólo tienen un valor potencial, cuya evolución en el tiempo es además imprevisible: depende de quién, cómo, cuándo y para qué lo use»**

La conservación de la información electrónica en óptimas condiciones para su acceso y uso es otra decisiva acción de la etapa de procesamiento. Debe responder fundamentalmente a 3 retos. En primer lugar, es necesaria la creación de depósitos de conservación adecuados y seguros, tanto físico-lógicos (discos compactos, videodiscos digitales, etc.) para los originales y las copias, como contenedores y almacenes de estos depósitos. Por otra parte es imprescindible la adopción de nuevas y urgentes medidas de prevención del deterioro ya que el soporte de lo digital es más vulnerable al paso del tiempo que el papel. Y por último, se debe garantizar a lo largo del tiempo el acceso y la legibilidad de la información contenida en los soportes, haciendo frente a la obsolescencia técnica de los depósitos, del hardware y del software. Estas acciones se deben recoger en un programa de intervención que consta de 3 partes: un plan de preservación con medidas de seguridad física y lógica y de actuación ante desastres, un conjunto de soluciones de conservación preventiva contra agentes de deterioro y virus informáticos y un plan de lucha contra la obsolescencia (Esteban, 2001).

**4. Análisis y producción.** Consiste en extraer con precisión y rapidez información a partir de los depósitos de datos, que induzca a la construcción de conocimiento. Esta fase marca la frontera entre información e inteligencia, que se manifiesta dentro de la estructura de los servicios de inteligencia en la separación entre los órganos responsables de la obtención de infor-



El ciclo de inteligencia para la seguridad y la defensa

mación y los encargados de su elaboración en función de sus áreas de actuación (nacional, internacional, etc.) mediante el trabajo de analistas que aplican todo su capital intelectual. Se realizan 3 operaciones: evaluación de los datos, integración de datos procedentes de diversas fuentes e interpretación.

Mediante la evaluación se trata de discriminar cuáles contribuyen a la satisfacción de los requerimientos de información formulados, en términos de fiabilidad de las fuentes, validez, oportunidad, pertinencia, relevancia y utilidad. La integración de datos de diversas procedencias se basa en un principio fundamental de los servicios de inteligencia: no aceptar nunca una única autoridad informativa (Berkowitz; Goodman, 2000, p. 22). Se trata de conseguir una sinergia donde la combinación de información procedente de los diferentes medios de obtención constituye un todo de mayor relevancia y alcance que cada una de las informaciones por separado (Isaacson; O'Connell, 2002). Su aplicación ha permitido incluso la aparición del concepto de *Multi-Int* (multinteligencia) para denominar el trabajo de los departamentos de análisis (Pappas; Simon, 2002).

Posteriormente, se procede a la interpretación de los datos, donde el resultado se recoge en un producto documental, cuya tipología (dossier, resumen, estadística, etc.) se establece de acuerdo con la mayor o menor elaboración de la información que transmite. En la cumbre se encuentra el informe de inteligencia: un documento elaborado por un experto en el área concreta de análisis, no muy extenso, altamente estructurado, con orientaciones para la interpretación de la información que se recoge, con valoración de los hechos que se analizan y con una calificación del grado de protección que se le debe aplicar.

**5. Comunicación.** Consiste en la distribución y puesta a disposición del documento creado al demandante de información o, por iniciativa propia del analista, al responsable de su departamento o del servicio, de modo seguro. También es conveniente que muchos



tipos de documentos sometidos a los niveles más bajos de protección se difundan también de manera horizontal entre otros analistas y departamentos, con el fin de facilitar la circulación de información elaborada en beneficio del cruce de datos. Esto supone romper con la rígida estructura jerárquica de los servicios de inteligencia, tan criticada en los últimos años por lenta y por inoperativa cuando la carga de trabajo es demasiado elevada, las fuentes muy variadas y el volumen de datos a controlar y analizar muy numeroso.

