Arbor



# Medios tecnológicos e Inteligencia: bases para una interrelación convergente

*Diego Navarro Bonilla*

Arbor CLXXX, 709 (Enero 2005), 289-313 pp.

*Se propone una reflexión en torno a los fundamentos tecnológicos que hacen posible la generación de inteligencia. Las inversiones en tecnologías de la información aplicadas al ámbito de la seguridad y la defensa crecen cada día y demuestran cómo la explosión de la información requiere de medios y técnicas cada vez más complejas para no quedar saturados por el desbordamiento informativo. La evaluación y el análisis de la información que se convertirá en inteligencia son aspectos clave de todo el proceso. Sin embargo, más allá de la necesaria actualización de los medios tecnológicos para la obtención, procesamiento y presentación de información y conocimiento por parte de los organismos de inteligencia no debe olvidarse que la globalización de las comunicaciones y el acceso a la tecnología punta por grupos terroristas pueden ser considerados una amenaza en caso de uso agresivo. Por otra parte, el desequilibro en el binomio libertad-seguridad proporciona argumentos para una reflexión en torno a las libertades individuales frente a la utilización masiva de tecnología para la captura, obtención y cruzamiento de informaciones mediante sistemas avanzados.*

## 1. Introducción

«When the world changes, the single most important requirement for intelligence is to change with it» (A. A. PAPPAS y J. M. SIMON, «Daunting

Challenges, Hard Decisions: The Intelligence Community: 2001-2015», en *Studies in Intelligence,* vol. 46: nº 1 (2002); www.odci.gov/csi/studies/vol46no1/article05.html).

Iniciemos estas páginas en torno a dos premisas básicas y aparentemente obvias: en el proceso de generación de inteligencia, la tecnología por sí sola no es de utilidad, al menos por ahora y en un plazo insondable. Y dos: Los medios tecnológicos utilizados por una nación para garantizar su prosperidad, seguridad y bienestar económico pueden devenir, como siniestro reverso de la misma imagen, en focos de amenaza al ser utilizados con fines destructivos contra esa misma nación o provocando inestabilidad al ser considerados como objetivos prioritarios de un hipotético ataque asimétrico. El informe elaborado por Melissa Applegate y publicado por el *Strategic Studies Institute* en septiembre de 2001 bajo el título *Preparing for Asymmetry: As seen through the lens of Joint Vision 2020* advertía de las amenazas englobadas bajo el concepto de guerra asimétrica, entendida como el recurso que grupos, potencias y redes terroristas utilizarán como alternativa al desarrollo convencional del conflicto. Por ello, una de las principales amenazas de la a priori benéfica superioridad tecnológica del primer mundo es el sagaz aprovechamiento de la nebulosa cibernética globalizada por parte de los grupos terroristas para valerse del entorno red en varias áreas, actualmente consideradas prioritarias en la investigación y en el análisis de los organismos de información e inteligencia: financiación de grupos mediante transferencias bancarias on-line, comunicación segura entre grupos para fijar los objetivos y asegurar la coordinación, reclutamiento de terroristas a través de avisos en páginas web volátiles, reivindicación inmediata de acciones terroristas, propaganda y contrainformación. El paradigma de guerra-red constituye un concepto raíz en la definición de la principal amenaza mundial actual focalizada en el terrorismo[1]. Javier Calderón resumió estas reflexiones al hablar de «tecnología del terrorismo»: «La globalización ha beneficiado a los grupos terroristas. Las nuevas tecnologías de la información han multiplicado las posibilidades de comunica-

[1] J. JORDÁN, «El terrorismo en la sociedad de la información: el caso de Al Qaida», en *El profesional de la información,* vol. 11: nº 4 (2002), 297-305. J. ARQUILLA y D. RONFELDT, *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político.* Madrid, Alianza, 2003. J. A. ISAACSON y K. M. O´CONNELL, «Beyond Sharing Intelligence, We must generate Knowledge» www.rand.org/publications/randreview/issues/rr.08.02/intelligence.html. 2002. Consultado: 7/09/2002.

ción anónima –cuasi clandestina– de los grupos terroristas. Las facilidades para el intercambio de capitales les han abierto nuevas oportunidades para financiarse. La apertura de fronteras y aduanas para permitir la circulación de personas y mercancías con mayor rapidez y menos restricciones y controles les han dado la posibilidad de rentabilizar al máximo sus cadenas logísticas. Y, por último, les ha facilitado el acceso a informaciones estratégicas que les permiten golpear sobre los puntos más sensibles de las sociedades occidentales»[2].

Resulta evidente que de estas inercias del pasado han sabido aprovecharse grupos paradigmáticos de esta concepción asimétrica como Al-Qaeda. Las redes de información y la tecnología adecuada para su obtención, análisis y transformación en conocimiento y, como consecuencia, en comprensión de los hechos para tomar una decisión, forma parte a juicio de Lee S. Strickland de las principales herramientas de la guerra futura. Es en este nuevo escenario de «no reglas» en el que los servicios de inteligencia desarrollarán sus capacidades operativas contando con el apoyo tecnológico más adelantado como factor imprescindible pero no suficiente[3]. Resulta indispensable, por tanto, replantear el nuevo escenario de conflicto ya que se trata de un concepto que no puede basarse exclusivamente en términos geográficos convencionales sino que el frente de batalla es el espacio red sin fronteras definidas[4].

Es cierto que, como ha indicado recientemente Javier Solana, una de las claves en la lucha antiterrorista se sitúa hoy en día en la prevención por medio del incremento al máximo de las estructuras y actividades de inteligencia[5]. Tras los atentados de 2001 y 2004 el protagonismo de los organismos de inteligencia nacionales o departamentales en todo el mundo ha promovido una corriente de reflexión en torno a su función, futuro, eficacia o necesidad de reforma[6]. Más allá de opiniones y controversias

---

[2] J. CALDERÓN, «Los servicios de inteligencia», en *Terrorismo Internacional en el siglo XXI* (X Curso Internacional de Defensa, Jaca, 16-20 de septiembre de 2002). Madrid, Ministerio de Defensa, 2003, 261.

[3] C. COKER, *Waging War Without Warriors? The changing Culture of Military Conflict*. London, International Institute of Strategic Studies, 2002.

[4] R. L. PFALTZGRAFF y R. H. SHULTZ Jr., «Future actors in Changing Security Environment», en Robert L. Pfaltzgraff Jr., y Richard H. Shultz Jr., (eds.), *War in the Information Age: New Challenges for U.S. Security Policy*. Washington; London, Brassey´s, 1997, 19.

[5] J. SOLANA, «Una guerra inteligente contra el terrorismo», en *El País*, 11 de noviembre de 2004.

[6] J. THIES, «El renacimiento de los servicios secretos», en *Política Exterior*, 101 (Sept.-Oct. 2004), 47-58.

para todos los gustos, se encuentran datos objetivos que ilustran el interés por el futuro inmediato de los servicios de inteligencia al amparo del balance de lo ocurrido. El modelo de inteligencia basado en un ciclo secuencial de actividades fue heredado de la Guerra Fría y, si bien estructuralmente define qué hace un servicio de inteligencia y para quién, funcionalmente choca con una realidad que debe basarse en una estructura cooperativa y coordinada más próxima al concepto red que al concepto ciclo o secuencia lineal[7]. Las recientes reformas en la actuación de los servicios de inteligencia tienen, por tanto, numerosas dimensiones a nuestro juicio englobadas en las siguientes ideas fuerza: normativa basada en leyes eficaces de funcionamiento y consolidación del marco jurídico de actuación de los servicios, una extraordinaria reflexión sobre la imbricación de los organismos de inteligencia en la Sociedad del Conocimiento Globalizado, la continua preocupación por dotar a dichos centros de una cultura organizativa ágil y eficaz así como por un decidido esfuerzo por favorecer una integración y coordinación internacional en materia de inteligencia, aun cuando los resultados de esta ansiada coordinación sean, cuando menos, perfectibles. Junto a ello no debe olvidarse que, como resultado y proceso, el trabajo de inteligencia requiere unos mecanismos de control, evaluación y valoración de la eficacia y la eficiencia[8].

