

# El imperativo de los macrodatos

## Inteligencia de la Fuerza Aérea para la edad de la información

CORONEL SHANE HAMILTON, FUERRA AÉREA DE EE. UU.

TENIENTE CORONEL MICHAEL KREUZER, FUERRA AÉREA DE EE. UU., PHD\*



Los “macrodatos” son el tema actual de muchos debates en los medios de comunicación y el gobierno. Unos los han descrito como un “botón sencillo” cuando se combinan con inteligencia artificial para reducir la función humana del análisis, otros como una amenaza potencial del orden democrático, y otros más como mucha exageración con pocos resultados realmente trascendentales.<sup>1</sup> ¿Qué son los macrodatos y por qué son tan vitales para el futuro de la comunidad de inteligencia (IC por sus siglas en inglés) y las operaciones militares combinadas?

En este artículo, indicamos que la revolución de la información ha cambiado radicalmente la inteligencia aumentando considerablemente el número y la variedad de recopiladores de inteligencia y creando una red global de análisis y máquinas para facilitar un reparto de datos e información, y aumentando el apetito de los operadores para efectuar evaluaciones más rápidas y pertinentes desde el

---

\*A los autores les gustaría dar las gracias a los que proporcionaron detalles e hicieron revisiones clave de este artículo, incluidos Kenneth Bray, el Dr. Jon Kimmisau, el Teniente Coronel Shawn Smagh y el Mayor Shaun Lee.

punto de vista de las operaciones acerca de amenazas y oportunidades de selección de objetivos. Además, ha cambiado la forma del entorno de las amenazas al crear nuevos centros de poder y recopilación en el ciberdominio, donde los adversarios pueden reclutar a miembros, planificar ataques y explotar ataques ordenados e inspirados mediante colectivos en línea. Nuestro entorno actual de potencial humano y limitación de recursos, combinado con estos factores, necesita nuevas estrategias para planificar y ejecutar operaciones de inteligencia, vigilancia y reconocimiento (ISR), e inversión para organizar, entrenar y equipar a analistas de la fuerza aérea con las herramientas para tener éxito en el entorno de información moderno. Los macrodatos, conceptualmente, son la base de este entorno e impulsarán nuestro entendimiento sobre cómo recopilar, estructurar y analizar datos, información e inteligencia en el futuro.

## Cómo reducir la exageración—¿Qué son los macrodatos?

Como su nombre implica, los *macrodatos* consisten al final en reunir, almacenar y procesar volúmenes muy grandes de datos e información. Los analistas de inteligencia apuntarán rápidamente que no hay nada nuevo sobre la recopilación y el almacenamiento de grandes volúmenes de información, ya que ha sido la finalidad central de entidades de inteligencia durante siglos. Los analistas no militares revisan normalmente grandes volúmenes de datos para hacer evaluaciones cuantitativas de conjuntos de problemas complejos basados en miles de observaciones de casos para múltiples variables. Así pues, ¿qué hace que los macrodatos sean nuevos y diferentes? La frase apareció por primera vez a principios de los años 2000, cuando el analista de la industria Doug Laney definió los macrodatos como algo diferenciado de los modelos anteriores en tres factores principales denominados las “tres V”<sup>2</sup>:

- **Volumen**—La Edad de la Información permite la adquisición y el almacenamiento de datos e información que pueden preservarse y accederse y analizarse de forma regular a escalas nunca vistas. La mayoría de las bases de datos anteriores para análisis podría estar contenida en una sola base de datos (como una base de datos Microsoft Excel) con líneas que van desde decenas hasta decenas de miles de líneas. Los macrodatos permiten recopilar de millones a miles de millones de datos.
- **Velocidad**—El volumen de datos e información se adquiere a una velocidad sin precedentes y debe tratarse inmediatamente. Twitter,<sup>®</sup> por ejemplo, recibió 500 millones de actualizaciones (tuits) por día en 2013;<sup>3</sup> donde cada tuit constituye un solo punto de datos de información.
- **Variedad**—Los datos y la información vienen en numerosos formatos de diversas fuentes. En el pasado, el analista o la entidad que requiere la información podría dar forma a lo que se recopiló y cómo se almacenó, pero la combinación de volumen y velocidad necesita hoy formar sistemas para gestionar e incorporar datos en la forma en que se adquirió; desde una imagen hasta una entrada de Twitter<sup>®</sup> o Facebook<sup>®</sup> pasando por una transcripción de una conversación o un discurso.

A medida que aumenta la percepción de los macrodatos, muchos académicos de hoy han añadido a estas tres V otras dimensiones como variabilidad y complejidad. En la USAF, ente otras instituciones, añadimos una cuarta “V” a esta lista:

- **Veracidad**: El volumen, la velocidad y la variedad de datos accesibles por medio de los macrodatos incluyen una gran cantidad de ruido y datos irrelevantes para el conjunto de problemas. Esto crea anomalías potenciales en análisis de datos y abre la puerta a un sesgo analítico en la selección de qué datos son importantes y cómo analizarlos. Las estrategias de los macrodatos deben incluir procesos para mantener los datos “limpios” y la percepción analítica de los peligros de trabajar con macrodatos.

Después de que emergieran los macrodatos, se puso en boga una fase nueva: la *analítica de macrodatos*.<sup>4</sup> Estos términos a menudo se usan de forma indistinta, pero representan dos caras de la misma moneda. Los macrodatos representan un proceso rápido de compilación, almacenamiento y acceso a grandes cantidades de datos e información de numerosas fuentes y con estructuras variables. La analítica de macrodatos representa las herramientas, la pericia profesional y los procesos que pueden transformar macrodatos en detalles, desde la preparación de inteligencia del entorno de operación hasta la advertencia de amenazas pasando por la percepción del espacio de combate predictivo para seleccionar objetivos. A su vez, estos detalles dan lugar a decisiones en toda la gama de operaciones militares y diplomáticas, desde operaciones de disuasión estratégica hasta enfrentamientos tácticos en tiempo casi real.

Los debates sobre el potencial de los macrodatos frente a la exageración se derivan principalmente de entender mal los macrodatos y la analítica de macrodatos.<sup>5</sup> Las animadoras de macrodatos históricamente han hecho cuatro afirmaciones interesantes sobre macrodatos que como mucho son simplificaciones exageradas optimistas: (1) el análisis de datos produce resultados asombrosamente exactos; (2) es innecesario muestrear porque los macrodatos nos permiten capturar todos los puntos de datos posibles; (3) los altos niveles de correlación en los macrodatos hacen que los debates cuantitativos de sus causas estén pasados de moda; y (4) los modelos estadísticos son similarmente irrelevantes porque “los datos hablan por sí solos.”<sup>6</sup> En verdad, los macrodatos no eliminan los retos tradicionales de recopilación y análisis de datos; cambian radicalmente la forma de dónde y cómo se producen los obstáculos. El reto principal se deriva de la afirmación final: los datos nunca hablan por sí mismos. La manera en que los datos se reúnen, organizan y procesan conforman el mensaje que los datos envían al usuario. Los algoritmos complejos realizan muchas de estas funciones para activar una analítica de macrodatos, pero esos algoritmos, incluso facilitados por la programación de máquinas, deben ser programadas por seres humanos y adaptados para responder a cuestiones especificadas de antemano.<sup>7</sup> Esto significa que los macrodatos siguen estando sujetos a sesgos en recopilación, visualización y análisis de los que los analistas deben estar muy al tanto. Los macrodatos permiten el acceso a puntos de datos exponencialmente en aumento para facilitar un análisis más rápido de más puntos de datos, pero los análisis de macrodatos defectuosos engendran un análisis defectuoso.

## Cómo los macrodatos cambian la forma de inteligencia

De las cuatro V de los macrodatos, los analistas han tenido que vérselas recientemente sobre todo con la primera y la tercera “V”, pero a una escala más pequeña y más manejable. El ritmo de recopilación, la uniformidad relativa de las amenazas planteadas por los actores estatales, y la obtención sin el contexto apropiado de análisis y producción junto con las líneas de producción de disciplina de inteligencia (las INT, es decir, inteligencia de señales [SIGINT], inteligencia geoespacial [GEOINT], inteligencia de imágenes [IMINT], inteligencia humana [HUMINT], inteligencia de fuentes abiertas [OSINT] e inteligencia de medidas y señales [MASINT]),<sup>8</sup> permitió la división del esfuerzo en problemas de datos separados que podrían ser analizados en partes por especialistas, con respuestas de inteligencia de todas las fuentes producidas combinando partes de componentes.

