Documento
Opinión

35/2021 22 de marzo de 2021

*Ángel Segundo Gómez González**

Tendencias de evolución de la inteligencia militar

Tendencias de evolución de la inteligencia militar

Resumen:

La inteligencia militar ha sido, es y seguirá siendo un pilar fundamental del éxito de las operaciones militares, un elemento clave para orientar la acción disuasoria, para planear las operaciones, para conducirlas y para valorar los efectos de las campañas y de las acciones tácticas. Su esencia es inmutable, pero sus orgánicas, sus procesos y sus medios materiales han evolucionado a lo largo de la historia. Lo han hecho impulsados por la propia evolución del entorno operativo, del arte militar, de la tecnología y del conocimiento disponible. Eso seguirá ocurriendo. La novedad en las próximas décadas vendrá dada, sobre todo, por los rápidos cambios geopolíticos y tecnológicos y por la complejidad que añade la incorporación de los ámbitos y dominios no físicos a las operaciones militares. Los avances tecnológicos podrán llegar a ser disruptivos (*game changers*) y la reconfiguración en curso del orden mundial cambiará el catálogo de amenazas y de posibles contextos operativos. Todo ello va a obligar a repensar la inteligencia militar. Sin cambiar su esencia, el edificio de la «inteligencia militar» deberá ser reformado por completo o quizá incluso haya que «construir uno nuevo».

Palabras clave:

Trasformación, conciencia situacional, disrupción tecnológica, JISR, camuflaje algorítmico, ciclo de inteligencia, dominio cognitivo.

Trends in the evolution of military intelligence

Abstract:

Military intelligence has been, is and will continue to be a fundamental pillar of the success of military operations, a key element to guide deterrent action, to plan operations, to conduct them and to assess the effects of campaigns and tactical actions. Its essence is immutable but its organization, its processes and its material resources have evolved throughout history. They have done so driven by the evolution of military art, of the operational environment, of technology and of the available knowledge. It will continue to do so. The novelty in the coming decades will come mainly from rapid geopolitical and technological changes and from the added complexity of incorporating non-physical domains into military operations. Technological advances may become disruptive —game changers— and the ongoing reconfiguration of the world order will change the catalogue of threats and possible operational contexts. All of this will force a rethinking of military intelligence and without changing its essence, the 'military intelligence' building will have to be completely revamped or perhaps even 'built anew'.

Keywords:

Transformation, situational awareness, technological disruption, JISR, algorithmic camouflage, intelligence cycle, cognitive domain.

Lo inmutable

«Josué, hijo de Nun, envió desde Sitim dos espías secretamente, diciéndoles:
Id, reconoced el terreno y, especialmente Jericó»
Deuteronomio, libro de Josué en relación con la batalla de Jericó. 1400 a. C.

La inteligencia militar es tan antigua como la guerra misma. Sus elementos esenciales y su razón de ser se han mantenido inmutables a lo largo de la historia. Ni los cambios en la concepción de la guerra y el modo de ejecutarla, ni las posibilidades de las herramientas disponibles —siempre en crecimiento— han hecho, ni harán, mutar esa esencia.

La inteligencia se dedica, como es bien sabido, a disipar la incertidumbre, a aportar comprensión sobre el entorno operativo y a dar a los jefes militares y sus Estados Mayores capacidad de anticipación, así como a contribuir a la neutralización de las amenazas a través del conocimiento de estas. Eso es lo que ha hecho durante milenios y es lo que, sin duda, seguirá haciendo. El pronóstico «meteorológico» sigue anunciando una persistente niebla clausewitziana[1] sobre el campo de batalla para las próximas décadas y será la inteligencia la que deba despejarla.

La visión, comprensión, claridad y agilidad que requerirá nuestra estrategia y también nuestra actuación operacional y táctica en los futuros entornos volátiles, inciertos, complejos y ambiguos, deberán sustentarse en gran medida, en nuestra inteligencia militar.

[1] «La guerra es el reino de la incertidumbre; tres cuartas partes de los factores en los que se basa la acción en la guerra están envueltos en una niebla de mayor o menor incertidumbre». *Vom Kriege*/*De la Guerra*. Carl von Clausewitz, 1832.