La detención de la cúpula de ETA en Francia a principios de octubre de 2004 así como la localización y desmantelamiento de una de sus principales bases en el Bearn ha vuelto a poner de manifiesto aspectos clave en la lucha antiterrorista como la coordinación de fuerzas y cuerpos de seguridad, la decidida intervención de la fiscalía o la participación conjunta de servicios de información de agencias y servicios policiales europeos. Sin embargo, un aspecto de capital importancia de cualquier operativo es la minuciosa preparación, utilización de medios y recursos tecnológicos y el concurso de numerosos elementos que, sabiamente combinados y orientados hacia un objetivo común permiten alcanzar el éxito de una operación. A menudo, de los éxitos policiales sólo se conoce su resultado final y, por razones obvias, se tiende a no dar demasiados detalles de sus preparati-

---

[7] R. CLARK, *Intelligence Analysis: a Target-Centric Approach*, Washington, CQPress, 2004, 13-27: «The Intelligence Process».

[8] M. Á. ESTEBÁN y D. NAVARRO, «Inteligencia para la seguridad y la defensa: el valor de la gestión del conocimiento», en Diego Navarro y Miguel Ángel Esteban (coords.), *Gestión del conocimiento y servicios de inteligencia.* Madrid, BOE; Universidad Carlos III de Madrid; Instituto Español de Estudios Estratégicos, 2004, 35-54.

vos. Los prolegómenos de una operación pueden abarcar años e, invariablemente, la eficaz combinación entre medios tecnológicos y gestión de información para generar nuevo conocimiento juegan un papel prioritario en el éxito o el fracaso de las actuaciones de las fuerzas y cuerpos de seguridad del estado en el ámbito de la prevención por medio de la información. Paralelamente, la incautación de documentación generada por la actividad logística de un comando terrorista en forma de discos duros, memorias ópticas, libros contables, correspondencia, memoranda, publicaciones, etc., origina un nuevo enlace, una nueva vía de investigación. Todas esas pruebas y evidencias documentales procedentes de la administración interna del comando tienen la virtualidad de generar un nuevo conocimiento que procesado, evaluado y combinado con todo el conocimiento previamente acumulado permite pensar en lograr el tal vez inalcanzable objetivo final de la seguridad total.

Desde otro punto de vista, las revisiones estratégicas internacionales proporcionan un marco global sobre las amenazas, las capacidades y la función encomendada a unas Fuerzas Armadas. Estos valiosos documentos que sintetizan la visión política y la reflexión militar no han dudado en incluir la importancia de la información como ámbito indiscutible de la defensa y la seguridad. A nuestro juicio, son dos las áreas de actuación en las que el dominio de la información despliega todo su potencial para las políticas de defensa: Tecnologías capaces de gestionar e integrar la información para desarrollar una comunicación efectiva y afianzamiento de los procesos de obtención, análisis y difusión del conocimiento generado en el seno de los servicios generales o departamentales de inteligencia vinculados a la defensa y seguridad del Estado a través del reforzamiento de iniciativas como la del futuro Centro de Inteligencia de las Fuerzas Armadas (BOE, 26 abril 2005). Este hecho insoslayable que vincula información, tecnología y amenaza se pone de manifiesto tanto en los textos de ámbito europeo (Estrategia Europea de Seguridad) como en los nacionales (Directiva de Defensa Nacional Española). El primero de ellos apuesta claramente por el empleo de medios diplomáticos, policiales, legales y de inteligencia en la identificación y neutralización de riesgos y amenazas. En cuanto a la Directiva Española se propone la unificación de los servicios de inteligencia militar bajo dependencia funcional del Centro Nacional de Inteligencia. Sin embargo, cuando se habla de unificación, coordinación, traspaso de información entre cuerpos, agencias y servicios no debe olvidarse la dimensión tecnológica subyacente en todo ese deseo. Los numerosos intentos por unificar bases de datos entre servicios de información dentro de los cuerpos y fuerzas de seguridad del Estado se unen a las propuestas europeas

conducentes a reforzar la integración e interconectividad de datos en las bases de EUROPOL o a los decididos esfuerzos de coordinación expresados por el coordinador europeo de la lucha contra el terrorismo, el holandés Gijs de Vries. La identificación por parte del Ministerio del Interior del terrorismo internacional como prioridad evidente se ve acompañada de una reflexión en torno a las estructuras, actuación y grado de colaboración y coordinación entre los servicios de información de la Guardia Civil y la Comisaría General de Información de la Dirección General de Policía. Pero la medida más visible de este plan ha consistido también en la creación en mayo de 2004 del Centro Nacional de Coordinación Antiterrorista, sin capacidad operativa, que tratará de paliar la descoordinación entre centros y organismos de producción de inteligencia. El nuevo centro tiene competencias funcionales en materia de inteligencia, centralización de recursos de información tales como las bases de datos y actuará también como un centro de evaluación y análisis de riesgos y amenazas. La principal novedad consiste en que por primera vez en veinte años el servicio de inteligencia español se incorpora a un organismo permanente y estable de coordinación en la lucha antiterrorista junto a Policía Nacional y Guardia Civil. Sin embargo la inteligencia militar queda al margen de este nuevo organismo desde el mismo instante en que no fueron incluidos orgánicamente en el Comité Ejecutivo del Mando Unificado.

Las características de la contemporánea sociedad de la información extienden su influencia por todos los sectores y naturalmente el de la seguridad y la defensa nacional es uno de los más afectados, llegando a imponer su dinámica y obligando a repensar el futuro del conflicto, teniendo no sólo a la información sino a las tecnologías y métodos para su obtención, control y organización como futuro caballo de batalla. La investigación en sistemas de información y comunicación basados en el entorno web, la seguridad en las comunicaciones, la biotecnología, nanotecnología, robótica y la biometría son actualmente áreas prioritarias en la gestión de información de todo tipo para generar conocimiento estratégico y táctico. De ahí que la realidad impuesta por los nuevos escenarios de seguridad y defensa basados en la importancia de la información y la adquisición de la denominada «ventaja de conocimiento» configure y determine el necesario acoplamiento de los servicios de inteligencia a esta realidad[9]. Una ventaja que no debe basarse en la cantidad de información

[9] M. HERMAN, *Intelligence services in the information age: theory and practice.* Ilford Essex, Frank Cass, 2001; –, «Counter-Terrorism, Information Technology and Intelligence Change», en *Intelligence and National Security*, vol. 18: nº 4 (2004), 40-58.

disponible, más que suficiente sin duda, sino en el grado de satisfacción diario mostrado por los destinatarios de todo el esfuerzo de inteligencia una vez que el vértice de todo el proceso de inteligencia debe trasladarse de la fase de obtención hacia el análisis, la discriminación y la evaluación de la información para elaborar inteligencia. Se trata, en definitiva de mantener el éxito en la dialéctica entre sobreabundancia de información y pertinencia garantizando siempre el concepto de actualidad informativa con objeto de no caer en la denominada «OBE (Overtaken by events)» o desfase de la información. Sabemos que información hay demasiada, quizá en exceso. El elemento clave es sin duda el análisis y el gran valor de los analistas de inteligencia como «factor humano» radica en que sus capacidades intelectuales combinadas con el auxilio de las tecnologías de la información ponen el acento sobre el estudio, la interrogación y la extracción de conclusiones a la luz de la información obtenida[10].