El impacto de la revolución de la información en aptitudes básicas de inteligencia de la USAF (recopilación, análisis, selección de objetivos e integración) se concentró primero en la recopilación y en segundo lugar en análisis de amenazas y objetivos (fig. 1). Se ha producido un aumento considerable de recopiladores y sensores disponibles, con ISR integrados globalmente permitiendo una explotación en tiempo casi real. Al mismo tiempo, las demandas operacionales desplazaron el análisis tanto para el análisis de amenazas como de objetivos hacia el tiempo casi real a fin de penetrar en el ciclo OODA (Observar, orientar, decidir y activar) del adversario.<sup>9</sup> En una época de recursos limitados con pocos indicios de recursos humanos significativamente mayores en el futuro cercano, cambiar la producción de inteligencia para cumplir con las demandas de operación de hoy es poco probable que

venga de una revolución adicional de recopilaciones o análisis. Hoy, incluso dentro de las INT, el volumen, la velocidad y la variedad de recopilación de datos e información han crecido hasta el punto que los analistas ya no podían examinar cuidadosamente todos los datos recopilados de forma suficiente para almacenarlos, y mucho menos analizarlos, todo ello sin ayuda de programas informáticos y procesos automatizados. Además, el advenimiento de una edad cibernética transformó la naturaleza de la recopilación de fuentes disponibles públicamente en que el análisis de fuentes abiertas ha evolucionado de una fuente de información a análisis de ayuda a una verdadera disciplina de inteligencia por propio derecho, OSINT, (por sus siglas en inglés) como temas profesionales, de gobierno y legales relacionados con la recopilación, el análisis y la producción.

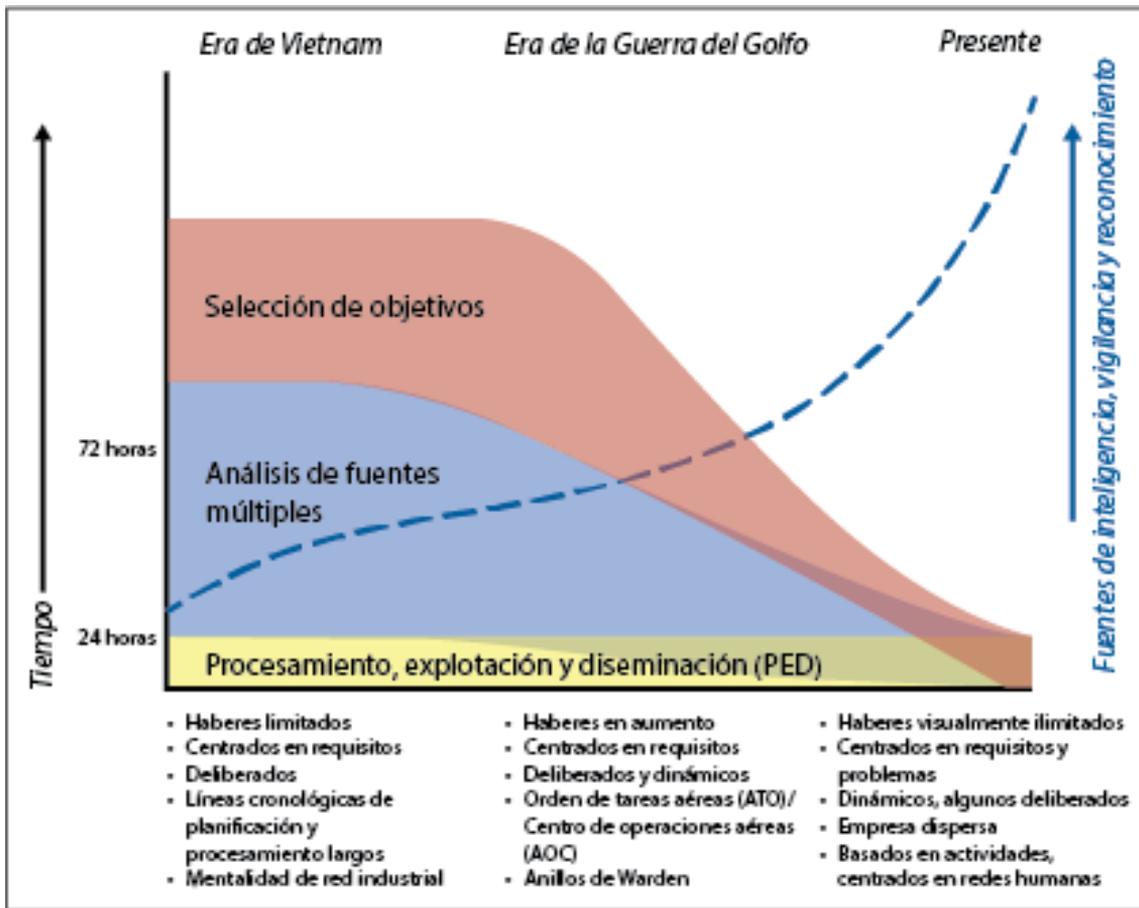
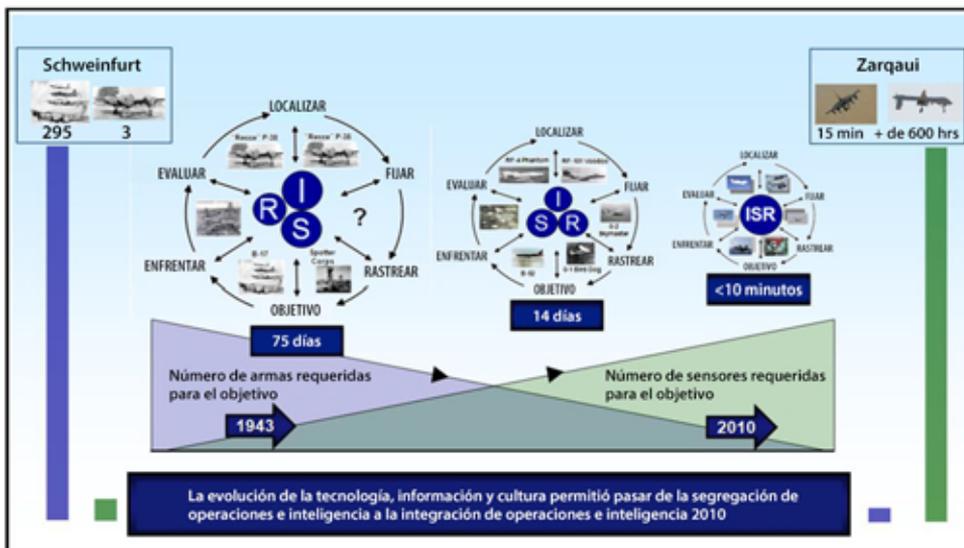


Figura 1. El impacto de la revolución de la información en la recopilación, análisis y selección de objetivos

El futuro está en la gestión de datos y la planificación de la inteligencia a fin de facilitar una inteligencia de la USAF centrada en problemas en vez de en requisitos. Los modelos industriales de producción ya no pueden mantener el ritmo del entorno de información. Como observó antes este año el director de la Agencia de Inteligencia Geoespacial Nacional, Robert Cardillo, “Si intentáramos explotar manualmente las imágenes de satélites comerciales que esperamos obtener durante los próximos

20 años, necesitaríamos ocho millones de analistas de imágenes. Incluso ahora, todos los días, en un solo teatro de operaciones de combate con un sensor individual, recopilamos datos equivalentes a tres temporadas de la NFL, de todos los partidos. ¡En alta definición!<sup>10</sup> Los analistas tienen más acceso a información que nunca y más herramientas a su disposición para recopilar información para rellenar lagunas de conocimientos. Facultar a esos analistas para dar forma a los conocimientos del comandante de lo que es conocido, lo que es evaluado, lo que es desconocido y conformar el conjunto adecuado de herramientas para responder a las cuestiones de inteligencia restantes es la forma de obtener la información adecuada para el encargado de tomar decisiones en el momento adecuado. La flexibilidad y la versatilidad deben aplicarse a la planificación y ejecución de campañas de ISR basadas en los efectos de la misma manera que se aplican a operaciones aéreas ofensivas.



**Figura 2. Implicaciones de la revolución de información para la selección de objetivos de la USAF.** Fuente: Centro de Doctrina, Desarrollo y Educación Curtis E. LeMay, *Documento de la Doctrina de Fuerza Aérea 2-0 Operaciones integradas globales de inteligencia, vigilancia y reconocimiento*, 6 de enero de 2012, 2, <https://fas.org/irp/doddir/usaf/afdd2-0.pdf>.