**6. Evaluación.** La comunicación de informes de inteligencia no supone el final de un proceso iniciado con una petición general o específica de información. Es necesario analizar las reacciones de los usuarios ante la información suministrada (Herman, 2001, pp. 293-296), identificar los objetivos cumplidos con las decisiones adoptadas sobre su base y valorar la importancia que la información ha tenido en el logro de esos objetivos. Sus resultados permiten replantear las conclusiones obtenidas con las acciones seguidas durante la fase de planificación e incluso condicionan los futuros procesos de adquisición de información, marcando los tipos de datos a conseguir y sus modos de obtención. Henry Kissinger, Secretario de Estado de los EUA, decía que desconocía qué productos de la inteligencia necesitaba pero que los reconocía cuando los veía en la mesa de su despacho.

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 el análisis de datos obtenidos por múltiples medios, identificados como necesarios a partir del estudio tanto de las necesidades como demandas de información de los usuarios y la evaluación de los resultados de la aplicación de inteligencia elaborada en momentos anteriores.

Las principales dificultades con que topa el ciclo de inteligencia provienen de la urgencia impuesta por los usuarios para disponer del análisis, aun antes de que se haya conseguido suficiente información, la incapacidad del analista para controlar todas las variables a estudio, el desconocimiento de la calidad de los datos debido a imperfecciones en el proceso de colecta, el énfasis que se debe dar a la predicción y el enfoque utilitario de los resultados (Marrin, 2002).

## 7. Medios de obtención de información

### 7.1. Medios tecnológicos

Se cuenta con numerosos y variados sistemas tecnológicos para la consecución de información:

a. De búsqueda y transmisión de señales electromagnéticas en cualquier onda (tipo de modulación) y frecuencia. Se dividen en dos tipos:

—De interceptación, descriptación y análisis de comunicaciones por ondas radiotelefónicas y radiotelegráficas mediante estaciones receptoras desconocidas por el emisor y la aplicación de tecnología de reconocimiento de voz con el fin de averiguar su identidad.

—De recogida y reconocimiento de información por medios electrónicos como radar, sensores microfónicos y ultrasónicos, aviones espías dotados de sistemas de control y alerta aerotransportado (*Awac*), aviones de detección y seguimiento de objetivos terrestres móviles y fijos (*Jstars*) provistos de videografía y termografía, satélites de reconocimiento electrónico (“hurones”) destinados a captar comunicaciones, vigilancia telemétrica de lanzamiento de misiles, etc.

**«Es necesario hacer un esfuerzo para reducir la brecha entre servicios de inteligencia y gestión del conocimiento, pues la comunicación y la interacción entre los mismos será positivo para el progreso de ambos»**

Cuando estos sistemas se aplican en el ámbito militar, el acopio de datos puede tener una dimensión táctica: localización e identificación de emplazamientos de armas y de efectivos concretos de un ejército enemigo real o potencial; o estratégica: vigilancia continua de la totalidad de un ejército y su despliegue (Richardson, 1987, p. 50).

b. De vigilancia de radiaciones procedentes de equipos o sistemas, tales como motores de ignición, líneas de conducción de energía eléctrica, etc.

c. De obtención y análisis de imágenes de objetivos fijos o móviles mediante aviones, satélites y estaciones avanzadas de procesamiento. La actual precisión y resolución de las imágenes permite localizar efectivos militares, fábricas y emplazamientos de armas, maniobras, etc. Las cámaras del satélite espía *Big Bird* pueden identificar objetos de tan sólo 30 centímetros. La organización y análisis del ingente material fotográfico por los servicios de inteligencia es un área de investigación pujante, de gran interés para otros ámbitos documentales (Bewley, 1999).

d. De interceptación y análisis de comunicaciones electrónicas como programas de rastreo de mensajes electrónicos (por ejemplo, *Carnivore*), ruptura de sistemas de seguridad de servidores de información telemáticos, control de transacciones de comercio electrónico, etc. Su desarrollo es considerado prioritario dentro del programa *Total information awareness (Conocimiento total de la información)* creado por los EUA

el pasado año como medio de lucha antiterrorista (Koch, 2002).

e. De información geoespacial, destinados a proporcionar una representación geográfica ajustada de las zonas involucradas en una acción militar (Payton, 2002)<sup>5</sup>.