La tan citada Revolución en los Asuntos Militares (en adelante RAM) ha consagrado el valor del sector de la información en el desarrollo del conflicto futuro asumiendo el cambio de paradigma en la forma de conducir la guerra hacia otro: «The revolution in military affairs generally refers to the quantum leap in communications and data processing technology and the accompanying global changes in the way we share, process and use information»[11]. Como paradigma o modelo conducente a la explotación satisfactoria de la alta tecnología en el ámbito militar, la RAM constituye de hecho la piedra de toque en la naturaleza del conflicto futuro, denominado de Cuarta Generación, que apuesta por la minimización de riesgos humanos en favor de una profunda y costosísima inversión económica en investigación y desarrollo tecnológico así como por el uso de pequeñas unidades de acción, con una menor necesidad de apoyo logístico masivo y una combinación integrada con centros de inteligencia en tiempo real[12]. En términos generales, RAM constituye el aban-

[10] P. W. LANG, *Intelligence: The Human factor*, Philadelphia, Chelsea House, 2004.

[11] E. MACKRELL, «Combined forces support: The evolution in military (intelligence) affairs», *Nato Review*, vol. 45: nº 6 (1997), 20-22: www.nato.int/docu/revue/1997/9706-06.html. A. LATHAM, «Warfare Transformed: A Braudelian Perspective on the "Revolution in Military affaire"», en *European Journal of Internacional Relations*, vol. 8: nº 2 (2002), 231-266.

[12] G. WILCOX, «La respuesta militar a la Guerra de la Cuarta Generación en Afganistán», en *Military Review* (septiembre-octubre 2003), 34-47. M. O´HANLON, *Technological Change and the Future of Warfare*, Washington D.C., Brooking Institution Press, 2000.

dono de un modelo de guerra total por otro en el que las operaciones bélicas de una envergadura más reducida, en conjunción con la aplicación tecnológica de precisión y el libramiento de una guerra en el ciberespacio tienden más a asfixiar la capacidad de respuesta de un enemigo que a conseguir su destrucción en términos absolutos. La adaptación de un enemigo infinitamente menor en capacidad y tecnología militar ha motivado que la debilidad militar convencional de un enemigo difuso se vea compensada por el reforzamiento de aquellos medios y formas de ataque a los que estos grupos tienen acceso, haciendo del entorno de la información para evitar dichos ataques el principal campo de batalla previo a operaciones militares sobre el terreno. De hecho, las comunicaciones vía satélite, el entorno web y los mapas de información disponibles para todos los niveles de la cadena de mando, proporcionando flujos horizontales y verticales de comunicación, son el resultado de las inversiones en I+D+I en tecnologías de la información para el campo de batalla[13]. El gran reto es poner a disposición de la unidad mínima de combate la información necesaria, actualizada y en tiempo real de todas las características de los objetivos militares. Sin embargo, presentar la guerra «lo más aceptable posible» ante la sociedad ha llevado, según Manuel Castells, a los países democráticos avanzados a establecer tres conclusiones inmediatas: a) el desarrollo de los conflictos bélicos sobre el terreno no debe implicar a los ciudadanos comunes sino que deben ser librados por ejércitos profesionales; b) el término guerra debe ser sinónimo de corta duración e incluso «instantaneidad», con el fin de que las consecuencias del conflicto no se extiendan; c) finalmente, ha de ser «limpia y esterilizada»[14]. De hecho, asistimos en ocasiones a una forma de combate a distancia, apoyada en medios tecnológicos supuestamente «quirúrgicos» y de un coste económico desorbitante.

En este sentido, no puede olvidarse todo un conjunto de reflexiones, algunas inquietantes en torno a los límites y las consecuencias legales o morales de la masiva utilización de las tecnologías y las redes de in-

---

[13] R. ACKERMAN, «Technology Empowers Information Operations in Afganistán», *Signal* (marzo 2002), http://www.us.net/signal/Archive/March02/Archive-march02.html. Consultado: 10/8/2002; –, «Intelligence Technology Development Accelerates: New directions spur in-house research, industry outreach», en *Signal* (junio 2002); http://www.us.net/signal/Archive/June02/intelligence-june.html. Consultado: 7/08/2002.

[14] M. CASTELLS, *La era de la información. Vol. 1: La sociedad red*, 2ª ed. Madrid, Alianza, 2000, 532-539.

formación en aras de una absoluta preeminencia de la seguridad y la defensa frente a las libertades civiles. Una consecuencia que subyace en todo este asunto es clara y de doble naturaleza: se produce una reducción de la intimidad y derecho a la privacidad frente a las necesidades impuestas por un mundo, al parecer, en perpetuo peligro de sufrir conflictos de información. Incluso la promulgación de una ley controvertida como la *Patriot Act* parece haber formalizado desde el punto legal un recorte en los derechos individuales en beneficio de la seguridad nacional, algo genéricamente aceptado por la sociedad norteamericana. Una noticia inquietante aparecida en el diario *El País* (28/05/03) hablaba de que las agencias de información de Estados Unidos disponen de datos de 31 millones de colombianos de una población total de casi 40 millones para controlar y vigilar la entrada en el país de supuestos terroristas y narcotraficantes. Parece ser que las agencias compraron dichos datos a Choice Point, dedicada a la compraventa de bases de datos mundiales que luego son revendidas a la administración norteamericana. La pregunta inmediata es doble: ¿cómo consiguieron los datos de casi toda la población de un país? ¿Han sido utilizados estos datos de carácter personal por las agencias de inteligencia? De hecho estas prácticas y la controversia causada por la aplicación de la *Patriot Act* han levantado la veda para que se pueda interferir en la vida privada en los secretos de correspondencia electrónica, en la libertad de información, o la investigación de agencias como el FBI en los registros de uso y préstamo de materiales bibliográficos en las bibliotecas norteamericanas. Recientes trabajos como el de Nacho García Mostazo reproducen el temor existente por la superprotección de los medios empleados para la seguridad nacional[15]. Entre ellos se encuentran el espionaje de las comunicaciones, en detrimento de las libertades individuales. Echelon, Promis, Carnivore o el *Terrorist Information and Prevention System* (TIPS en sus siglas inglesas que incluye una legión de informantes y ciudadanos anónimos que recogen datos en el transcurso de su actividad cotidiana) constituyen formas de acceder al conocimiento a base de la interceptación de la comunicación humana o mediante el informe, la denuncia o la puesta en conocimiento de la autoridad competente conductas, sospechas o indicios de posibles actitudes o hechos susceptibles de ser considerados sospechosos para la seguridad, esencialmente nor-

[15] I. GARCÍA MOSTAZO, *Libertad vigilada: el espionaje de las comunicaciones.* Barcelona [etc.], Ediciones B, 2003. D. NATAF, *La guerre informatique.* París, Presses de la Renaissance, 2003.

teamericana[16]. A todo ello habría que sumar la normativa jurídica que protege la intimidad personal y especialmente el contenido de las comunicaciones, como por ejemplo el documento de la UE sobre vigilancia de las comunicaciones electrónicas en el lugar de trabajo (mayo de 2002) o el castigo impuesto desde el Código Penal a quien vulnere la intimidad de otro apoderándose de cartas, papeles, mensajes o e-mails. Redes, bases de datos, archivos y, lo que es más letal, el cruzamiento de todos ellos amenazan con restringir la libertad individual y el derecho a la intimidad de las personas al generarse en aras de la denominada seguridad nacional instrumentos y herramientas de información que almacenan millones de datos sobre actividades cotidianas[17]. Algo tan habitual como el registro de un pasajero que accede a un aeropuerto norteamericano quedará perfectamente controlado e identificado gracias a proyectos como la megabase de datos Matrix, capaz de cruzar a una altísima velocidad billones de elementos de información sobre los habitantes de un país. Autores como Lee Strickland defienden por contra precisamente la necesidad de incrementar los controles, la calidad y el entrecruzamiento de los datos almacenados en miles de bases de datos que almacenan este tipo de actividades diarias en beneficio de la seguridad y la defensa nacional[18]. El endurecimiento de las condiciones de acceso a Estados Unidos por parte de ciudadanos de países como los centroamericanos está en el origen de aplicaciones de control de información y datos personales como el CAPPS o Sistema de control preventivo asistido por ordenador, donde existe un auténtico cruzamiento de datos con objeto de etiquetar y clasificar a cada individuo en función de su capacidad de constituir una amenaza seria, potencial o nula. Di-

[16] R. SOHR, *Claves para entender las guerras.* Barcelona, Mondadori, 2003, 169: «TIPS, en todo caso, no tiene nada de gracioso. Es un asunto de lo más serio y que podría cambiar la vida de los estadounidenses. La red de informantes que es reclutada por el Ministerio de Justicia constará de carteros, bomberos, chóferes de buses, ambulancias, taxistas, electricistas, repartidores de comida rápida y de todos aquellos que puedan informar a la autoridad de situaciones sospechosas». D. CAMPBELL, *Surveillance électronique planétaire,* París, Allia, 2001, 11-14 : La polémique Echelon.