## Las cuatro V y la recopilación de inteligencia

El carácter de la guerra contra el terrorismo combinado con las innovaciones de la revolución de información de selección de objetivos de precisión ha desplazado el equilibrio de los esfuerzos de la USAF desde el volumen de munición lanzada hasta la demanda de recopilación de ISR. La Figura 2 muestra el desplazamiento dramático del equilibrio entre las aeronaves y la inteligencia requeridas para ejecutar un ataque aéreo para el efecto estratégico desde la SGM, donde tres horas de inteligencia apoyaron a 293 bombarderos, el 14 de octubre de 1943, en la incursión de Schweinfurt en la Alemania nazi comparadas con las más de 600 horas de trabajo de inteligencia para apoyar un intervalo de 15 minutos de una salida en la incursión de Abu Musab al Zarqai en 2006. El ataque de precisión requiere inteligencia de precisión, que cambia la carga de recursos humanos de operaciones de vuelo a procesamiento, explotación y análisis para facilitar la operación de ataque. Reconocer la mayor demanda de inteligencia para aumentar la capacidad de ataque ha resultado en un aumento constante

y pronunciado de las plataformas de recopilación, los sensores y el ancho de banda para apoyar las operaciones de “apoyo electrónico a distancia”, pero no necesariamente un aumento conmensurado de recursos humanos para analizar el gran volumen de recopilación dentro de los requisitos de tiempo para facilitar las operaciones. Al mismo tiempo, el desplazamiento de énfasis a operaciones de apoyo electrónico a distancia combinado con las fortalezas y vulnerabilidades de las operaciones en la Edad de la Información embarra más la delineación histórica de un área delantera y trasera de operación, convirtiendo este concepto del entorno de operación en una noción arcaica para las fuerzas aéreas modernas.

Para GEOINT, esto se manifestó más visiblemente en una explosión de demanda de recopilación de vídeos de movimiento completo (FMV por sus siglas en inglés). Durante gran parte de la última década, la USAF ha estado inmersa en FMV, y no está sola, ya que las capacidades orgánicas del Ejército, las operaciones especiales y las naciones asociadas tratan de ampliar el tamaño de sus flotas, aumentar el número de salidas de aeronaves guiadas por control remoto (RPA) e invertir en el ancho de banda para sostener esta demanda casi insaciable.<sup>11</sup> Las altas cargas de trabajo asociadas con el estado de “desplegados en posición” hizo que la IC redujera constantemente su fuerza de trabajo hasta 2015, perdiendo analistas de imágenes a un ritmo más rápido del que podían entrenarlos.<sup>12</sup> Varias iniciativas de calidad de vida implementadas desde ese tiempo reducen las horas y combaten la presión, pero también resultan en una capacidad reducida. En 2015, la USAF redujo brevemente su número de patrullas de RPA de 65–60 para ayudar a el piloto, el operador de sensores y las fuerzas de trabajo de inteligencia,<sup>13</sup> que se recuperen, pero las realidades operacionales obligaron a los militares a complementar su fuerza de RPA de servicio activo con contratistas para satisfacer la demanda.

Los FMV atrajeron la mayor parte de la atención fuera de la IC, pero incluso dentro del dominio de GEOINT/IMINT representan simplemente una fuente de inteligencia que aumentó considerablemente su demanda para satisfacer sus necesidades operacionales. Las necesidades de imágenes multiespectrales, imágenes hiperespectrales y fuentes indicadoras de objetivos móviles terrestres siguen aumentando la demanda en numerosas áreas de operación;<sup>14</sup> incluidos Irak, Siria y Afganistán, entre otros. Los conjuntos de sensores especializados proporcionan a la USAF capacidades de recopilación sin rival en generaciones previas, pero vienen con un entrenamiento, una dotación y un análisis de calidad intensivo con respecto al tiempo que hace que sea intensiva cada capacidad de potencial humano; llevando al límite el suministro de análisis de imágenes disponibles para procesar esta recopilación creciente.

El aumento considerable de los sensores GEOINT y de las capacidades de recopilación introducen otro reto significativo para una analítica efectiva sin la ayuda de soluciones de macrodatos. La variedad de información de datos recopilada en varios formatos gráficos “no puede ser descubierta” por los analistas, o lo que a veces se caracteriza como *datos oscuros*. La GEOINT explotada generalmente tiene resúmenes textuales que pueden buscarse mediante consultas similares a una búsqueda de imágenes en Google, pero debido a la falta de texto para dar una pista al analista, las imágenes relevantes pueden permanecer enterradas, sin ser descubiertas, en archivos de datos. Los algoritmos de macrodatos y las plantillas de explotación automatizadas pueden permitir que todas las imágenes, en tiempo casi real, estén asociadas con coordenadas geográficas, alineadas con lugares conocidos y archivadas automáticamente en bases de datos, en capas que se pueden buscar con imágenes relacionadas con el tiempo. Mientras que el modelo actual para ISR se centra en las operaciones, lo que requiere nuevas salidas para reunir información geoespacial (particularmente para conjuntos de problemas como pauta de vida), la analítica de macrodatos proporcionará a los futuros analistas acceso a una biblioteca de datos históricos y las herramientas para escudriñar rápidamente posibles miles de imágenes para ver cambios en función del tiempo y analizar el significado.

La GEOINT no está sola en ver un aumento exponencial en la demanda de recopilación y análisis. El aumento de las plataformas de recopilación también desembocó en un aumento de las cargas útiles de recopilación en disciplinas de inteligencia, incluidas las cargas útiles de SIGINT. A medida que aumenta el número de oportunidades de recopilación, y a medida que aumenta la conectividad global

en la Edad de la Información con la emergencia de amenazas globales conectadas por red, el volumen, la velocidad y la variedad de las señales recopiladas siguen aumentando, a menudo a un ritmo más rápido que nuestra capacidad de reclutar y entrenar a analistas.<sup>15</sup> Así como las horas de vídeo adquiridas por las RPA pueden quedarse sin analizar durante años sin la posibilidad de analítica de macrodatos para dar pistas y ayudar a los analistas en segmentos clave de recopilación para el análisis, las horas de comunicaciones interceptadas pueden quedarse sin analizar si no se tienen las herramientas automatizadas para separar el trigo de la paja de los petabytes de recopilación. Más allá de SIGINT y GEOINT, la MASINT similarmente ha experimentado un auge de recopilaciones y demanda de producción, con radar de apertura sintética y detección de cambios coherente, entre otras capacidades en una demanda cada vez más alta.<sup>16</sup>

## Inteligencia de fuentes abiertas

Tal vez no haya ningún ejemplo que explique mejor el enorme cambio en la recopilación en lo referente a las V de macrodatos que la creación de OSINT como verdadera disciplina de inteligencia. Cuando decimos que OSINT es una nueva disciplina muchos analistas de la guerra fría advierten, “No, siempre hemos tenido OSINT, y prueba de ello es el Centro de Fuentes Abiertas de la Agencia Central de Inteligencia (CIA)”.<sup>17</sup> De hecho, una regla general común citada durante décadas, que se remonta a una afirmación del entonces director de la CIA, Allen Dulles, es que más del 80% de los análisis de inteligencia se derivan al final de una fuente abierta. Todo esto es cierto, pero, desde un punto de vista de la doctrina, estaría mejor caracterizada como *información de fuentes abiertas*. La OSINT como disciplina de inteligencia está directamente asociada con la proliferación de internet y de los medios de comunicación sociales y con ello la necesidad de desarrollar nuevos instrumentos profesionales para buscar y descubrir información, supervisión para asegurarse de que las leyes relevantes, y las órdenes de protección de ciudadanos e información y salvaguardia sean observadas por la IC, y control del proceso. Sin las soluciones analíticas de macrodatos sería imposible para los analistas revisar cuidadosamente los miles de millones de puntos de datos disponibles (volumen, variedad y velocidad), identificar los datos relevantes e irrelevantes (veracidad), salvaguardar los derechos de los ciudadanos y seguir otras leyes y reglamentos correspondientes, y descubrir detalles de inteligencia relevantes para satisfacer las necesidades de los clientes.

La revolución de la información ha desembocado en una nueva cultura en línea de compartir, y lo que muchos caracterizan como compartir en exceso.<sup>18</sup> El lado positivo para la IC es que a través de Twitter, Facebook, Snapchat, blogs y numerosos sitios de medios de comunicación sociales aún no inventados, la inteligencia tiene decenas de millones de recopiladores pasivos de todo el mundo. En la década de 1990, los analistas se enfrentaron a la posibilidad de que la evaluación de daños en combate podría ser llevada a cabo en CNN antes de que tuviera el tiempo de completar el ciclo de inteligencia para su evaluación. Hoy, si un RPA pierde conectividad y se estrella, es probable que se informe en Twitter y que se retuitee múltiples veces antes de que se confirme la pérdida de la aeronave. Los análisis de investigación e inteligencia académicos se basan ahora en análisis de sentimientos, en esencia, una versión refinada y adaptable de “tendencias” en Twitter, para determinar los sentimientos de las poblaciones a fin de predecir potencialmente la futura actividad (Disturbios civiles, y así sucesivamente).