## 7.2. Medios humanos

Se entiende que son aquellos donde la presencia y la acción del hombre tienen una función preponderante en la observación y recogida de datos. El espionaje, el contacto con informantes y el interrogatorio son sus principales manifestaciones.

El incuestionable protagonismo de la tecnología de la información para la seguridad y la defensa no debe invitarnos a sobrevalorar y sacralizar su importancia en detrimento de otras fuentes de información. Muchas voces se alzan en pro de una reflexión sobre sus resultados en el marco general de la gestión del conocimiento, para fijar su eficacia y aplicación real frente a otros medios (Ackerman, 2001). La apuesta por una inteligencia de base tecnológica en detrimento de una tradicional centrada en los recursos humanos, con agentes rastreando información y procesando conocimiento sobre el terreno ha destapado, sobre todo a partir de los fallos de seguridad evidenciados tras los atentados del 11 de septiembre de 2001, carencias de disponibilidad y formación de hombres y mujeres capaces de enfrentarse a las amenazas terroristas.

## 7.3. Recursos documentales abiertos

El tercer medio de obtención de información está formado por fuentes de información o recursos documentales abiertos: obras de referencia (enciclopedias, anuarios, quién es quién, directorios, etc.), monografías, publicaciones seriadas, bases de datos, literatura gris, fotografías y cualquier otro documento impreso o electrónico de acceso y uso público en cualquier idioma, con datos políticos, geográficos, económicos, militares, científicos, técnicos, sociológicos, etc. Su uso recibía escasa atención hasta hace poco tiempo pero su análisis mediante el cruce de datos constituye ahora una parte sustancial del trabajo de inteligencia, donde la aplicación del conjunto de conocimientos y habilidades de los documentalistas es necesaria para su búsqueda y selección, así como para la representación y organización de su contenido<sup>6</sup>.

## 8. Auditoría de los recursos de información

El desarrollo del ciclo de producción de inteligencia o conocimiento en una organización exige conocer con detalle la naturaleza, los caracteres, la disponibilidad, el uso y el valor de los recursos de información

con los que se cuenta. Su conocimiento mediante una auditoría debe ser una actividad periódica ya que su tipología, cantidad, rasgos y eficiencia varían con el tiempo por motivos que dependen tanto de la propia evolución del servicio como de la modificación de las áreas de interés de la organización y de los cambios que se producen en el entorno. La auditoría de los recursos de información es una acción inexcusable cuando se produce una reestructuración de las funciones, la estructura o los objetivos estratégicos de la organización, como sucede con el paso del *Cesid* al *CNI*. Es el único medio de saber dónde y cómo se está y cuánto falta para llegar a la meta.

Se han propuesto dos métodos para realizar la auditoría de la información. Uno se centra en la identificación y topografía de entidades y depósitos de información, así como la asignación de valor a éstos, a partir del análisis de su coste económico y del beneficio que origina su uso dentro de los procesos de negocio y la toma de decisiones estratégicas (Burk; Horton, 1988). El segundo se basa en el inventario de documentos, tecnologías y procesos de gestión de la información, con especial incidencia en sus flujos internos, y el descubrimiento de la relación que se establece durante su generación y uso con los valores y las acciones de la organización, con el fin de diseñar una política de información corporativa (Orna, 1990; Henczel, 2001). Ambos procedimientos se han aplicado con un éxito desigual, que ha dejado constancia de la necesidad de su integración, pues pueden ser complementarios. No obstante, todavía no se ha realizado esta deseada unificación, aunque sí se han sentado sus bases (Buchanan; Gibb, 1998).