[17] R. ALBERCH FUGUERAS y J. R. CRUZ MUNDET, *¡Archívese!: los documentos del poder, el poder de los documentos.* Madrid, Alianza, 1999.

[18] L. STRICKLAND, «Information and the War Against Terrorism, Part V: The Business Implications», en *Bulletin of the American Society for Information Science and Technology*, vol. 28: nº 1 (August/September 2002), 18-21; –, «Fighting Terrorism with Information», en *The Information Management Journal*, vol. 36: nº 4 (July/August 2002), 27-34.

chas prácticas se aproximan al establecimiento de un Estado de «vigilancia perpetua» según expresión de Ignacio Ramonet.

## 2. Evolución tecnológica

No obstante, consideramos acertado repensar el sustantivo de revolución y especialmente aludir a la raíz histórica aplicada al enfrentamiento bélico. De hecho, la RAM puede considerarse como una etapa más en un proceso histórico de larga duración. Al igual que la revolución de la información no es estrictamente nueva, pues a juicio de Peter Burke[19] todas las civilizaciones y sociedades lo han sido de la información, la revolución militar ha conocido importantes jalones históricos oportunamente estudiados por el historiador Geoffrey Parker[20]. Para Michael J. Vickers ha habido no menos de ocho revoluciones militares desde el siglo XV[21]. Seis de ellas en los últimos doscientos años y comprenden desde el impulso a la logística de guerra aportada por el ferrocarril y la máquina de vapor hasta la generalización del rifle de repetición, el telégrafo y las comunicaciones militares hasta la más cercana del submarino y el portaviones como plataformas combinadas de ataque balístico en un caso y aeronaval en el otro.

Será precisamente la historia de las formas de comunicación un concepto íntimamente ligado a los soportes de almacenamiento y registro de información y a la evolución en el tiempo de las técnicas de envío, transmisión y recepción como instrumentos conducentes al avance de una sociedad[22]. El ciclo comunicativo basado en el emisor, el receptor, medio, mensaje y canal se vio pronto amenazado por los empeños de penetrar en el mensaje con fines económicos, políticos o militares desde la más temprana Antigüedad. El desarrollo de las técnicas criptográficas

---

[19] P. BURKE, *A Social History of Knowledge.* Cambridge, Polity Press; Blackwell, 2000. Cito la edición española: *Historia social del conocimiento: de Gutenberg a Diderot.* Barcelona; Buenos Aires; México, Paidós, 153-192.

[20] G. PARKER, *La revolución militar: Las innovaciones militares y el apogeo de Occidente 1500-1800*, Barcelona, Crítica, 1990.

[21] M. J. VICKERS, «The Revolution in Military Affairs and Military Capabilities», en Robert L. Pfaltzgraff Jr., y Richard H. Shultz Jr., (eds.), *War in the Information Age: New Challenges for U.S. Security Policy.* Washington; London, Brassey´s, 1997, 29-46.

[22] L. MUMFORD, *Técnica y civilización.* Madrid, Alianza, 1994, p. 261: «La cultura del hombre depende para su transmisión en el tiempo del registro o archivo permanente; el edificio, el monumento, la palabra escrita».

(protección del significado) y esteganográficas (protección del mensaje) hunden sus raíces en la necesidad de comunicar sin ser interceptado. En el siglo XIX la evolución tecnológica dará paso a una gran variedad de sistemas de comunicación no basados únicamente en la escritura, posibilitando la variedad comunicativa pero también los riesgos de interceptación. Como ha estudiado John Keegan la utilidad de la inteligencia había estado limitada por la difusión de la voz humana, el corto alcance de la vista y la velocidad en la entrega del mensaje[23]. En los albores de la inteligencia «sin hilos» deben situarse las estaciones de señales para comunicar el Almirantazgo en Londres y el puerto de Deal en 1796. A través de estos «semáforos» cualquier mensaje podía ser enviado y recibido entre ambas localizaciones en menos de dos minutos. La red se extendería en 1806 a Plymouth. Pero también durante las guerras napoleónicas las torres de «semáforos» hicieron posible el envío de mensajes de forma rápida y con un alcance muy superior. Tan sólo era necesario hacerse con el libro de códigos de tales semáforos para descifrar el mensaje. Hacia 1840 el invento de Morse permitía traducir los puntos y rayas en mensajes completos emitidos y recibidos en tiempo real dejando obsoletos otros medios anteriores. La clasificación de la inteligencia atendiendo a su procedencia o método de obtención empleado permite identificar tres tipos de fuentes de información utilizadas para la generación de otros tantos tipos de inteligencia: humana, tecnológica y de información abierta. En todas ellas, el elemento tecnológico ocupa un papel prioritario tanto en la obtención, en el control o en la transmisión.

La base tecnológica de la inteligencia de señales (SIGINT) se sitúa en los sistemas de transmisión y recogida de información utilizando señales electromagnéticas en cualquier onda y frecuencia. La inteligencia militar de señales puede dividirse a su vez en táctica y estratégica. La primera persigue localizar e identificar emplazamientos de armas y efectivos militares concretos de un ejército enemigo real o potencial. Pueden emplearse medios electrónicos pero también humanos como los exploradores avanzados encargados de reconocer y fijar objetivos para la aviación. La inteligencia de señales estratégica abarca un espectro mayor, dirigiéndose a la vigilancia continua de la totalidad de un ejército y su despliegue. Sin salir de esta clasificación, la interceptación de comunicaciones ver-

[23] J. KEEGAN, *Intelligence in War: Knowledge of the enemy from Napoleon to Al-Qaeda.* N. York, Alfred A. Knopf, 2003, 99-100.

bales efectuadas desde teléfonos móviles, mediante la colocación de escuchas o el barrido sistemático del espectro comunicativo desde plataformas aéreas SIGINT y ELINT (*Electronic Intelligence*) está en la base del trabajo de inteligencia.

A pesar de lo escurridiza que puede resultar la actuación de unidades paramilitares, o la flexible estructura celular de grupos terroristas, la inevitable necesidad de comunicación (verbal, escrita o gestual) entre sus miembros es precisamente lo que hace exponer al emisor a la captación del mensaje por parte de un receptor no deseado constituyendo siempre el terreno de las comunicaciones, y especialmente su uso indiscriminado sin tener en cuenta los mínimos requerimientos de seguridad, su talón de Aquiles y la puerta de acceso a la información que los servicios de inteligencia manejan para contrarrestar la superioridad asimétrica de estos grupos. La localización definitiva que permitió la captura del narco Pablo Escobar se produjo gracias a la interceptación de una comunicación por un teléfono móvil. Pero también la caída del lugarteniente de Al-Qaeda Ramzi Bin al Shibh en septiembre de 2002 fue posible merced al tupido dispositivo de escuchas montado por la CIA en Pakistán y el continuo barrido efectuado por aviones AWAC (*Airborne Warning and Control System*). La detección de las llamadas efectuadas por Ramzi desde un teléfono por satélite precipitó su captura en una sangrienta y espectacular acción y, junto a él, diez miembros de la red terrorista. Sin embargo esta misma dependencia y actuación previsible de los sistemas de interceptación hizo posible, paradójicamente, la huida del propio Bin Laden de las montañas de Tora Bora a finales de 2001. Según el testimonio aportado por su guardaespaldas personal, el marroquí Abdalá Tabarak, detenido e interrogado en Guantánamo, fue el propio líder de Al Qaeda quien entregó su teléfono móvil a Tabarak, quien lo dejó abierto para que pudiese ser interceptado. Mientras tanto, Bin Laden y un grupo reducido de sus hombres escapaban en dirección contraria (*Washington Post,* 21 de enero de 2003).