## Demandas de tiempo de las operaciones

En la mayoría de los debates comerciales de los macrodatos, la velocidad se concentra en la rapidez con la que se adquiere la información. Para las operaciones de inteligencia, la velocidad puede aplicarse igualmente a la velocidad con la que los operadores, comandantes y otras personas encargadas de tomar decisiones requieren resultados de inteligencia para facilitar operaciones. La campaña con-

tra el Estado Islámico es para Estados Unidos predominantemente una campaña centrada en el aire, haciendo énfasis en una selección de objetivos deliberada y dinámica para aislar y degradar un proestado con una infraestructura fija limitada y que se mezcla inmediatamente con la población para defenderse de los ataques.<sup>19</sup> Esta combinación, junto con la necesidad de minimizar el riesgo de los daños colaterales, ha servido solamente para aumentar las demandas de ISR. Esto incluye localizar y caracterizar objetivos, manteniendo una vigilancia de la ubicación de los lugares escogidos como blancos potenciales, y entender las pautas de vida de la población. El Teniente General Charles Q. Brown Jr., comandante del componente aéreo de las fuerzas de la coalición, fue al grano explícitamente en mayo de 2016, al afirmar que, “Porque lo que me ayuda a hacer es desarrollar objetivos para que podamos atacar al mismo tiempo que los desarrollamos. Cuanta más ISR tenga, más puedo minimizar el riesgo de bajas civiles y continuar la campaña aérea de precisión que tenemos.”<sup>20</sup>

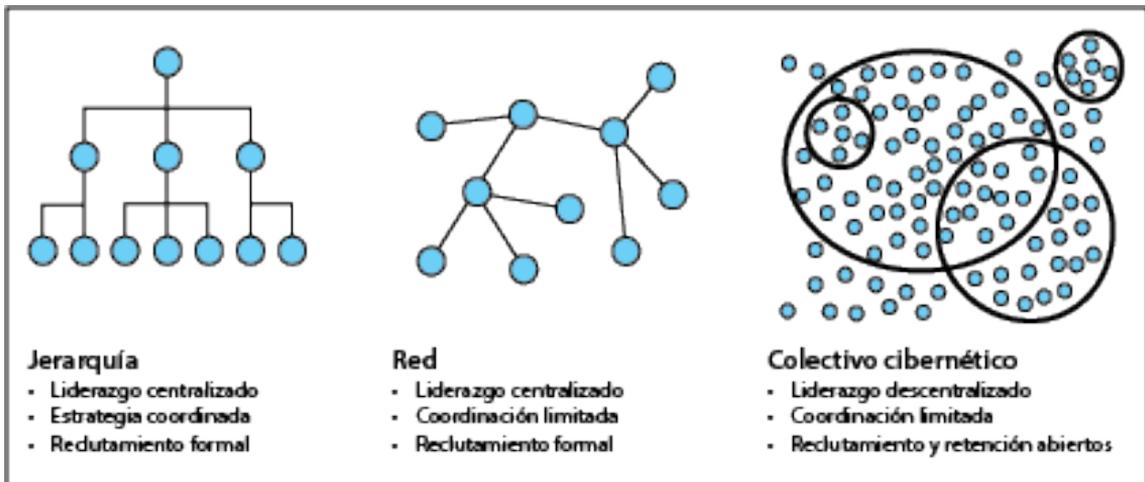
Más en este contexto tiene dimensiones de volumen y tiempo, ya que el tiempo en que la información sea de valor en un ataque dinámico es mínimo, especialmente comparado con un objetivo más tradicional como un campo de aviación, un búnker de comando o una parte de una red de comunicaciones. La naturaleza en tiempo casi real de los FMV y su función crítica en la fase de participación/terminación de operaciones llevó a muchos observadores a concluir que la selección de objetivos es más fácil de hacer hoy en tiempo real, pero en la práctica esto representa la punta del iceberg de inteligencia que facilitó el ataque. Las fuerzas de la coalición requieren una red de analistas sincronizada globalmente para fusionar rápidamente las imágenes, las interceptaciones electrónicas y los consejos de informantes para dar pie a atacar objetivos potenciales. La ISR integrados globalmente facilita estas redes por medio de un acceso oportuno a más recopilación, pero con ello un problema de veracidad significativo. Al mismo tiempo, este sistema está suscitando simultáneamente críticas de organizaciones de derechos humanos con preocupaciones de que se produzcan bajas civiles y de los defensores de campañas aéreas más tradicionales que dicen que los números totales de objetivos alcanzados son insuficientes incluso según las normas de las campañas recientes.<sup>21</sup> La comunidad de ISR, y la IC se deben enfrentar, más ampliamente, al complejo problema de la gestión de operaciones distribuidas, control de análisis de calidad y gestión de conjuntos de datos para dar a la empresa de ISR y a los operadores que actúen en tiempo real una visibilidad completa al avance del desarrollo de objetivos.

## El entorno de amenazas

Las frecuentes apelaciones del Estado Islámico en Irak y Siria (ISIS) al terrorismo de los “lobos solitarios”, a través de lo que se ha llamado el *califato digital*, resalta el reto que plantea la internet para la seguridad en Occidente.<sup>22</sup> Antes de eso, colectivos cibernéticos como 4chan/“Anonymous” estaban explotando la conectividad en línea para formar comunidades caóticas de reparto de información que al final facilitaron la acción colectiva en una serie de temas.<sup>23</sup> Como la inteligencia militar de EE.UU. ha considerado tradicionalmente el dominio militar convencional como el foco de su misión, en la Edad de la Información la narrativa armada está ganando rápidamente terreno como un teatro de operaciones para la seguridad nacional.<sup>24</sup> Entender el entorno de amenazas en la Edad de la Información solamente será posible con soluciones de macrodatos y a su utilización efectiva. Aunque contrarrestar este reto probablemente recaerá finalmente en las entidades que no son el Departamento de Defensa, como el Departamento de Estado, la misión de la USAF exige conocimientos y defensa del ciberdominio. Como tal, los analistas de inteligencia de la USAF deben estar a la vanguardia del análisis y descubrimiento de amenazas en el ciberdominio.

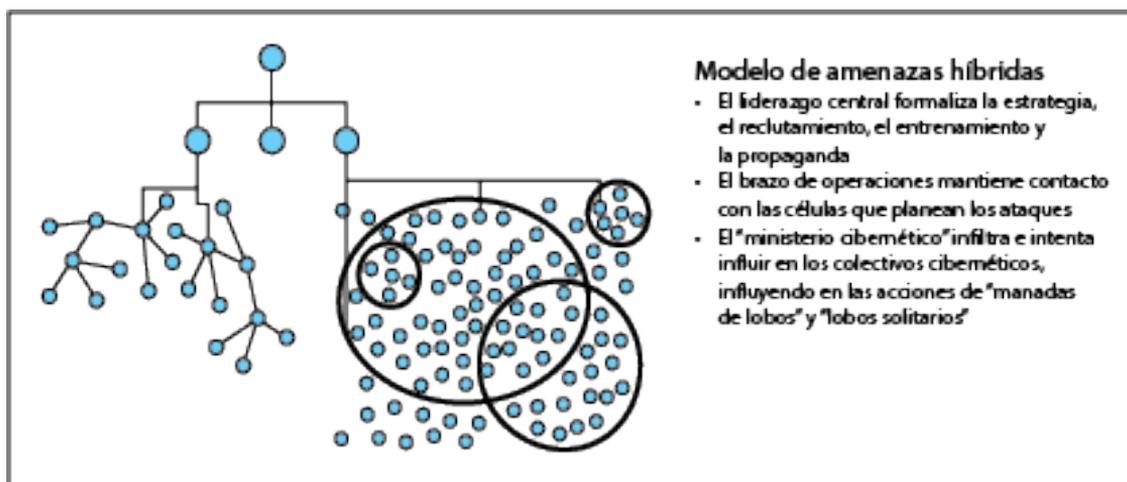
La pasada década de operaciones de contraterrorismo y contrainsurgencia ha hecho que los analistas de inteligencia de la USAF sean expertos en el monitoreo y la evaluación de redes terroristas en zonas de conflicto, particularmente en Irak como fue el caso de al Qaeda en Irak y con grupos relacionados con el Talibán en Afganistán. No obstante, los colectivos cibernéticos representan un reto diferenciado. Estos colectivos carecen de una estructura de mando centralizada, en vez de operar en gran

medida a través de las normas y los valores de la comunidad en línea. Su afiliación es abierta, sin mecanismos formales de reclutamiento o retención, y su planificación estratégica es mínima. La mayoría tiende a resistir a cualquiera que emerja como líder o portavoz de su grupo; podrían emerger personas con influencia durante períodos limitados, pero la naturaleza abierta y diversa de la afiliación impide a cualquiera emerger durante un período prolongado sin fracturar el grupo. Las comunidades más pequeñas podrían desarrollar jerarquías internas más fuertes, ya que la afiliación limitada conlleva ideologías homogéneas, pero este sirve para limitar el alcance global y la influencia de colectivos más grandes.<sup>25</sup> La Figura 3 muestra de forma resumida las distinciones entre una jerarquía, una red y los colectivos cibernéticos.