Los cambios

> «Este mundo globalizado se caracteriza por el incremento permanente de la velocidad del cambio, en el que cada vez es más frecuente la aparición de hechos disruptivos»
>
> *Panorama de tendencias geopolíticas. Horizonte 2040*[2]

> «Si queremos que todo permanezca como es, debemos cambiarlo todo»
>
> *El gatopardo*, Giuseppe Tomasi di Lampedusa

La naturaleza de la inteligencia militar no ha cambiado ni parece que vaya a cambiar, pero, sin duda, las características y magnitud del reto a que se enfrenta sí que han evolucionado y lo harán mucho más en el horizonte temporal (2035/2040) en el que se están centrando, en este momento, los esfuerzos de transformación y desarrollo de capacidades de las Fuerzas Armadas (FAS).

El acelerado ritmo de los cambios en curso y la previsible continuidad del cambio como rasgo definitorio de nuestra era, serán las características principales de las próximas décadas. El cambio será, quizá, el único elemento permanente, lo único sobre lo que podremos estar completamente seguros.

Es por ello por lo que la inteligencia militar, sus procesos, sus organizaciones y también sus estrategias con los objetivos, líneas de actuación y recursos a emplear; deberán mantener su capacidad de adaptarse ante los probables cambios. Algunos de estos cambios están ya en curso y podemos observarlos. Otros aún no han llegado y, por ello, deberíamos mantener la capacidad de responder con flexibilidad ante la aparición de sorpresas en el camino, de imprevistos. Imprevistos en el ámbito de la tecnología, de la geopolítica o de las amenazas. Sorpresas que, a veces, podrán suponer un cambio de las reglas del juego. Ante tal contingencia, tendremos que ser capaces, a pesar de todo, de seguir «jugando la partida»; sin interrumpirla nos adaptamos.

[2] *Panorama de tendencias geopolíticas. Horizonte 2040*. Ministerio de Defensa. Secretaría General Técnica, 2018. ISBN 978-84-9091-380-2

Las dimensiones múltiples del cambio

Desde el punto de vista de la teoría del arte militar, el «entorno operativo» se entiende como el tablero de juego del enfrentamiento militar, como el conjunto de elementos que participan en el enfrentamiento o que lo condicionan. Los avances técnicos y otros cambios que han llegado a lomos de dichos avances nos han llevado a identificar y definir nuevos espacios de confrontación, nuevos elementos del entorno operativo.

Los dominios y ámbitos no físicos de las operaciones son aspectos todavía novedosos[3], pero su preponderancia futura es innegable. Algunas doctrinas nacionales de nuestros aliados ya consideran las acciones kinéticas en el mundo real, la destrucción física y el movimiento, como actividades de apoyo a la maniobra de la información, que será el verdadero esfuerzo principal de las operaciones militares. El ciberespacio y el ámbito cognitivo centrarán, por tanto, gran parte de nuestra atención en las próximas décadas. La inteligencia deberá situarse —ya lo está haciendo, no sin cierta incomodidad inicial— en la frontera entre los dominios físicos y no físicos, manteniendo su capacidad de actuar en ambos y de integrarlos en su mirada y en su análisis.

Los avances en la tecnología y la importante aceleración en el desarrollo de viejas y nuevas tecnologías nos sorprenden cada día. Podemos imaginar que su impacto en las actividades militares y, en particular, en los procesos de inteligencia militar será muy importante en las próximas décadas. La conocida ley de Amara[4] nos avisa de que la tecnología y su impacto en nuestros procesos superará nuestras expectativas a medio y largo plazo. Podemos estar seguros de que el horizonte tecnológico de 2040 presentará para la inteligencia militar un panorama tan distinto del actual que quizá no baste con reformar «el edificio de la inteligencia». Es posible que necesitemos «construir uno nuevo».

[3] El ciberespacio no fue establecido oficialmente por la OTAN como dominio de las operaciones militares hasta la reciente Cumbre de Varsovia, 2016.
[4] «We tend to overestimate the effect of technology in the short run and underestimate in the long run» (Roy Charles Amara).