Para nosotros, el método está determinado por el fin que se persigue. La auditoría de los recursos de información de una organización consiste en el inventario de los diferentes tipos de recursos de que dispone, la localización de sus almacenes y medios de comunicación, la descripción de sus características y estructura, el análisis de su disponibilidad, dinámica y uso, la evaluación de su empleo de acuerdo con el contexto y la valoración de su capacidad para generar conocimiento útil para la organización; con el fin de conseguir una gestión más eficaz que redunde en el logro de los objetivos estratégicos de la corporación. Se lleva a cabo mediante las siguientes actividades:

1. Análisis de la organización, consistente en:

—La determinación de sus fines y objetivos.

—El descubrimiento de su cultura y valores.

—La situación en el entorno mediante un análisis dafo: identificación de las debilidades y las fortalezas

internas de la organización y de las amenazas y oportunidades que surgen del ambiente.

—La descripción de la estructura orgánico-funcional.

—La identificación y descripción de los procesos estratégicos de negocio o de prestación de servicios.

—La fijación de los trámites administrativos.

2. Inventario de los recursos de información existentes en la organización de acuerdo con una tipología que integre datos, flujos de información, documentos, tecnologías, conocimientos tácitos de las personas, etc.

3. Identificación y localización de los recursos en soportes, depósitos y canales de circulación, mediante análisis de las formas de fijación, codificación, conservación, transmisión y recuperación.

4. Descripción de los caracteres y la estructura de los recursos de información.

5. Análisis tanto de la disponibilidad como la dinámica de los recursos, con atención a los modos de obtención y acceso, incluido el cuándo y cómo se usan.

Para la realización de las dos últimas actividades se elabora una hoja técnica por cada recurso, con independencia de su carácter formal o informal, su estado tácito o explícito y su procedencia interna o externa, donde se indica una serie de datos previamente normalizados sobre su naturaleza y uso. Los datos recogen los identificadores formales del recurso, sus rasgos físicos, la descripción de su contenido, quién lo tiene o conserva, dónde se localiza, cuándo se usa, quienes lo emplean, por qué se utiliza, para qué se usa, los derechos, niveles y modos de acceso, cómo fluye por la organización (desde o hacia el exterior), los obstáculos y retardos que impiden o dificultan su distribución y uso, las pérdidas (cuándo, quién y cómo se pierde), los indicadores de uso, las relaciones (de depen-

dencia, de complementariedad, etc.) que mantiene con otros recursos, etc.

Cada ficha técnica se acompaña de un diagrama que presenta el flujo del recurso a través de la organización mostrando de un modo gráfico, mediante una serie de convenciones que facilitan su comprensión, los depósitos, canales de comunicación, válvulas, obstáculos y contenidos concretos que fluyen.

Se utilizan como técnicas de recogida de datos, entre otras, el análisis de las normas y los procedimientos administrativos actuantes, la exploración de la estructura de los ficheros informáticos, la observación directa de los procesos de trabajo, el análisis de los logs de tráfico de la red informática y la realización de cuestionarios, entrevistas y reuniones con el personal de la organización.

El conjunto de todas las fichas y diagramas compone el mapa de la información de una organización.

6. Evaluación del uso de los recursos de información, no mediante una escala universal, sino de acuerdo con los fines, valores, estructura y formas de actuación de cada organización. La evaluación se puede acompañar de una propuesta de medidas de mejora de los rasgos y la dinámica de cada recurso con objeto de aumentar su valor potencial.

7. Valoración de la utilidad de cada recurso y de la totalidad para satisfacer las necesidades y demandas de información, atendiendo a sus costes y a los resultados de las decisiones que adopta, así como las acciones que emprende la organización con el conocimiento obtenido mediante su uso.