**Figura 3: Jerarquías, redes y colectivos cibernéticos.** (Extraída de fuentes en Max Sterling, “The Cyber Collective Threat: A Pack of Lone Wolf Terrorists” (La amenaza de los colectivos cibernéticos: una manada de lobos solitarios terroristas), *El Proyecto sobre Paz y Seguridad Internacionales, Instituto de Teoría y Práctica de Relaciones Internacionales, College of William and Mary*, abril de 2017, [http://www.wm.edu/offices/itpir/projects/pips/\\_documents/pips/2016-2017/Sterling.Max.pdf](http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Sterling.Max.pdf).)

El carácter de los colectivos de inteligencia proporciona un foro que puede ser infiltrado para incitar ataques de lobos solitarios o de manadas de lobos; la información propagada simultáneamente entre un círculo del colectivo inicia una acción, imaginémosnos un “flash mob”, con poca o ninguna advertencia. Al mismo tiempo, el carácter caótico de los colectivos tiende a hacer que sus justificaciones sean también caóticas; su *forma de operar* a menudo consiste en oponerse a figuras de autoridad y abusos de poder, no a tratar de reemplazarlas activamente por una nueva ideología dominante. Por esta razón, muchos ataques de lobos solitarios y de manadas de lobos iniciados por individuos reclutados a través de colectivos, incluso cuando se inspiran en organizaciones con ideologías específicas, no muestran necesariamente una afinidad de posiciones ideológicas específicas; solamente su naturaleza reaccionaria. Por ejemplo, es posible que el pistolero del club nocturno de Orlando, Omar Mateen no haya entendido la diferencia entre ISIS, al Qaeda e Hizbulá, a pesar de que haya distinciones significativas sectarias y estratégicas entre estos grupos.<sup>26</sup> No obstante, a tenor de las características de los colectivos cibernéticos, estos grupos están relacionados en línea por sentimientos antioccidentales y un punto de vista caótico con respecto al orden occidental. Las llamadas a incitar al caos para vengar daños morales se propagan en ese entorno, mientras que no lo hacen mensajes ideológicos específicos y alineaciones más formales con grupos específicos.



**Figura 4. La amenaza híbrida de los colectivos cibernéticos infiltrados**

El reto para las agencias de inteligencia que se deriva de esta organización descentralizada nueva es la perspectiva de infiltración de colectivos como parte de una estrategia múltiple dirigida simultáneamente a desestabilizar adversarios mediante ataques profundos al estado mientras concentran una violencia más organizada y estratégica contra gobiernos locales mediante organizaciones conectadas por red y jerárquicas.<sup>27</sup> La Figura 4 explica cómo podría ser este modelo híbrido, con un núcleo de liderazgo estratégico central que dirija acciones a través de múltiples departamentos para reclutamiento, propaganda, entrenamiento, operaciones de acción directa, coordinación con redes e infiltración de propaganda en línea de colectivos cibernéticos. A pesar de que estas redes son amplias y diversas, la representación de redes tradicionales no es posible dado lo rápido que pueden cambiar y la rapidez con que se pueden compartir los mensajes a través de colectivos. La identificación de las personas con influencia dentro de la red requiere soluciones de macrodatos para seguir el volumen de tráfico de mensajes, identificar qué temas podrían ser más comentados y qué mensajes podrían ser receptivos en qué áreas, e identificar cambios en tendencias en esos mensajes que podrían presagiar un cambio en estrategias de ataque (tiroteos masivos, estrellar vehículos y la siguiente evolución de amenazas). Este nivel de entendimiento de organizaciones y mensajes adversarios es vital para contrarrestar a los adversarios directamente a nivel de operación y por encima, pero potencialmente es más importante para indicaciones táctica y advertencias para proteger la fuerza.

Así como los adversarios pueden usar el ciberdominio para llevar a cabo operaciones mediante influencia, pueden usar ciberherramientas para impedir la inteligencia y amplificar sus mensajes. Uno de los más predominantes hoy en día es el uso de bots,<sup>28</sup> robots de software diseñados para propagar automáticamente mensajes por medios sociales y otros modos en línea. Estos pueden distorsionar los datos para el análisis de sentimientos, cambiar completamente la opinión pública mediante un efecto moda haciendo que sea más popular, propagando automáticamente desinformación a través de colectivos cibernéticos y amplificando el reclutamiento. Las investigaciones de actividades potenciales de Rusia en la elección de 2016 no se han concentrado tanto en la amenaza de pirateo informático en el sentido tradicional, sino en la ingeniería social ejecutada por bots con mensajes dirigidos a grupos específicos.<sup>29</sup> A partir de ahora, los analistas que operan en un entorno multidominio complejo deben entender la naturaleza emergente de las amenazas planteadas por el dominio cibernético.<sup>30</sup> El mantenimiento de la percepción básica de la situación, y el entendimiento de las operaciones, solamente

puede conseguirse al entender mejor la analítica de los macrodatos y el reconocimiento de su poder como herramienta y sus vulnerabilidades.

## El modelo de inteligencia de la Edad Industrial comparado con el modelo de la Edad de la Información

Las tres V de los macrodatos, combinadas con sus implicaciones para amigos y enemigos por igual, necesitan un replanteamiento de nuestro modelo industrial para la producción de inteligencia. Todos los operadores de inteligencia están entrenados desde sus cursos básicos en el ciclo de inteligencia de cinco pasos conocido como planificación y dirección; recopilación; procesamiento, explotación y disseminación (PED, por sus siglas en inglés); análisis y producción; y disseminación (PCPAD).<sup>31</sup> Este proceso estructurado y repetible asegura la claridad de los pasos de producción y controla los procesos analíticos. También contiene elementos burocráticos, en particular para grandes organizaciones como inteligencia de USAF que correlacionan los pasos del ciclo PCPAD con diferentes unidades/oficinas. Un modelo de inteligencia de la Edad de la Información debe encontrar formas de moverse más allá del modelo burocrático solamente (no reemplazarlo, sino complementarlo), y facilitar la gestión de datos en una empresa distribuida para apoyar inteligencia de calidad de decisiones para demandas operacionales. La ciencia de datos debe considerarse como una aptitud básica de la comunidad de inteligencia en la Edad de la Información, y analistas de inteligencia tradicionales deben trabajar mano a mano con científicos informáticos y gerentes de datos diestros para facilitar la producción de inteligencia.

Otro reto/oportunidad para la inteligencia de la USAF es la combinación de inteligencia e ISR. El Departamento de Defensa define ISR como “una actividad que sincroniza e integra la planificación y operación de sensores, haberes, y sistemas de procesamiento, explotación y disseminación en apoyo directo a operaciones actuales y futuras. Se trata de una función integrada de inteligencia y operaciones”.<sup>32</sup> Aunque es una combinación de inteligencia y operaciones, representa un subconjunto del ciclo de inteligencia total. La asignación de tareas representa la parte final del proceso de planificación, donde se asignan requisitos a las unidades a través de la orden de asignación de tareas aéreas (ATO), mientras que la recopilación y PED reflejan esas etapas del ciclo de PCPAD, según se explica en la figura 5.