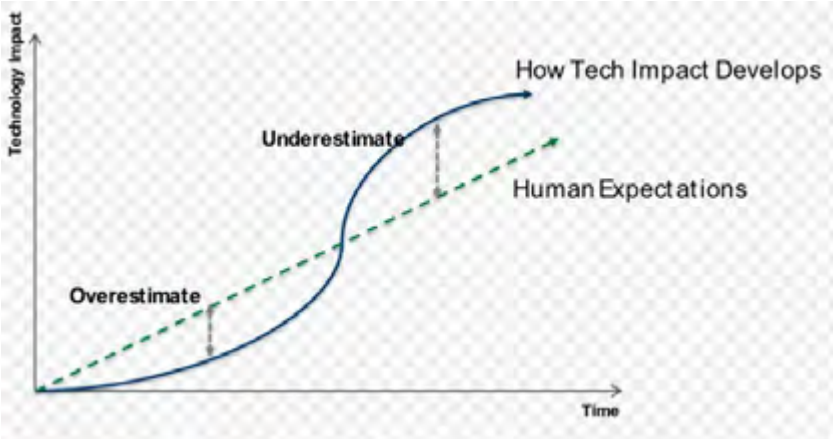

Figura 1. Ley de Amara.

El escenario geopolítico y de seguridad cambiará casi tan rápidamente como las tecnologías. Ya lo está haciendo y no deja de sorprendernos. Los cambios en curso y los que veremos en las próximas décadas nos obligarán a reorientar prioridades y modos de trabajar en la inteligencia militar y a vigilar aspectos y dimensiones que hemos desatendido hasta ahora. La pandemia por SARS-CoV-2 ya nos ha dado algunas pistas en ese sentido.

Además del cambio en los equilibrios del poder militar y en las dinámicas geopolíticas globales o regionales, habrá cambios también en la tipología de los conflictos para los que deberemos estar preparados. Algunos tipos de conflicto olvidados durante décadas, como el enfrentamiento simétrico (*peer-to-peer*) de alta intensidad vuelven a estar en el horizonte geopolítico. Ambos cambios considerados conjuntamente y unidos a escenarios novedosos de actuación de las FAS, en funciones de protección civil en apoyo a las autoridades civiles, configuran un variado catálogo de contextos operativos (CO). Estos diversos CO tendrán requerimientos nuevos en materia de inteligencia y exigirán de nuestra inteligencia militar un esfuerzo de adaptación que será mayúsculo en algunos casos.

También habrá cambios importantes en relación con los recursos humanos y el contexto sociocultural. Las personas han sido y seguirán siendo el elemento esencial de las FAS. Dejando de lado la demografía y su impacto cuantitativo en el problema de la generación y mantenimiento de fuerzas militares, el aspecto cualitativo también debe considerarse. Las nuevas generaciones, nativas digitales, tendrán dificultades para la comprensión del mundo físico. Sin embargo, el mundo físico y el enfrentamiento letal seguirán existiendo

a pesar de la preponderancia de la maniobra de la información. En casos extremos de enfrentamiento militar, la lucha en tierra, mar y aire será el elemento decisorio del resultado del conflicto. La capacidad para entender que los objetos representados en nuestras pantallas se corresponden con objetos reales del mundo y que los *trending topics* tienen detrás corazones y mentes de personas reales será una habilidad imprescindible para los futuros analistas de inteligencia, y parece claro que no la traerán «de serie» cuando se incorporen a las FAS.

La inteligencia militar 2040. Algunas líneas generales

La tecnología. Proveedora de soluciones y generadora de transformación

En el reciente documento *Science&Technology Trends 2020-2040. Exploring the S&T Edge*, la OTAN hace un interesante estudio de prospectiva tecnológica que orienta acerca de lo que podremos esperar de la tecnología en las próximas décadas.

Hay algunas áreas en las que se espera un desarrollo exponencial. Muchas de ellas tendrán gran impacto en la actividad militar en los próximos años y podrían agruparse, en base a su naturaleza, en cuatro grandes categorías: tecnologías inteligentes, tecnologías digitales, tecnologías distribuidas y tecnologías interconectadas[5].