El coste de un recurso de información es la suma de los medios materiales invertidos, el tiempo laboral utilizado y el porcentaje de los gastos generales de una organización que le correspondan para la adquisición, organización, conservación y puesta en disposición para su uso y comunicación. En cuanto a la medición de su valor, no existen técnicas normalizadas, debido a su dificultad. Se pueden adoptar tres perspectivas para su cálculo: la de inversión analiza el precio que el usuario estaría dispuesto a pagar por el mismo, la del proceso calcula el impacto que su uso tiene en una actividad, y la de rendimiento observa su utilidad para conseguir objetivos previamente establecidos. Todas las técnicas tienen, al menos, un elemento común: la convicción de que el uso de la información está siempre vinculado a un contexto.

Una fuente de información no tiene, por tanto, un valor inherente, sino que lo adquiere en un contexto determinado y según le asigne el usuario, atendiendo a su capacidad para generar conocimiento útil y aplicable en el ámbito de acción de la organización. Su valor se cal-

**El profesional de la información** está abierto a todos los bibliotecarios, documentalistas y otros profesionales de la información, así como a las empresas y organizaciones del sector para que puedan exponer sus noticias, productos, servicios, experiencias y opiniones.

Dirigir todas las colaboraciones para publicar a:

*El profesional de la información*

Apartado 32.280

08080 Barcelona

Fax: +34-932 701 145

[epi@sarenet.es](mailto:epi@sarenet.es)

cula de acuerdo con las necesidades y los objetivos corporativos y, como éstos son variables, resulta que los recursos de información sólo tienen un valor potencial, cuya evolución en el tiempo es además imprevisible: depende de quién, cómo, cuándo y para qué lo use.

## 9. Conclusión

Es necesario hacer un esfuerzo para reducir la brecha entre servicios de inteligencia y gestión del conocimiento, si consideramos la comunicación y la interacción entre esas áreas un elemento positivo para el progreso de ambas. De este modo los avances en la gestión del conocimiento incidirán directamente en la mejora del funcionamiento de los servicios de inteligencia para la seguridad y la defensa. Asimismo, los continuos progresos en los modos de producción de inteligencia y conocimiento por parte de estos servicios se integrarán en el marco disciplinar de la gestión del conocimiento, favoreciendo su recepción por otros ámbitos, como la empresa, la industria, las finanzas o la administración pública.

Estos adelantos, muchos de los cuales preceden a la aparición del término gestión del conocimiento, son notables en técnicas tales como la captura de datos por medios tecnológicos, el tratamiento y análisis electrónico de cantidades ingentes de datos, la observación y seguimiento de la evolución del entorno, la integración de datos de diversa procedencia y modo de obtención, y la producción de información analizada y evaluada.

## Notas

1. Art. 1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (BOE, 7 de mayo de 2002). La legislación sobre el CNI se completa con la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia (BOE, 7 de mayo de 2002); el Real Decreto 436/2002, de 10 de mayo, por el que se establece la estructura orgánica del Centro Nacional de Inteligencia (BOE, 11 de mayo de 2002); y el Real decreto 593/2002, de 28 de junio, por el que se desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia (BOE, 29 de junio de 2002).
2. La revisión estratégica de la defensa, presentada por el Ministerio de Defensa el año 2002 con el objetivo de fijar las necesidades de España en seguridad y defensa, así como las capacidades y recursos imprescindibles, con una visión de futuro hacia el año 2015, resalta también la importancia que está adquiriendo en el nuevo escenario estratégico la inteligencia militar. Así, apuesta por la potenciación del Centro de Inteligencia de las Fuerzas Armadas (Cifas), que deberá convertirse en el elemento clave del proceso de racionalización y coordinación de este área, presente en todas y cada una de las operaciones militares que se lleven a cabo (Jiménez-Ugarte, 2003).
3. Los servicios de inteligencia cuentan con los DSS más avanzados para el filtrado y la integración de múltiples datos para permitir la toma de decisiones con gran rapidez. Destacan el software de comunicaciones y de gestión de información en campaña del cuerpo de Marines de las Usaf (Kenyon, 2001) y el programa EKP (The brain enterprise knowledge platform) creado por la empresa The Brain Technologies Corporation en colaboración con el Joint Experimentation Directorate (J-9) dependiente del Joint Forces Command (Jfcom) de las Usaf. Estas aplicaciones integran y gestionan múltiples elementos de información de modo conjunto y en tiempo real, simulan hipotéticos escenarios con situaciones del tipo "what if..." y sustituyen la presentación jerárquica de la información por asociaciones de datos basadas en parámetros mentales (Lawlor, 2002). <http://www.thebrain.com>