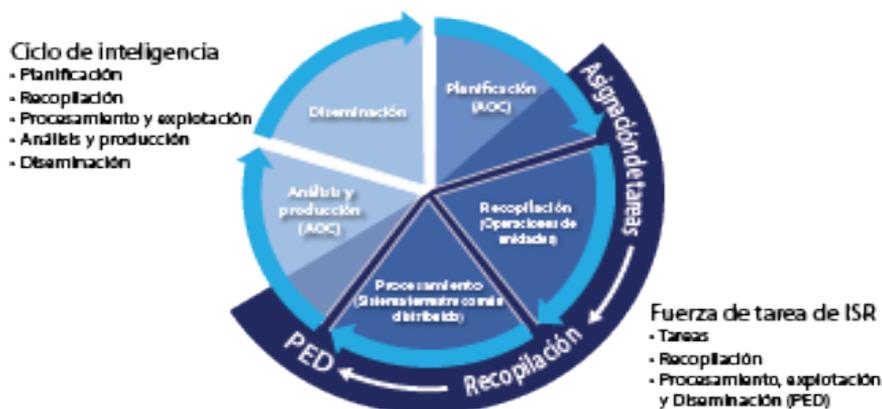


Figura 5. Modelo industrial de producción de inteligencia

Este modelo configura una infraestructura de análisis de inteligencia que demostró ser efectiva para evaluar los actores de estado, pero su carácter de secuencia en el tiempo ha puesto en práctica un

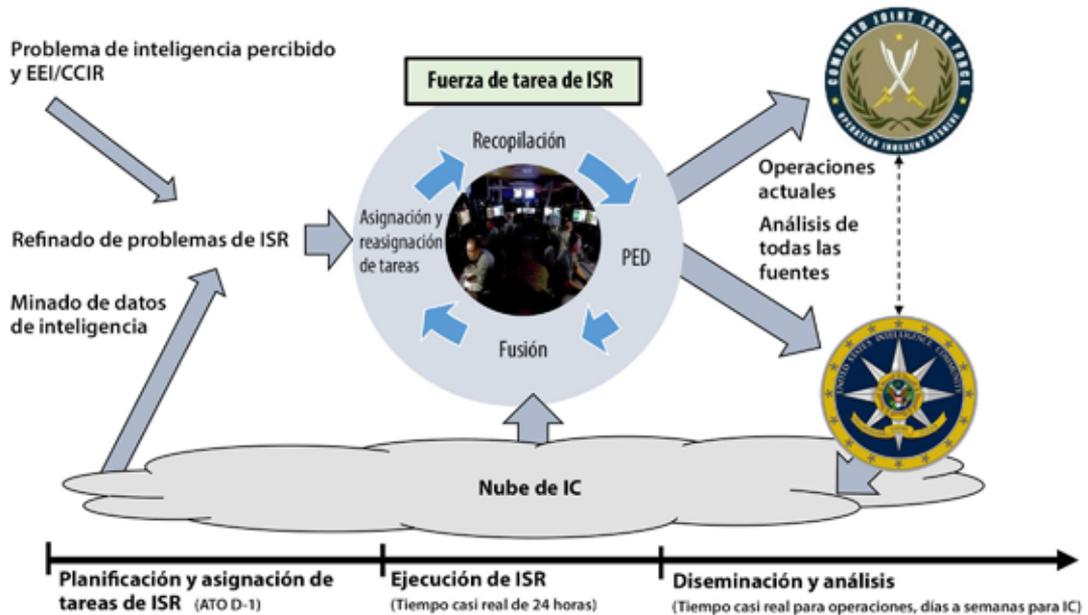
factor de limitación en el ciclo OODA de ISR de la USAF. La planificación de ISR se ejecuta mediante el ciclo de tareas de ATO de 72 horas y está controlada por un proceso de gestión de recopilación por el que las prioridades de los comandantes para los objetivos de recopilación (sitios de los que se van a captar imágenes o recopilar de otra forma) se recogen y apilan mediante un proceso de prioridades de la junta o arbitrado antes de la ejecución de la ATO. Esto es seguido por un proceso de análisis que puede añadir días al proceso para un análisis a nivel operacional dentro de la USAF, o semanas para una producción de todas las fuentes en agencias nacionales. Esto interfiere desde un punto de vista de ISR con el principio de flexibilidad de la USAF, que debe permitir a los operadores de ISR amasar y maniobrar efectos de ISR en puntos críticos del entorno de operación para su integración en tiempo, espacio y finalidad.<sup>33</sup> Además, como las fuentes de ISR se han hecho más complejas y crece el apilamiento de datos e información de inteligencia básicos, es poco probable que modelos tradicionales para desarrollar requisitos de inteligencia prioritarios, requisitos de información crítica del comandante y otras solicitudes de recopilación de inteligencia en el futuro seguirán siendo un medio eficiente de fijar prioridades de haberes de recopilación.

A mediados de la década de 2000, los operadores de ISR se enfrentaron al reto de explicar a los clientes, “No solicite un haber como el Predator; solicite una capacidad como FMV”. Hoy en día, el problema se complica a medida que las fuentes de recopilación están mucho más especializadas y numerosas, dejando al personal táctico de ISR mejor situado para determinar qué fuente de ISR está mejor posicionada para rellenar lagunas de inteligencia. La adición de sensores pasivos como OSINT y análisis de macrodatos descubribles de HUMINT, SIGINT, GEOINT y MASINT existentes puede responder rápidamente a un problema percibido de un cliente sin necesidad de efectuar una recopilación adicional a un nivel de confianza suficiente para justificar que no se vuelva a asignar el haber. Aunque la gran mayoría de las asignaciones de haberes y recopilación seguirá, en un futuro inmediato, mediante este proceso estándar, una parte de los haberes aéreos de ISR y de la capacidad analítica debe dedicarse a una alternativa de la Edad de la Información para conformar directamente la campaña aérea en tiempo casi real.

La alternativa para la Edad de la Información es inteligencia centrada en problemas, encabezada por una fuerza de tarea de ISR. En vez de recopilar tareas, la entrada de las operaciones al proceso de ISR debe percibirse como problemas de inteligencia, que los especialistas de ISR pueden traducir después a problemas de ISR refinados, lagunas de inteligencia y prioridad de sensores de ISR en un esquema combinado de maniobrar para rellenar esas lagunas. Una fuerza de tarea de ISR, facultada por un solo comandante de gestión con autoridades de requisitos de recopilación orgánicos y autoridades de gestión de operaciones de recopilación, está facultada para formar un plan de ISR integrado para un objetivo operacional especificado. Este es el paso siguiente en el avance de la directiva de 2009 del Mando Central de la Fuerza Aérea de EE.UU. codificando órdenes de tipo de misión (MTO, por sus siglas en inglés) de ISR como críticas para apoyar operaciones de contingencia de operación.<sup>34</sup> A falta de una fuerza de tarea de ISR especificada con posesión de haberes de ISR y autoridad para asignarles tareas, la estructura de MTO actual es más parecida a una tarjeta de coordinación de ISR para reasignar tareas que una verdadera orden de tipo de misión según se define en la Publicación Conjunta 3-50, *Recuperación de personal*.

Este modelo de fuerza de tarea de ISR, descrito en la figura 6, reestructura el proceso de planificación para haberes aéreos orgánicos de ISR a un molde centrado en los problemas, incorporando analíticas de macrodatos para refinar el problema de ISR asignado. La “nube de IC”, compuesta de acceso a datos de OSINT en tiempo casi real y la base de datos completa de análisis de múltiples inteligencias de toda la IC, permite a los analistas de las primeras etapas del proceso conformar respuestas al problema del cliente, mientras se refinan sus cuestiones de inteligencia basadas en un entendimiento refinado de lo que realmente conoce la IC. El personal táctico de ISR puede hacer corresponder después la mejor plataforma de recopilación para responder a la laguna de inteligencia. Las operaciones de ISR pueden ser reasignadas de inmediato por la fuerza de tarea de ISR, bajo la autoridad del comandante gracias a la intención de la MTO; en práctica por un operador designado con

autoridad de asignación de tareas a sensores. Esto refina el tiempo casi real de recopilación en concierto con PED y entidades de fusión, maximizando la utilidad del sensor. Los productos de la fuerza de tarea de ISR pueden distribuirse después simultáneamente en tiempo casi real a clientes operacionales para planificar y tomar decisiones y a la IC más grande para un análisis adicional y finalmente la incorporación en la nube de IC para su futura explotación.



**Figura 6. El modelo de fuerza de tarea de inteligencia, vigilancia y reconocimiento para inteligencia aérea.** (Fuente: Mayor Michael P. Kreuzer y Mayor Denis A. Dallaire, “Targeting the Islamic State” (Determinación del Estado Islámico como objetivo) *The Mitchell Institute for Aerospace Studies*, 14 de abril de 2017, [http://docs.wixstatic.com/ugd/a2dd91\\_4892807f169341188b7ebcd2f775671d.pdf](http://docs.wixstatic.com/ugd/a2dd91_4892807f169341188b7ebcd2f775671d.pdf)).

Permitir esta solución de macrodatos a un análisis de inteligencia y asignación de tareas de ISR también requiere que la comunidad de inteligencia de la USAF piense en términos más amplios acerca de sus opciones de personal de ahora en adelante, según se describe en la Figura 6. La IC hasta la fecha ha aceptado a especialistas en una serie de campos científicos más allá de los oficiales de inteligencia y el personal alistado. Para que los macrodatos den resultado en el futuro, la empresa de inteligencia de la USAF debe incorporar científicos de datos, programadores informáticos y científicos sociales con conocimientos expertos en el ciberdominio a fin de entender la naturaleza de los datos a los que accedemos, y analizar efectivamente el entorno de operación del ciberdominio.