Esta búsqueda de señales acústicas y electromagnéticas se puede dividir a su vez en la denominada inteligencia de Comunicaciones (COMINT) consistente en la interceptación, análisis y descriptación de comunicaciones por ondas radiotelefónicas y radiotelegráficas. Requiere el establecimiento de estaciones receptoras, desconocidas para el emisor, para descodificar el mensaje emitido. En este apartado se incluiría el desarrollo de sistemas reconocimiento de voz dentro de las denominadas industrias de la lengua con el fin de averiguar la identidad de los emisores en el transcurso de sus conversaciones Finalmente, la inteligencia

electrónica (ELINT) se ocupa de controlar la información obtenida mediante señales de radar. En ella se incluye la industria de sensores microfónicos, ultrasónicos, de infrarrojos y dispositivos de reconocimiento[24]. El papel jugado por los denominados «Aviones espía» en el desarrollo de un conflicto proporcionan argumento para alimentar la guerra electrónica[25]. El barrido del espacio aéreo por medio de aviones dotados de sistemas de control y alerta aerotransportado (AWAC) así como los aviones de detección y seguimiento de objetivos terrestres móviles y fijos (JSTARS) conforman buena parte de la acción encaminada a obtener y controlar información desde el aire.

La dimensión espacial de la guerra de la información hace tiempo que está consolidada por medio del lanzamiento y mantenimiento de satélites de vigilancia. Queda atrás la carrera armamentística del espacio que enfrentó en la Guerra Fría a Estados Unidos y la Unión Soviética por alcanzar el primer puesto en el desarrollo espacial. Hoy en día, los satélites de vigilancia y reconocimiento constituyen piezas esenciales de los servicios de inteligencia nacionales. Agencias nacionales y departamentos de defensa de todos los países tienen su división de vigilancia espacial dedicada al mantenimiento y gestión de la información proporcionada por los satélites para fines de gestión de crisis y vigilancia de amenazas y riesgos[26]. Los satélites de reconocimiento electrónico «hurones» captan numerosas comunicaciones, vigilancia telemétrica de lanzamiento de misiles, etc. En la actualidad constituyen instrumentos indispensables en el desarrollo de la guerra tecnológica moderna[27]. El poderío militar estadounidense en el campo de la inteligencia aeroespacial, como en todos los demás, es incontestable. Los *USAF Space Almanac* proporcionan interesantes datos acerca de los principales sistemas de satélite para la defensa, así como aquellos otros de carácter civil pero usados también para propósitos

[24] M. de ARCANGELIS, *Historia del espionaje electrónico: de la Primera Guerra Mundial a las incursiones americanas contra Libia.* Madrid, San Martín, 1988.

[25] N PULMAR, *Spyplane: The U-2 History declassified.* Osceola (WI), MBI, 2001.

[26] F. DAVARA, «La observación espacial en la gestión de crisis», en Diego Navarro y Miguel Ángel Esteban (coords.), *Gestión del conocimiento y servicios de inteligencia.* Madrid, BOE; Universidad Carlos III de Madrid; Instituto Español de Estudios Estratégicos, 2004, 207-218.

[27] G. W. GOODMAN jr.., «Space-Based Surveillance: Reconnaissance Satellites are a National Security Sine Qua Non», en *Intelligence, Surveillance and Recognition Journal,* 3 (2002): http://www.afji.com/ISR/Mags/2002/Issue1/transforming.html. Consultado: 9/08/2002.

militares[28]. Por su parte, la actividad continua de los satélites de vigilancia y reconocimiento implica la captura de grandes cantidades de información visual de zonas geográficas muy extensas. La precisión y la resolución de las imágenes permiten disponer de información de gran valor para localizar efectivos militares, emplazamientos de misiles, maniobras, etc. Las cámaras del mayor satélite espía «Big bird» puede llegar a identificar objetos de tan sólo 30 cm. Los resultados fotográficos se envían a estaciones avanzadas de procesamiento de imágenes[29].

La información geográfica digital constituye una herramienta básica para la defensa de un país, puesto que todos los sistemas de mando y control de las Fuerzas Armadas utilizan esta información para proporcionar una representación geográfica ajustada de las zonas involucradas en una acción militar a los cuadros de mando involucrados[30]. En Estados Unidos es necesario destacar la función de la *National Imagery and Mapping Agency* cuya página mantiene un enlace a la inteligencia geoespacial (http://www.nima.mil/). Agencia que, a partir del 24 de noviembre de 2003 se ha convertido en la *National Geospatial-Intelligence Agency* tras unir los esfuerzos de la CIA, DIA y NSA. Por otra parte, el objetivo de los diferentes grupos de trabajo de información geográfica digital es conseguir mapas inteligentes de toda la superficie terrestre a partir de estándares normalizados de digitalización. Estos recursos de información cartográfica van a jugar un papel fundamental en la planificación de operaciones conjuntas por parte de los Estados Mayores y también constituyen una fuente imprescindible para la inteligencia estratégica. En España, la Carta Militar digital de España[31] es la contribución de nuestro país al mapa vectorial mundial (VMAP) con el que todos los países participantes en el proyecto, podrán disponer de la cartografía mundial tras haber contribuido al VMAP con su propia aportación individual con-

[28] Una completa descripción técnica de cada uno de ellos en «USAF Space Almanac», *Air Force Magazine: Journal of the Air Force Association*, vol. 82: nº 8 (Agosto 1999), 42-44.

[29] Recomiendo la lectura del número especial dedicado a Sistemas de Información Geoespacial publicado por la revista *Signal*, vol. 55: nº 7 (marzo de 2001): http://www.us.net/signal/Archive/Mar01/Archive-march01.html.

[30] S. C. PAYTON, «Maps to Information Superiority: The Rapid Terrain Visualization Advanced Concept Technology Demonstration», en *Intelligence, Surveillance and Reconnaissance Journal*, 3 (2002): http://www.afji.com/ISR/Mags/2002/Issue3/maps.html. Consultado: 5/08/2002.

[31] *Carta militar digital de España vector-raster*. Madrid, Ministerio de Defensa, 2000 (1 cd rom).

sistente en la digitalización cartográfica de su nación así como de alguna zona de influencia histórica colonial[32].

En otro orden de cosas, la información geográfica procedente de imágenes captadas por satélites comerciales es un recurso que debe tenerse en cuenta y que rompe con el monopolio militar de la explotación de imágenes de satélite. Existen empresas especializadas en la comercialización de imágenes geográficas obtenidas por satélite (*commercial imagery*) con las que se configuran mapas y planos de extensas zonas de interés como apoyo informativo geográfico al resto de informaciones que serán sometidas al análisis para la generación de inteligencia[33]. La utilización de estos recursos fotográficos ha sido resaltada recientemente como apoyo a la inteligencia desplegada en Afganistán[34]. En este sentido, conviene subrayar la opinión experta de Peregrín Pascual para quien: «la diferencia entre los satélites de observación militar y los comerciales se está disolviendo. La calidad y la resolución de estos últimos son tales que los productos comerciales representan un serio peligro para la protección de ciertos secretos nacionales, pues proporcionan fotos de gran detalle que pueden ser compradas por cualquiera, aunque no precisamente baratas»[35].