4. La CIA va a invertir en los próximos años 27 millones de US\$ para el desarrollo de sistemas avanzados de minería de datos y técnicas de análisis automático de información electrónica (Matthews, 2002).
5. Existe un proyecto de realización de un mapa inteligente de toda la superficie terrestre a partir de estándares de digitalización denominado *Mapa vectorial mundial (Vmap)*, liderado por la *National Imagery and Mapping Agency* de EUA y con la participación de diferentes países aliados, que dispondrán de toda la cartografía mundial a cambio de aportar la digitalización cartográfica de su territorio y de algunas de sus zonas de influencia histórica colonial. La *Carta militar digital de España vector-raster*, editada en cd-rom por el Ministerio de Defensa en 2002, es la contribución de nuestro país al proyecto.
6. Existen incluso compañías que se dedican por encargo al análisis de información para la seguridad y la defensa a partir de fuentes abiertas, como la *Open Source Solutions*, dirigida por el ex-agente de la CIA, Robert David Steele (2000). Steele es también miembro fundador de la asociación *Council on Intelligence*, destinada a reflexionar sobre el papel de los recursos de información libres para la generación de inteligencia. <http://www.oss.com>  
<http://www.council-on-intelligence.com>

## Bibliografía

- Ackerman, Robert. "The information technology community may be driving the land warriors of the next conflict". En: *Signal magazine*, 2001, agosto. Consultado en: 20-11-02. <http://www.us.net/signal/Archive/Aug01/electronics-aug.html>
- Ackerman, Robert. "Intelligence technology development accelerates: new directions spur in-house research, industry outreach". En: *Signal magazine*, 2002, junio. Consultado en: 25-11-02. <http://www.us.net/signal/Archive/June02/intelligence-june.html>
- Berkowitz, Bruce D.; Goodman, Allan E. *Best truth: intelligence in the information age*. Yale: Yale University Press, 2000.
- Bewley, Robert. *Archiving aerial photography and remote sensing data: a guide to good practice*. Oxford: Oxbow Books; David Brown Book Company, 1999.
- Burk, C. F.; Horton, F. W. *InfoMap: a complete guide for discovering corporate information resources*. Englewood Cliffs: Prentice-Hall, 1988.
- Buchanan, S.; Gibb, F. "The information audit: an integrated strategic approach". En: *International journal of information management*, 1998, v. 18, n. 1, pp. 29-47.
- Clerc, Phillippe. "Inteligencia económica: retos actuales y perspectivas". En: *Informe mundial sobre la información 1997/98*: Madrid, Unesco; Cindoc, 1997, pp. 322-335.
- Davenport, Thomas H.; Prusak, Laurence. *Working knowledge: how organizations manage what they know*. Boston: Harvard Business School Press, 1998.
- Díaz Fernández, Antonio Manuel. "La función de los servicios de inteligencia". En: Cueto, Carlos; Jordán, Javier (coords.). *Introducción a los estudios de seguridad y defensa*. Albolote (Granada): Comares, 2001, pp. 155-173.
- Echeverría, Javier. *Los señores del aire: Telépolis y el tercer entorno*. Barcelona: Destino, 1999.
- Esteban Navarro, Miguel Ángel. "Los archivos de documentos electrónicos". En: *El profesional de la información*, 2001, diciembre, v. 10, n. 12, pp. 41-45.
- Ford, Harold P. *Estimative intelligence: the purposes and problems of national intelligence estimating*. Lanham (Maryland): University Press of America; Washington: Defense Intelligence College, 1993.
- Fraguas, Rafael. "Servicios secretos y razón de estado". En: *Claves de razón práctica*, 1991, v. 14, pp. 64-68.
- Grier, Peter. "The combination that worked". En: *Air force magazine: journal of the Air Force Association*, 2002, abril, v. 85, n. 4, pp. 30-32.
- Guisnel, Jean. *Cyberwars. Espionage on the internet*. New York: Plenum Trade, 1997 (ed. or. en francés, 1995).