## Conclusión

Según una cita antigua modificada, tal vez usted no esté interesado en los macrodatos, pero los macrodatos están interesados en usted.<sup>35</sup> Los macrodatos conforman el entorno de información moderno, y al compartir información y acceder a la nube, los macrodatos ya están reestructurando radicalmente cómo los analistas procesan e interpretan los datos. Los adversarios explotan el complejo entorno cibernético, influyen en las poblaciones y ejecutan ataques contra intereses de EE.UU. de un

modo que solo se puede detectar mediante soluciones de macrodatos. Nuestra capacidad de recopilar y almacenar datos en bruto sigue excediendo nuestra capacidad de procesar lo que hemos recopilado, lo que significa que probablemente ya tenemos, en algún lugar de nuestras vastas bases de datos de información, las respuestas a los rompecabezas que los clientes de inteligencia tienen hoy y los que plantearán mañana. A falta de macrodatos para gestionar los datos y la información, seguimos recopilando y llevándola a los planificadores de ISR rápidamente para facilitar una recopilación más inteligente y oportuna, la comunidad de inteligencia de la USAF se enfrentará a una sobrecarga de información resultando en una parálisis de decisiones. Obtener la información adecuada, para el cliente adecuado, en el momento adecuado significa replantearse la planificación de ISR, y adoptar soluciones de macrodatos a los retos de ISR a los que nos enfrentamos. □

## Notas

1. David Rotman, "How Technology Is Destroying Jobs" (Cómo la tecnología está destruyendo trabajos), *MIT Technology Review*, 12 de junio de 2012, <https://www.technologyreview.com/s/515926/how-technology-is-destroying-jobs/>; Zeynep Tufekci, "The Machines are Coming" (Las máquinas están viniendo), *New York Times*, 18 de abril de 2015, [https://www.nytimes.com/2015/04/19/opinion/sunday/the-machines-are-coming.html?\\_r=0](https://www.nytimes.com/2015/04/19/opinion/sunday/the-machines-are-coming.html?_r=0); Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zacari, Andrej Zwitter, "Will Democracy Survive Big Data and Artificial Intelligence?" (¿Sobrevivirá la democracia a los macrodatos y a la inteligencia artificial) *Scientific American*, 25 de febrero de 2017, <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>; y Tim Harford, "Big Data: Are We Making a Big Mistake?" (Macrodatos: ¿estamos cometiendo un error), *Financial Times*, 28 de marzo de 2014, <https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0>.
2. SAS Institute, "Big Data: What It Is and Why It Matters" (Macrodatos: lo que son y por qué importan), 24 de mayo de 2017, [https://www.sas.com/en\\_us/insights/big-data/what-is-big-data.html](https://www.sas.com/en_us/insights/big-data/what-is-big-data.html).
3. Richard Holt, "Twitter in Numbers" (Twitter en números). *Telegraph*, 21 de marzo de 2013, <http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html>
4. SAS Institute, "Big Data Analytics" (Análítica de macrodatos).
5. Geethika B. Peddibhotla, "Gartner 2015 Hype Cycle: Big Data is Out, Machine Learning is in" (Ciclo de exageración de 2015 de Gartner: los macrodatos no están de moda, la programación de máquinas sí), *KD Nuggets*, <http://www.kdnuggets.com/2015/08/gartner-2015-hype-cycle-big-data-is-out-machine-learning-is-in.html>.
6. Harford, "Big Data" (Macrodatos).
7. SAS Institute, "Machine Learning: What It is and Why It Matters" (Programación de máquinas: lo que son y por qué importan), 24 de mayo de 2017, [https://www.sas.com/en\\_us/insights/analytics/machine-learning.html](https://www.sas.com/en_us/insights/analytics/machine-learning.html).
8. Oficina del Director Nacional de Inteligencia, "What is Intelligence?" (¿Qué es inteligencia?), 24 de mayo 2017, <https://www.dni.gov/index.php/what-we-do/what-is-intelligence>.
9. Desarrollado por John en la década de 1950 e introducido en el entrenamiento de la Fuerza Aérea en las décadas de 1960 y 1970, el "ciclo OODA" (observar, orientar, decidir, actuar) representa un modelo de toma de decisiones en cuatro fases con la implicación de que un ciclo OODA más rápido y mejor que el de su oponente es esencial para obtener una ventaja en combate. Como ejemplo corto, *vea* Richard Feloni y Anacle Pellisson, "A Retired Marine and Elite Fighter Pilot Breaks Down the OODA Loop, the Military Decision-making Process that Guides 'Every Single Thing' in Life" (Un infante de Marina retirado y un piloto de avión caza de élite rompe el ciclo OODA, el proceso de toma de decisiones militar que guía todas las cosas en la vida), *Business Insider*, 13 de Agosto de 2017, <http://www.businessinsider.com/ooda-loop-decision-making-2017-8>.
10. Robert Cardillo, "National Geospatial Intelligence Agency (NGIA) 2017 Symposium Remarks" (Comentarios del Simposio de 2017 de la Agencia Nacional de Inteligencia Geoespacial), (conferencia, sede la NGIA, Springfield, VA, 5 de junio de 2017), <https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/GEOINT-2017-Symposium.aspx>.
11. Christopher Drew, "Military Is Awash in Data from Drones" (Los militares están llenos de datos procedentes de drones), *New York Times*, 10 de enero de 2010, <http://www.nytimes.com/2010/01/11/business/11drone.html>; Kevin McCaney, "Pentagon Plans to Boost Drone Flights by 50 Percent" (Planes del Pentágono para aumentar los vuelos de drones en un 50 %), *Defense Systems*, 17 de agosto de 2015, <https://defensesystems.com/articles/2015/08/17/pentagon-to-increase-drone-flights-50-percent.aspx>; y Julian E. Barnes, "NATO Invests in More Bandwidth for New Data-Hungry Drones" (La OTAN invierte en más ancho de banda para nuevos drones hambrientos de datos), *Wall Street Journal*, 27 de marzo de 2017, <https://www.wsj.com/articles/nato-invests-in-more-bandwidth-for-new-data-hungry-drones-1490601588>.
12. Pratrach Chatterjee, "The Side of Drone Warfare No One Is Talking About" (El aspecto cara de la guerra de drones del que nadie habla), *Nation*, 13 de julio de 2015, <https://www.thenation.com/article/the-side-of-drone-warfare-no-one-is-talking-about/>.
13. Marcus Weisgerber, "Air Force Trims Drone Ops to Get Workforce 'Healthy'" (La Fuerza Aérea recorta las operaciones de drones para curar a la fuerza laboral), *Defense One*, 18 de mayo de 2015, <http://www.defenseone.com/business/2015/05/air-force-trims-drone-ops-workforce-healthy/113122/>.

14. Joey Cheng, “Hyperspectral Sensor Lets Drones See through Camouflage, Spot Explosives” (Sensor hiperespectral que deja que los drones vean a través del camuflaje, localicen explosivos), *Defense Systems*, 25 de febrero de 2015, <https://defensesystems.com/articles/2014/02/25/air-force-aces-hy-hyperspectral.aspx?admgarea=DS>.

15. Agencia de Seguridad Nacional (NSA), “Signals Intelligence” (Inteligencia de señales), *NSA*, 24 de mayo de 2017, <https://www.nsa.gov/what-we-do/signals-intelligence/>.

16. “RQ-4A/B Global Hawk HALE Reconnaissance UAV, United States of America” (UAV de reconocimiento RQ-4A/B Global Hawk HALE, Estados Unidos de América), *Air Force Technology*, 24 de mayo de 2017, <http://www.airforce-technology.com/projects/rq4-global-hawk-uav/rq4-global-hawk-uav6.html>.

17. Agencia Central de Inteligencia (CIA), “Open Source Center” (Centro de fuentes abiertas), *CIA*, 24 de mayo de 2017, <https://www.cia.gov/careers/games-information/view-our-advertising/pdf/OSC%20Insert.pdf>.

18. Mary D. Harrington y Lisa E. Heffernan, “Oversharing: Why Do We Do It and How Do We Stop (Compartir en exceso; ¿por qué lo hacemos y cómo lo dejamos de hacer?)”, *Huffington Post*, 3 de febrero de 2014, [http://www.huffingtonpost.com/grown-and-flown/oversharing-why-do-we-do-it-and-how-do-we-stop\\_b\\_4378997.html](http://www.huffingtonpost.com/grown-and-flown/oversharing-why-do-we-do-it-and-how-do-we-stop_b_4378997.html).