La combinación de los avances en sistemas inteligentes y digitales nos llevará a progresos sorprendentes en la «batalla de la precisión», tanto en el ámbito de la obtención como en el del posicionamiento y la navegación. Las futuras redes serán digitales e interconectadas y con elementos de red distribuidos y expandidos hasta vincular los ámbitos cibernético, cognitivo y físico. En esta última dimensión serán importantes la implantación del IoMT (*internet of the military things*) y del D2D (*device to device communication*).

La combinación de tecnologías inteligentes y distribuidas llevará a una expansión sin precedentes de los sistemas autónomos; una autonomía que encontrará sus límites en las leyes o en la ética más que en las carencias, cada vez menores, de la tecnología.

Serán muchas las disciplinas que experimentarán un avance notable: ciencia de los datos, computación cuántica, inteligencia artificial, biotecnología, sistemas autónomos, espacio, velocidad hipersónica y los nuevos materiales. Las combinaciones de los

[5] Disponible en: https://www.sto.nato.int/pages/tech-trends.aspx (Fecha de la consulta: 20/2/2021).

avances en algunos de estos campos producirán efectos verdaderamente disruptivos en la inteligencia militar y propiciarán, incluso obligarán a cambios importantes en sus procesos y en sus organizaciones.

En el ámbito de las disciplinas de obtención los ejemplos del impacto de la tecnología son tantos que no hay espacio en estas breves líneas ni siquiera para una simple enumeración. Sí mencionaré, por ser un ejemplo paradigmático, cómo la disciplina más antigua y clásica de obtención, la inteligencia de fuentes humanas (HUMINT), se verá también afectada drásticamente. El HUMINT seguirá existiendo tal y como lo conocemos, pero se extenderá la interacción humana remota (cyberHUMINT), la traducción lingüística automatizada, la detección de la mentira por procesamiento de elementos biométricos o el perfilado indirecto de la personalidad de las fuentes humanas mediante el uso de la inteligencia artificial.

JADC2ISR[6], agilidad y transversalidad multidominio

La iniciativa JISR de la Alianza Atlántica (lanzada en la Cumbre de Chicago de 2012) ha mejorado las capacidades de la OTAN en el apoyo de inteligencia a las operaciones, en especial en relación con los eventos que requieren respuesta urgente y gran agilidad. Esto es especialmente visible en el ámbito de la contribución a la conciencia situacional en las operaciones en curso y en el *targeting*, singularmente el *time sensitive targeting*. Su efecto modernizador en la eficiencia y la interoperabilidad todavía no ha finalizado[7].

El ritmo de las operaciones seguirá previsiblemente creciendo y la necesidad de respuesta inmediata exigirá cada vez más eficiencia y agilidad de la inteligencia y del JISR, de sus organizaciones, de sus procesos, de las redes, de los servicios y de los sistemas funcionales. Además, el enfoque multidominio de las operaciones y la relación entre los dominios físicos y no físicos darán complejidad al reto y obligarán a reinventar el JISR[8]. Por ejemplo, los procesos de *X-cueing*[9] multidominio deberán implantarse para dar eficiencia a la parte dinámica de la conducción de las operaciones de ISR[10],

[6] JADC2ISR: Joint All Domain, Command, Control, Intelligence, Surveillance and Reconnaissance.
[7] La iniciativa JISR de la Alianza Atlántica alcanzó su IOC en 2015/16, pero no se ha establecido un objetivo de capacidades ni un horizonte temporal para una hipotética FOC.
[8] JADC2: Getting to Real-Time Object Data and Tracking in All Battlespace Domains. Disponible en: https://www.saic.com/blogs/jadc2/getting-to-real-time-object-data-tracking-from-all-battlespace-domains
[9] *X-cueing*: La activación dirigida de un medio de obtención (plataforma+sensor) durante la conducción de las operaciones de obtención ISR en base a la información obtenida por otro.
[10] El subproceso llamado *collection operations management* (COM), que forma parte del proceso JISR.

integrando la obtención en los dominios físicos y no físicos en un mismo sistema de gestión de las operaciones de obtención.