- Henczel, Susan.** *The information audit: a practical guide*. München: K. G. Saur, 2001.
- Herman, Michael.** *Intelligence power in peace and war*. Cambridge: Cambridge University Press, 2001.
- Isaacson, Jeffrey A.; O'Connell, Kevin M.** *Beyond sharing intelligence, we must generate knowledge*. Consultado en: 07-11-02.  
<http://www.rand.org/publications/randreview/issues/rr.08.02/intelligence.html>
- Jiménez-Ugarte, Javier.** "Síntesis y comentarios sobre la revisión estratégica de la defensa". En: *Revista española de la defensa*, 2003, separata, n. 179.
- Johnson, Craig L.** "Information war is not a paper war". En: *Journal of electronic defense*, 1994, agosto.
- Jones, Andy; Kovacich, Gerald L.; Luzwick, Perry G.** *Global information warfare: how businesses, governments, and others achieve objectives and attain competitive advantages*. Boca Raton (Florida): Auerbach, 2002.
- Kahn, David.** "An historical theory of intelligence". En: *Intelligence and national security*, 2001, v. 16, n. 3, pp. 79-92.
- Kent, Sherman.** *Strategic intelligence for American world policy*. Princeton University Press, 1966. Existe edición en castellano (Madrid: Pleamar, 1978).
- Kenyon, Henry S.** "Bent pipes, intelligent agents aid corps: cunning devices, solutions help Marines fight smarter". En: *Signal magazine*, 2001, mayo. Consultado en: 20-11-02.  
<http://www.us.net/signal/Archive/May01/bent-may.html>
- Koch, Andrew.** "US Department of Defense seeks radical information network". En: *Jane's defense weekly*, 2002, v. 38, n. 3, p. 6.
- Latham, Andrew.** "Warfare transformed: a braudelien perspective on the revolution in military affairs". En: *European journal of international relations*, 2002, v. 8, n. 2, pp. 231-266.
- Lawlor, Maryann.** "Information plus context equals knowledge: software tool connects the dots between related pieces of data". En: *Signal magazine*, 2002, marzo. Consultado en: 22-11-02.  
<http://www.us.net/signal/Virtual/March02/information-feb.html>
- Mackrell, Eileen.** "Combined forces support: the evolution in military (intelligence) affairs". En: *Nato review*, 1997, v. 45, n. 6, pp. 20-22. Consultado en: 31-10-02.  
<http://www.nato.int/docu/revue/1997/9706-06.htm>
- Marrin, Stephen.** *CIA's Kent School: a step in the right direction*. Consultado en: 31-10-02.  
<http://www.isanet.org/noarchive/marrin.html>
- Masback, Keith J.** "Transforming army intelligence". En: *Intelligence, surveillance and reconnaissance journal*, 2002, v. 1. Consultado en: 05-10-02.  
<http://www.afji.com/ISR/Mags/2002/Issue1/transforming.html>
- Matthews, William.** *Squeezing out the sparks: CIA to invest millions in developing software to sift through digital data*. Consultado en: 05-11-02.  
<http://www.fcw.com/fcw/articles/2002/0805/tec-cia-08-05-02.asp>
- Montero Gómez, Andrés.** "Valor de inteligencia". En: *Ejército: revista ilustrada de las armas y servicios*, 1998, febrero-marzo, n. 686, pp. 28-36.