La información gráfica de objetivos fijos o móviles constituye uno de los pilares básicos de la inteligencia de imágenes (IMINT O PHOTINT). Imágenes fotográficas digitales obtenidas por aviones o por satélites militares y civiles son el núcleo básico de información incluido en este apartado. Sin embargo, la gran revolución tecnológica en la inteligencia de imágenes procede de los vehículos aéreos no tripulados. Hablar hoy de inteligencia de imágenes resulta imposible sin referirse a los conceptos de ISR (*Intelligence, Surveillance and Reconnaissance*) y UAV (*Unmanned Air Vehicle*)[36]. El *Quadrennial Defense Review Report* (30 de septiembre de 2001), publicado

---

[32] Para más información sobre este proyecto con participación española: D. MANRIQUE, «Inteligencia geoespacial», en *Revista Española de Defensa*, vol. 13: nº 148 (2000), 36-37.

[33] Entre otras: www.orincon.com, www.digitalglobe.com, http://www.autometric.com/index.cfm, http://www.cartographic.com/, http://www.imagesatintl.conm.

[34] R. K. ACKERMAN, «Commercial Imagery Aids Afganistán Operations: orbital eye spies serve multiple roles», en *Signal*, (diciembre 2001): http://www.us.net/signal/Archive/Dec01/commercialdec.html. Consultado: 1/08/2002.

[35] P. PASCUAL CHORRO, *Soldados, marinos y aviadores: Los guerreros del tercer milenio* en *Defensa: Revista Internacional de ejércitos, armamento y tecnología*, 65 (2003), 62 (Número especial).

[36] Recomiendo la lectura de la publicación on-line: www.uvonline.com donde se analiza periódicamente la utilización y características de los aparatos no tripulados y las ope-

por el Departamento de Defensa de los Estados Unidos destacaba ya la necesidad de contar con operaciones coordinadas de ISR con el fin de proporcionar a los mandos militares la información visual en tiempo real que ayudados por equipos de ayuda y soporte a la decisión (DSS) permitan una estrategia coherente y fácilmente adaptable al surgimiento de situaciones que requieren rapidez de actuación. En suma, los ataques lanzados desde plataformas UAV en Afganistán reproducen este esquema con alto grado de eficacia y que la plana mayor del gabinete Bush consideró aumentar por los excelentes resultados en materia de IMINT estaba proporcionando su explotación directa por la CIA[37]. El siguiente paso en la revolución tecnológica aplicada a la inteligencia de imágenes es el equipamiento de los aparatos no tripulados con sistemas de armas convirtiendo el UAV en UCAV (*Unmanned combat air vehicle*) con capacidad para convertirse en plataformas individuales de obtención y clasificación de la imagen obtenida mediante la incorporación de software específico de identificación, interpretación y valoración de la amenaza en tiempo real, sin necesidad de esperar a la intervención de un equipo en tierra[38]. Prueba de la importancia concedida a los aparatos no tripulados de vigilancia fue el impulso que el anterior gobierno del Partido Popular quiso dar a estos aviones en el seno de la Revisión Estratégica de la Defensa favoreciendo el programa de creación de un prototipo europeo de UAV, el denominado «Eagle 1» desarrollado por EADS-CASA, rival de los americanos Predator y Global Hawk. La misión, encomendada al Ministerio de Ciencia y Tecnología, contaba con un presupuesto inicial de 50 millones de euros. El informe final elaborado conjuntamente por el Estado Mayor de la Defensa, el Centro Nacional de Inteligencia y la Guardia Civil fue definitivo para impulsar este proyecto, siendo la protección aérea de Canarias, Ceuta y Melilla el principal cometido de los futuros aviones no tripulados. Por otra parte, impulsado por el Instituto Nacional de Técnica Aeroespacial (INTA) el SIVA (Sistema de vigilancia aérea) fue presentado formalmente en la feria aeroespacial de Le Bourget (París, junio de 2003). Y como resultado del interés por una «rápida capacidad de alcance global», surge el más revolucionario proyecto que tiene como protagonistas a los UAV. Se trata del plan de diseño y cons-

raciones en las que se utilizan. G. W. jr. GOODMAN, «Space-Based Surveillance: Reconnaissance Satellites are a National Security Sine Qua Non», en *Intelligence, Surveillance and Recognition Journal*, 3 (2002): http://www.afji.com/ISR/Mags/2002/Issue1/transforming.html. Consultado: 9/08/2002.

[37] B. WOODWARD, *Bush en guerra*, Barcelona, Península, 2002, p. 245.

[38] R. J. NEWMAN, «*War from Afar*», en *Air Force Magazine*, agosto 2003, 58-61.

trucción de un avión UAV hipersónico por parte de la agencia DARPA, denominado HCV (*Hypersonic Cruise Vehicle*) capaz de atacar objetivos en cualquier parte del globo, según se indicaba en la prensa mundial a comienzos de julio de 2003. Sin embargo, no sólo el espacio aéreo es el ámbito de acción de los aparatos no tripulados, sino que también se ha consolidado la producción de los UUV (*unmanned underwater vehicle*) o aparatos no tripulados de vigilancia y observación submarina. También los avances en materia de robótica han sido utilizados con cierto éxito en las campañas militares de Afganistán al utilizar pequeños aparatos dirigidos por control remoto como el robot «Hermes» para inspeccionar las cuevas de las inmediaciones de Tora Bora[39].

Por todo ello, uno de los principales apoyos tecnológicos puestos a disposición de la inteligencia militar de imágenes actual se basa en la operatividad de los ya citados aviones no pilotados como los RQ-1A Predator (*General Atomics Aeronautical Systems*) RQ-4 Global Hawk (*Northrop Grumman*) o los ultramodernos modelos diseñados para el reconocimiento y el ataque aire-tierra (UCAV) X-45 (Boeing-Agencia DARPA) y X-47B (*Northrop Grumman-Agencia Darpa*)[40]. Su capacidad para capturar imágenes en tiempo real y poderlas transmitir vía satélite a un centro de mando operativo e incluso su posible equipamiento con misiles aire-tierra (Hellfire) accionados por control remoto hacen de estos aparatos auténticas *Imint Data Collection Platforms* y aportan una nueva dimensión a la inteligencia de imágenes en tiempo real[41]. Sin embargo, las acciones aéreas de vigilancia y obtención de imágenes llevadas a cabo por aviones tripulados ponen de manifiesto en muchas ocasiones el alto riesgo corrido por estas plataformas aéreas de obtención de información gráfica llegando incluso a ser abatidas por la defensa antiaérea del país vigilado[42]. Uno de los casos más recientes lo ha protagonizado la caída, por causas aún desconocidas, de un aparato U-2 norteamericano al sur de la capital surcoreana (27 de enero de 2003).

---

[39] J. C. AMBROJO, «La infantería norteamericana recluta robots para rastreo y asistencia médica», *Ciberpaís*, 3 de abril 2003, 6.

[40] Con respecto a la capacidad de bombardero del X-45, originalmente diseñado como un modelo UAV: J. A. TIRPAK, «Heavyweight contender», en *Air Force Magazine: Journal of the Air Force Association*, vol. 85 : nº 7 (Julio 2002), 32-38.

[41] Las características técnicas de estos aviones de ISR (Intelligence, Surveillance and Reconnaissance) en «2002 USAF Almanac», publicado en *Air Force Magazine: Journal of the Air Force Association*, vol. 85 : nº 5 (Mayo 2002), 139-141.

[42] L. TART, y R. KEEFE, *The price of Vigilance: Attacks on American Surveillance Flights*. N. York, Ballantine Books, 2001.

Por último, la aplicación tecnológica a la obtención de información tienen en la inteligencia de radiaciones (RADINT o MASINT, *Measurement and signature intelligence*) una de las formas menos conocidas dentro de la Inteligencia militar. Consiste en la adquisición de información por medio de la vigilancia a través de sensores de radiaciones procedentes de equipos o sistemas que no tienen en sí mismas información, tales como ignición de motores, líneas de conducción de energía eléctrica, etc. Según John W. Ives: «MASINT includes the advanced processing and exploitation of data derived from imagery intelligence (IMINT) and signals intelligence (SIGINT) collection sources. MASINT sensors include, but are not limited to, radar, optical, infrared, acoustic, nuclear, radiation detection, spectroradiometric and seismic systems as well as gas, liquid and solid sampling systems»[43].