Nuevos contextos operativos. Nuevas amenazas

Los cambios en el entorno geopolítico obligarán a la inteligencia militar a mantener la capacidad para enfrentarse a una amplia variedad de amenazas y contendientes militares. El enfrentamiento se producirá en los diversos dominios físicos y no físicos y a lo largo del amplio espectro de los conflictos, en muchos casos sin abandonar la llamada «zona gris».

Algunas de las amenazas aprovecharán las oportunidades de los vastos espacios casi vacíos de gobernanza y de población del Magreb, Sáhara y el Sahel. La capacidad para la monitorización de estas zonas sin ocupación o con una muy baja densidad de ocupación militar dará más importancia, si cabe, a las actividades de inteligencia, vigilancia y reconocimiento. En este ámbito tendrán preponderancia, entre otros sistemas y disciplinas de obtención, los sensores de vigilancia de amplias zonas (WAS, por sus siglas en inglés), singularmente el GMTI[11] y los sensores que obtienen imágenes ópticas, infrarrojas o radar, embarcados en aeronaves con piloto a bordo, pilotadas remotamente o autónomas, así como los sensores terrestres desatendidos.

El contexto operativo del combate en áreas urbanas y suburbanas, en muchos casos incluso en megaurbes, obligará a nuevas técnicas, tácticas y procedimientos, y también a mirar ciertos aspectos con un enfoque renovado. Por poner solo un ejemplo, la información geográfica y de infraestructuras requerirá de una actualización en tiempo próximo al real para poder navegar entre obstrucciones y destrucciones en terreno urbano, así como para identificar obstáculos semipermanentes. La miniaturización de las tecnologías de barrido laser (LIDAR) embarcadas en pequeños RPAS será la solución a este reto y ya estará disponible en el horizonte temporal más inmediato. Estos sistemas permitirán también modelizar en 3D infraestructuras en cuyo interior vayan a desarrollarse operaciones.

[11] *Ground moving target indicator*.

El mapa de situación. La contribución de inteligencia a la COP

«Treat data as a strategic asset»[12]

La Common Operational Picture (COP) adquirirá una complejidad inusitada en las operaciones multidominio. El término recientemente acuñado *data based cop* hace referencia a un «mapa de situación» digital multicapa, configurable a demanda y capaz de ingerir y presentar un volumen descomunal de datos crudos, estructurados o desestructurados, con presentación infográfica automatizada, y también de objetos ya procesados. Las redes de alta capacidad darán conectividad a todo tipo de sensores atendidos y desatendidos en el entorno multidominio. La capacitación muy mejorada que proporcionará el IoMT/D2D y el 5/6G[13] serán artífices en gran medida de esta COP mejorada que será una superconsumidora de datos. Estos datos tendrán origen en proveedores y sensores no solamente militares.

La transmisión y el almacenamiento de datos y su explotación

El tráfico de datos que soportarán las futuras redes militares es difícil de estimar. La inteligencia futura, como la presente, será la comunidad operativa que más exija a las redes de comunicaciones en cuanto al intercambio y almacenamiento de información. Las plataformas sensorizadas con o sin piloto a bordo, autónomas o desatendidas (por ejemplo, RPAS-seudosatélites), los sensores terrestres o marítimos desatendidos, y muchos otros recursos de obtención en todos los dominios, producirán un volumen descomunal de datos. Nuestra capacidad de explotación y fusión se enfrentará a un reto. Mantener nuestra capacidad de ingestión y explotación a la altura de la demanda creciente generada por la ingente obtención será una de las claves del éxito en la futura inteligencia multidominio.

En su reciente e innovador documento *NATO guide to data collection and management for analysis support to operations*[14], la OTAN afirma que el dato no caduca jamás. Este incontestable postulado planteará un reto importante también para el almacenamiento

[12] US DoD Digital modernization strategy. 2019. Disponible en: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF (Fecha de la consulta: 24/2/2021).
[13] El 5G nos promete velocidades de hasta 20 Gbps; el 6G podría alcanzar 1 Tbps.
[14] TR-SAS-111 Science and Technology Organization, agosto de 2020. NATO UNCLASSIFIED.

de datos crudos o explotados en nuestros repositorios. Su capacidad deberá ser siempre suficiente para acoger ese flujo ininterrumpido y en constante crecimiento de datos e información entrantes, procedentes de todos los dominios y ámbitos del entorno operativo.