- Ortiz, Román.** "Más rápido, más lejos, más letal". En: *Revista española de defensa*, 2000, v. 13, n. 151, pp. 42-49.
- Orna, Elisabeth.** *Practical information policies: how to manage information flows in organisations*. Aldershot: Gower, 1990 (2ª ed. rev. y aum.: 1999).
- Pappas, Aris A.; Simon, James M.** "Daunting challenges, hard decisions: the intelligence community: 2001-2015". En: *Studies in intelligence*, 2002, v. 64, n. 1. Consultado en: 10-11-02.  
<http://www.odci.gov/csi/studies/vol46no1/article05.html>
- Payton, Sue C.** "Maps to information superiority: the rapid terrain visualization advanced concept technology demonstration". En: *Intelligence, surveillance and reconnaissance journal*, 2002, v. 3. Consultado en: 05-10-02.  
<http://www.afji.com/ISR/Mags/2002/Issue3/maps.html>
- Pollard, Andrew.** *Competitor intelligence*. Londres: Financial Times, 1999.
- Rapetto, Humberto; Di Nuncio, Roberto.** *Le nuove guerre: dalla cyberwar ai Black Bloc, dal sabotaggio mediatico a Bin Laden*. Milán: RCS, 2001.
- Richardson, Doug.** *Guía ilustrada de técnicas y equipos de la guerra electrónica*. Barcelona: Orbis, 1987.
- Sanz Casado, Elías.** *Manual de estudios de usuarios*. Madrid: Fundación Germán Sánchez Ruipérez; Pirámide, 1994.
- Smith, Perry.** *How the CNN fought the war*. New York: Birch Lane, 1991.
- Steele, Robert David.** *On intelligence, spies and secrecy in an open world*. Fairfax (Virginia): Afcea International Press, 2000.
- Tena Millán, Joaquín; Comai, Alessandro.** "Los propósitos de la inteligencia en la empresa: competidora, cooperativa, neutral e individual". En: *El profesional de la información*, 2001, mayo, v. 10, n. 5, pp. 4-10.
- Taplin, Winn L.** "Six general principles of intelligence". En: *International journal of intelligence and counterintelligence*, 1989, v. 3, n. 4, pp. 475-491.
- Troy, Thomas F.** "The correct definition of intelligence". En: *International journal of intelligence and counterintelligence*, 1991-1992, v. 5, n. 4, pp. 433-454.
- Virilio, Paul.** *El ciber mundo, la política de lo peor*. Madrid: Cátedra, 1997.
- Warner, Michael.** "Wanted: a definition of intelligence". En: *Studies in intelligence*, 2002, v. 46, n. 3. Consultado en: 13-11-02.  
<http://www.cia.gov/csi/studies/vol46no3/article02.html>
- Miguel Ángel Esteban Navarro**, Departamento de Ciencias de la Documentación, Universidad de Zaragoza.  
[mesteban@unizar.es](mailto:mesteban@unizar.es)
- Diego Navarro Bonilla**, Departamento de Biblioteconomía y Documentación, Universidad Carlos III de Madrid.  
[dnavarro@bib.uc3m.es](mailto:dnavarro@bib.uc3m.es)

## Próximos temas especiales

Septiembre 2003

Noviembre 2003

Enero 2004

Recursos-e sobre ciencias sociales/derecho

Gestión de documentación multimedia

Minería en la web (web mining)

Los interesados pueden remitir notas, artículos, propuestas, publicidad, comentarios, etc., sobre estos temas a:

[epi@sarenet.es](mailto:epi@sarenet.es)