## 3. Guerra en la Red

Dentro de este amplio paraguas que define el futuro de la guerra se incluyen los conceptos clave de «Information Warfare, Information Assurance, Information Operations, Information Superiority...»[44]. Es probablemente la definición de Guerra de Información la que mejor explique esta vinculación entre información, tecnología y conflicto, esencial para entender el subsiguiente análisis de los servicios de inteligencia: «IW is a coherent and synchronized blending of physical and virtual actions to have countries, organizations, and individuals perform, or not perform, actions so that your goals and objectives are attained and maintained, while simultaneously preventing competitors from doing the same to you»[45]. Por su parte, Peregrín Pascual la define, desde un punto de vista distinto al de la propaganda y las operaciones psicológicas como el con-

[43] J. W. IVES, *Army Vision 2010: Integrating Measurement and Signature Intelligence*. Pennsylvania, U.S. Army War College, 2002.

[44] A. JONES; G. L. KOVACICH y P. G. LUZWICK, *Global Information Warfare: How businesses, Governments, and Others achieve Objectives and Attain Competitive Advantages*. Boca Raton (Florida), Auerbach, 2002.

[45] Ibidem. W. SCHWARTAU, *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, 1994; –, «An introduction to Information Warfare», en Robert L. Pfaltzgraff Jr., y Richard H. Shultz Jr., (eds.), *War in the Information Age: New Challenges for U.S. Security Policy*, Washington; London, Brassey´s, 1997, 47-60. J. TRAMULLAS, «Concepto y fuentes para el estudio de la «Information Warfare»», en *Anales de Documentación*, vol. 1 (1998), 185-192.

junto de «acciones ofensivas y defensivas para aprovechar y proteger los sistemas de información propios, y destruir o neutralizar los del enemigo, entendiendo como sistemas de información los materiales y las redes capaces de recopilar, procesar y diseminar datos»[46].

Para estos autores, en lo que constituye una completa y actualizada puesta al día de los componentes informativos y tecnológicos de la guerra del siglo XXI, las áreas que engloba IW abarcan desde la gestión de Redes a las operaciones de información o las aplicaciones de I + D. Sin embargo, queremos destacar la integración dentro de la IW de dos áreas fundamentales para articular nuestro análisis. Jones, Kovacich y Luzwick, en un esquema clarificador de las «IW Areas» no dudan en considerar los procesos y elementos integrantes que definen la Inteligencia y la Gestión del Conocimiento como ámbitos profundamente vinculados a la IW. Dentro de la Inteligencia, los autores incluyen los conceptos de: Alerta estratégica, Recursos abiertos, SIGINT y HUMINT. Dentro de la Gestión del Conocimiento su esquema incluye los desarrollos de Minería de datos, Gestión de documentos e información compartida. Dicho de otra manera: el concepto de IW es el marco global en el que se incluyen no sólo «todos los medios capaces de neutralizar el empleo de redes de ordenadores de un enemigo» sino también todas las operaciones relacionadas con la obtención, procesamiento y uso de la información, desarrolladas en un entorno real o virtual para alcanzar un objetivo de ventaja predominante sobre un posible competidor económico, político y militar. Dentro del sector de la defensa nacional, la conjunción entre inteligencia, gestión del conocimiento y guerra de información, proporciona, en suma, un nuevo entorno altamente poderoso. Las consecuencias de la revolución del sector información en la seguridad de los estados se percibe intensamente en una serie de amenazas para cuya detección y supresión se desarrollan métodos de alerta, vigilancia y seguridad de información: Detección criminal cibernética, Seguridad Informática, Ataques físicos o electrónicos a los sistemas de información, Ciberterrorismo, Guerra de información desarrollada por estados o grupos políticos-religiosos limitados por no disponer de una fuerza militar convencional y desinformación[47].

---

[46] P. PASCUAL CHORRO, «Soldados, marinos y aviadores: Los guerreros del tercer milenio», en *Defensa: Revista Internacional de ejércitos, armamento y tecnología*, 65 (2003), p. 11. (Número especial).

[47] T. KÖPPEL y M. NORGARTE, «The security Dimension of the Information Revolution», en *The future of the Information Revolution in Europe: Proceedings of an International Conference*, Sta. Monica; Arlington; Pittsburgh, 2001, 45-54: http://www.rand.org/publications/CF/CF2172/.

De hecho, la tecnología aplicada a la búsqueda y estrangulamiento de las comunicaciones, las fuentes de financiación y la infraestructura de los grupos terroristas, así como los programas de I+D conducentes a la explotación de las fuentes de información en sus más variados formatos y tipologías figuran entre las vías de mayor proyección futura para llevar a cabo la controvertida doctrina de «autodefensa preventiva» antes de recurrir en una segunda fase al empleo de la fuerza militar según el programa creado por el Departamento de Defensa Norteamericano y su titular Donald Rumsfeld. Proyectos desarrollados en el seno de agencias estatales cuyo objetivo es la investigación para la explotación de las tecnologías de la información tienen en DARPA (darpa.mil) (*Defense Advanced Research Projects Agency*) y los programas vinculados (*Information Awareness Office Programs; Information Processing Technology Programs; Information Exploitation Office Programs*) las mejores muestras de lo que estamos exponiendo. La agencia de proyectos de investigación avanzada para la defensa es probablemente el mejor exponente de organismo íntegramente destinado a la investigación para la seguridad y la defensa de los Estados Unidos. Una parte fundamental de sus objetivos está orientada a la búsqueda y experimentación de nuevos programas y tecnologías con las que desarrollar una explotación eficaz de la información. Su objetivo es la generación de nuevas herramientas tecnológicas, software y hardware, con objeto de generar un entorno de investigación orientada a la tecnología de la información para la seguridad nacional. En el seno de la agencia DARPA se han desarrollado numerosas iniciativas que conforman un conjunto de programas específicos para la explotación de la tecnología de la información. El control de las comunicaciones electrónicas, el vaciado y gestión de millones de datos a partir de la minería de datos o la traducción automática de informaciones transmitidas en lenguas minoritarias, la bio vigilancia o la aplicación de las herramientas englobadas en las denominadas industrias de la lengua son algunas de las áreas de interés prioritario.

Paralelamente, otros programas como el *Wargaming the Asymmetric Environment* (WAE) desarrollan técnicas de predicción para incrementar significativamente la anticipación de actos terroristas mediante indicadores obtenidos del análisis de la conducta de terroristas individuales a través de datos procedentes de su contexto político, cultural e ideológico. Este programa, en unión con el Departamento de Defensa y la Comunidad de Inteligencia norteamericana, ha creado indicadores y modelos de predicción de próximas acciones terroristas basados en la simulación de conducta y mentalidad.

A mediados de noviembre de 2002 saltaba a la prensa la creación de la denominada *Total Information Awareness* (traducida en español como «Conocimiento total de la información») que pretendía ser una solución de carácter «absoluto, global y determinante» para rastrear, localizar y controlar billones de comunicaciones electrónicas diarias, transacciones comerciales y en definitiva, cualquier rastro de información intercambiada que permita aportar datos fiables para la lucha antiterrorista[48]. Su configuración se basó en el desarrollo de tres áreas: a) Arquitectura de enormes bases de datos de contra-terrorismo, con elementos de información unidos a bases de datos sobre población; b)Utilización de nuevos algoritmos para extraer, combinar, cruzar y refinar la información proporcionada por diferentes repositorios de información para crear nuevas bases de datos; c) Nuevos modelos, herramientas y métodos que modifiquen el análisis y el «cruce de información» de las bases de datos para crear inteligencia operativa.