19. ayor Michael P. Kreuzer y Mayot Denis A. Dallaire, “Targeting the Islamic State” (Determinación del Estado Islámico como objetivo), *The Mitchell Institute for Aerospace Studies*, 14 de abril de 2017, [http://docs.wixstatic.com/ugd/a2dd91\\_4892807f169341188b7ebcd2f775671d.pdf](http://docs.wixstatic.com/ugd/a2dd91_4892807f169341188b7ebcd2f775671d.pdf); y Dave Majumdar, “Pentagon: ISIS Adapting to Air Strikes, Targeting Becoming ‘More Difficult’” (Pentágono: el ISIS se adapta a ataques aéreos, la selección de objetivos se hace cada vez más difícil), *USNI News*, 11 de agosto de 2014, <https://news.usni.org/2014/08/11/pentagon-isis-adapting-air-strikes-targeting-becoming-difficult>.

20. Kristina Wong, “US Commander: Lack of Intelligence Assets Slowing Down ISIS War” (Comandante de EE.UU.: la falta de haberes de inteligencia disminuyen la velocidad de la guerra contra el ISIS), *Hill*, 7 de junio de 2016, <http://thehill.com/policy/defense/282457-isis-air-war-commander-short-on-intelligence-assets>.

21. Eric Schmitt, “U.S. Says Its Strikes Are Hitting More Significant ISIS Targets” (EE.UU. dice que sus ataques están alcanzado blancos de ISIS más significativos), *New York Times*, 25 de mayo de 2016, [https://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?\\_r=0](https://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?_r=0).

22. Haroon Ullah, “Taking on the ‘Digital Caliphate’ in Our Fight Against ISIS” (Enfrentamiento con el ‘califato digital’ en nuestra lucha contra el ISIS). DIPNOTE: *Blog oficial del Departamento de Estado de EE.UU.*, 27 de marzo de 2017, <https://blogs.state.gov/stories/2017/03/27/en/taking-digital-caliphate-our-fight-against-isis>.

23. Max Sterling, “The Cyber Collective Threat: A Pack of Lone Wolf Terrorists” (La amenaza cibercolectiva: una manada de lobos solitarios terroristas), *El Proyecto de Paz y Seguridad Internacionales, Instituto para la Teoría y Práctica de Relaciones Internacionales, College of William and Mary*, abril de 2017, [http://www.wm.edu/offices/itpir/projects/pips/\\_documents/pips/2016-2017/Sterling.Max.pdf](http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Sterling.Max.pdf); y Dale Beran, “4chan: The Skeleton Key to the Rise of Trump” (4chan: la maestra del ascenso de Trump), *Medium*, 14 de febrero de 2017, <https://medium.com/@DaleBeran/4chan-the-skeleton-key-to-the-rise-of-trump-624e7cb798cb>.

24. Brad Allenby, “Weaponized Narrative is the New Battlespace” (La narrativa armada es el nuevo espacio de combate), *Defense One*, 3 de enero de 2017, <http://cdn.defenseone.com/b/defenseone/interstitial.html?v=7.5.0&rf=http%3A%2F%2Fwww.defenseone.com%2Fideas%2F2017%2F01%2Fweaponized-narrative-new-battlespace%2F134284%2F%3Foref%3DDefenseOneFB>.

25. Sterling, “Cyber Collective Threat” (Amenaza de los colectivos cibernéticos).

26. Adam Taylor, “Omar Mateen May Not Have Understood the Difference between ISIS, al-Qaeda and Hezbollah” (Es posible que Omar Mateen no haya entendido la diferencia entre ISIS, al-Qaeda e Hizbulá), *Washington Post*, 13 de junio 2016, [https://www.washingtonpost.com/news/worldviews/wp/2016/06/13/omar-mateen-may-not-have-understood-the-difference-between-isis-al-qaeda-and-hezbollah/?utm\\_term=.4718e23fe6f5](https://www.washingtonpost.com/news/worldviews/wp/2016/06/13/omar-mateen-may-not-have-understood-the-difference-between-isis-al-qaeda-and-hezbollah/?utm_term=.4718e23fe6f5).

27. Charlie Winter, “What I Learned from Reading the Islamic State’s Propaganda Instruction Manual” (Lo que he aprendido al leer el manual de instrucciones de propaganda del Estado Islámico), *Lawfare*, 2 de abril de 2017, <https://www.lawfareblog.com/what-i-learned-reading-islamic-states-propaganda-instruction-manual>.

28. Matthew Bondy, “Bad Bots” (Bots defectuosos), *El Proyecto de Paz y Seguridad Internacionales, Instituto para la Teoría y Práctica de Relaciones Internacionales, College of William and Mary*, abril de 2017, [http://www.wm.edu/offices/itpir/projects/pips/\\_documents/pips/2016-2017/Bondy.Matthew.pdf](http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Bondy.Matthew.pdf).

29. Gabe O’Connor, “How Russian Twitter Bots Pumped Out Fake News During The 2016 Election” (Cómo los bots de Twitter rusos propagaron noticias falsas durante la elección de 2016), *NPR*, 3 de abril de 2017, <http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election>.

30. Sargento Segundo Robert Barnett, “Goldfein: Future of War is Networked, Multi-domain” (Goldfein: el future de la guerra es un dominio múltiple conectado por red), *Mando Central de la Fuerzas Aéreas de EE.UU.*, 22 de marzo de 2017, <http://www.afcent.af.mil/News/Article/1127569/goldfein-future-of-war-is-networked-multi-domain/>.

31. CIA, “The Intelligence Cycle” (El ciclo de inteligencia), *CIA*, 24 de mayo de 2017, <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html>.

32. Estado Mayor Conjunto, *DOD Dictionary of Military and Associated Terms* (Diccionario de términos militares y asociados del Departamento de Defensa), 118, marzo de 2017, [http://www.dtic.mil/doctrine/new\\_pubs/dictionary.pdf](http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf).

33. Centro para Doctrina, Desarrollo y Educación Curtis E. LeMay, *Tomo 1, Doctrina básica: flexibilidad y versatilidad*, 27 de febrero de 2015, <https://doctrine.af.mil/download.jsp?filename=V1-D82-Flexibility-Versatility.pdf>.

34. Capitán Jaylan M. Haley, "An Evolution in Intelligence Doctrine: The Intelligence, Surveillance, and Reconnaissance Mission Type Order" (Evolución de la doctrina de inteligencia: orden de tipo de misión de inteligencia, vigilancia y reconocimiento), *Air & Space Power Journal*, octubre de 2012, [http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-26\\_Issue-5/ASPJ-Sept-Oct-2012.pdf](http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-26_Issue-5/ASPJ-Sept-Oct-2012.pdf).

35. Ken Blackwell y Bob Morrison, "Like It or Not, War Is Interested in You" (Tanto si le gusta como si no, la guerra está interesada en usted), *American Thinker*, 23 de abril de 2013, [http://www.americanthinker.com/articles/2013/04/like\\_it\\_or\\_not\\_war\\_is\\_interested\\_in\\_you.html](http://www.americanthinker.com/articles/2013/04/like_it_or_not_war_is_interested_in_you.html).



**Colonel Shane P. Hamilton, USAF** (MS, USAFA; MS, Escuela de Estudios Avanzados Aéreos y Espaciales (SAASS), Universidad Aeronáutica Embry-Riddle; MS, Colegio Industrial de las Fuerzas Armadas) es el subdirector de inteligencia, Comandancia del Mando de Combate Aéreo (ACC). Ha estado al mando a nivel de escuadrón y grupo, lideró la Fusión de Inteligencia Conjunta de las Fuerzas Aéreas de EE.UU. en Corea, y más recientemente sirvió como director del ACC para el Directorio de Análisis de Inteligencia, Selección de Objetivos y Gestión de Recopilación. Se graduó de la Escuela de Armas de la USAF y de la SAASS.



**Teniente Coronel Michael P. Kreuzer, PhD, USAF.** El Teniente Coronel Kreuzer (BA, USAFA; PhD, Universidad de Princeton; MPA, Universidad de Alaska-Anchorage; MSI, Universidad Militar de EE.UU.) es el jefe ejecutivo del Directorio de Inteligencia del Mando de Combate Aéreo. Es un oficial de inteligencia de carrera que ha servido como director de programas especiales en dispositivos contra explosivos improvisados y gestión de recopilación para la División Multinacional Norte en Irak, oficial de estado mayor del Equipo de Reconstrucción Provincial de Kapisa en Afganistán y jefe de Adiestramiento Formal de Oficiales de Inteligencia de la USAF.