Finalmente, uno de los más recientes proyectos impulsados por la administración Bush en esta segunda legislatura recién estrenada ha sido la denominada *Global Information Grid.* Los empeños por alcanzar soluciones «globales, de alcance planetario» en la vigilancia, control y conocimiento de lo que ocurre en los principales focos de tensión están en el origen de iniciativas como esta «rejilla de información global»[49]. Su objetivo se dirige a obtener una red de fusión entre operaciones militares e inteligencia de tal manera que una vastísima red de inteligencia de imágenes a través de satélites, aviones no tripulados (UAV), etc., permitan obtener desde cualquier ordenador en tierra una visión global del campo de batalla en tiempo real. Esta Rejilla de información global ofrece un conocimiento exhaustivo en tiempo real para satisfacer los requerimientos tanto del Departamento de Defensa como de la Comunidad de Inteligencia norteamericana sobre cualquier asunto de interés acerca de la seguridad nacional. A través de iniciativas como ésta, posibles gracias a las astronómicas cifras destinadas a investigación en sistemas de información se pretende alcanzar la tan ansiada superioridad de información, concepto ligado a la ya mencionada revolución en los asuntos militares. La Agencia de Sistemas de Información de la Defensa (disa.mil), la Agencia para el desarrollo de Proyectos Avanzados de la Defensa (darpa.mil) así como la pléyade de empresas externas vinculadas a cualquiera de las

[48] A. KOCH, «US Department of Defense seeks radical information network», en *Jane´s Defence Weekly*, vol. 38: nº 3 (2002), 6.

[49] I. RAMONET, «Vigilancia Total», en *Le Monde Diplomatique*, vol. VII: nº 94 (2003), 1.

agencias de la comunidad de inteligencia (p.ej: In-Q-tel.com) desarrollan los principales proyectos para garantizar esa superioridad.

## 4. El reto de las fuentes abiertas

> «Otro ejemplo más de cómo el exceso de ruido informativo impide hacerse cargo de lo que pasa». D. INNENARITY, *La sociedad invisible*, Madrid, Espasa-Calpé, 2004, 68.

Sin duda, uno de los grandes retos de los servicios de inteligencia a comienzos del siglo XXI es la sobreabundancia de información y la necesidad de operar en entornos corporativos de redes que de forma coordinada permitan disponer de grandes bancos de datos al servicio de un organismo de inteligencia o un conjunto de ellos. La red interna de la comunidad de inteligencia norteamericana *intelink* es un ejemplo evidente de recurso compartido de conocimiento (http://www.topsecretnet.com/intelink/) reservado al uso exclusivo de las agencias y organismos de inteligencia del sistema de seguridad nacional. Los modelos de arquitectura de inteligencia de una comunidad nacional requieren unas especificaciones de normalización de sus recursos de información compartidos basadas en la interoperabilidad y la interconectividad. Paso previo fundamental es «la necesaria homogeneidad de los sistemas de información, normalizados y conectados entre sí para su explotación eficaz según protocolos de intercambio, descripción y almacenamiento compartido. Es decir, que un sistema de información de una organización de inteligencia pueda interactuar con el sistema de otro servicio perfectamente»[50].

Sobre la capital importancia de las fuentes abiertas comienza a haber una importante literatura científica[51]. La producción de documentos fácilmente obtenible por medios abiertos amenaza, por sus dimensiones cuantitativas, con colapsar cualquier intento razonable de control y explotación eficaz. De ahí que proyectos conducentes a la generación tam-

---

[50] D. NAVARRO BONILLA, «Introducción», en *Estudios sobre inteligencia: fundamentos para la seguridad internacional*, Madrid, Instituto Español de Estudios Estratégicos; Centro Nacional de Inteligencia, 2004, 13-40; (Cuadernos de Estrategia; 127). T. MARTIN, *«Top Secret Internet: How U.S. Intelligence Built Intelink»*. Prentice Hall, 1999.

[51] R. D. STEELE, *On intelligence, spies and secrecy in an open world*. Fairfax, Virginia, AFCEA International Press, 2000; –, *The New Craft of Intelligence: Personal, Public and Political*. OSS International Press, 2002. S. GIBSON, «Open Source Intelligence: An Intelligence Lifeline», en *Rusi Journal*, (febrero 2004).

bién automática de síntesis y resúmenes de grandes volúmenes de datos traten de automatizar funciones reservadas tradicionalmente a las habilidades humanas de síntesis e indización. Discriminar, valorar, evaluar y analizar la información son el fundamento de productos de valor añadido elaborados en las últimas fases del ciclo de inteligencia. Y no sólo nos referimos a las dimensiones informativas de la red Internet puesto que la gestión de fuentes abiertas de información incluye muchas otras tipologías documentales, no solamente las electrónicas[52]. En un reciente trabajo, Jesús Tramullas ha identificado un inventario de las principales aplicaciones tecnológicas en la gestión, explotación y transformación de información en conocimiento desde la perspectiva de las ciencias de la documentación[53]. Herramientas utilizadas en la gestión del conocimiento tales como programas para trabajo en grupo, gestión de contenidos, recuperación de la información, portales e intranets se unen a las específicas de visualización de la información en representaciones sintéticas capaces de aunar en un único mapa conceptual el resultado del trabajo de inteligencia. Sin embargo, queremos destacar las denominadas herramientas para la recuperación de información y minería de datos entendida como «el conjunto de técnicas y herramientas orientadas a descubrir patrones y reglas ocultos en grandes volúmenes de datos»[54]. La gestión de recursos tecnológicos tanto de hardware como de software, el diseño de sistemas de gestión de bases de datos, la descripción normalizada de documentos en formato electrónico, el mantenimiento de sistemas de alerta informativa, la gestión diaria de la información transmitida por los medios de comunicación o el desarrollo de sistemas de gestión y conservación de documentos generados en el transcurso de las actividades de un organismo de inteligencia son sólo unos pocos ejemplos de las áreas en las que las tecnologías de la información despliegan todo su sentido. La destreza en la interrogación de bases de datos especializadas requiere la formación de expertos en recursos de información abiertos,

---

[52] D. NAVARRO, «Fuentes abiertas de información e Inteligencia estratégica», en Diego Navarro y Miguel Ángel Esteban (coords.), *Gestión del conocimiento y servicios de inteligencia.* Madrid, BOE; Universidad Carlos III de Madrid; Instituto Español de Estudios Estratégicos, 2004, 55-74.

[53] J. TRAMULLAS, «Tecnologías para la gestión del conocimiento y la generación de inteligencia», en Diego Navarro y Miguel Ángel Esteban (coords.), *Gestión del conocimiento y servicios de inteligencia.* Madrid, BOE; Universidad Carlos III de Madrid; Instituto Español de Estudios Estratégicos, 2004, 75-100.

[54] M DEROSA, *Data Mining and Data Analysis for Counterterrorism.*Washington, Center for Strategic & Intelligence studies, 2004.

capaces de identificar requerimientos de información y proporcionar respuestas adecuadas a esas necesidades. Para tratar de controlar con cierta eficacia toda la producción informativa generada simplemente en una semana y puesta a disposición de la comunidad de usuarios en forma abierta, los servicios de inteligencia se plantean soluciones externas basadas en la creación y mantenimiento de las denominadas reservas de inteligencia[55]. Es decir, en el empleo de grupos de expertos en áreas muy especializadas que actualizan sus conocimientos sobre las fuentes relativas a su especialidad de forma permanente y eficaz. Expertos humanos, en suma y para concluir, que refuerzan la idea que planteábamos al inicio de estas líneas: «la tecnología por sí sola no produce inteligencia».

[55] F. GALVACHE VALERO, «La inteligencia compartida», en Diego Navarro (coord.), *Estudios sobre inteligencia: fundamentos para la seguridad internacional.* Madrid, Instituto Español de Estudios Estratégicos; Centro Nacional de Inteligencia, 2004, p. 161: «El asesoramiento externo y las reservas de inteligencia».

ciencia
pensamiento
y cultura

Arbor

*De próxima publicación:*

SISTEMA NACIONAL DE SALUD
¿PATRIMONIO ÚNICO?
Alfonso Flórez Díaz (Editor)

La Revista Arbor está incluída en el apartado de Arte y Humanides del CITATION INDEX