Otro aspecto interesante es la progresiva disolución de los límites, que una vez fueron rígidos, entre los niveles de conducción de las operaciones: estratégico, operacional, táctico. Esta evolución se dará de manera muy clara en la inteligencia militar y obligará a la completa conectividad entre redes y al completo acceso a los repositorios (con las salvedades de seguridad y necesidad operativa que se establezcan) desde todos los niveles[15].

Reservas de inteligencia e integración de dominios de seguridad

Hace ya varios años que la inteligencia militar ha comprendido la necesidad de afrontar el estudio del entorno operativo con un enfoque integral y una metodologia holística para descifrar su poliédrica complejidad. El nuevo entorno operativo multidominio no hace más que añadir complejidad a este reto.

En el pasado, tanto el acceso a la información como el conocimiento experto en las materias de interés para la inteligencia militar se encontraban predominantemente en el ámbito de las FAS. Hoy ya no es así, y en el futuro aún lo será menos. La inteligencia militar deberá integrar las capacidades existentes en otras organizaciones (las llamadas *reservas de inteligencia*) e incluso el conocimiento y el talento de individuos que trabajen en otros ámbitos de la Administración o fuera de ella.

Esto exigirá soluciones seguras para la interconexion entre las redes y dominios clasificados (con distintos niveles) y las redes no clasificadas, e incluso el Internet.

Deslocalización y esfuerzos federados

Existe una tendencia ya en curso de tratar de reducir nuestra huella sobre el teatro de operaciones, nuestra presencia física en el mismo. En aplicación del concepto *reachback*

[15] EVERSDEN, Andrew. «Army connecting tactical and enterprise networks for multidomain operations». Disponible en: https://www.c4isrnet.com/battlefield-tech/it-networks/2021/01/25/army-connecting-tactical-and-enterprise-networks-for-multidomain-operations/ (Fecha de la consulta: 19/2/2021).

ya se han trasladado fuera de las zonas de operaciones muchos elementos de análisis y de gestión de procesos y subprocesos del ciclo de inteligencia y del proceso JISR. Esta tendencia crecerá en el futuro, con unidades de gestion de la obtención, así como de procesamiento, explotación de JISR y de fusión de inteligencia, separados fisicamente de las unidades de obtención desplegadas en la zona de operaciones. Para ello, se requerirán soluciones técnicas robustas que aseguren la disponibilidad del apoyo y la continuidad del flujo de datos.

Inteligencia e influencia

> «We are good at killing terrorists or kinetic actions. However, we fail to realize that we can't kill an idea»[16]
>
> *The cognitive war*, Edward L. Haugland

En las nuevas batallas en el dominio cognitivo, necesariamente sincronizadas con las acciones en el mundo físico, la inteligencia militar deberá ser un importante contribuyente a la nueva función conjunta información. En realidad, siempre lo ha sido, aunque nadie en el pasado hubiera definido la función conjunta información ni el ámbito cognitivo de las operaciones. Como afirma la RAND Coorporation en un reciente documento de análisis[17], las operaciones de información y la inteligencia han sido siempre parte esencial de las operaciones militares, y la «información», en su aceptación semántica genérica, ha sido y es la esencia de ambas comunidades.

La contribución de JISR e inteligencia a las acciones de influencia/*targeting* no letal (*influence artillery rounds*[18]) responderá a una lógica similar al *targeting* letal, pero adquirirá una complejidad mucho mayor. El desarrollo de capacidades en este campo y de procedimientos de colaboración sinérgica entre las comunidades de inteligencia y de información/influencia exigirá un gran esfuerzo de modernización creativa. Los procesos de inteligencia y su sincronización con la nueva comunidad operativa de influencia

[16] «Future military intelligence CONOPS and S&T investment roadmap 2035-2050. The cognitive war». Edward L. Haugland (US Army Intelligence/DA DCS G2). 2019. Disponible en: https://nsiteam.com/future-military-intelligence-conops-and-st-investment-roadmap-2035-2050-the-cognitive-war/ (Fecha de la consulta: 17/2/2021).
[17] «Intelligence support to operations in the information environment», RAND Corporation 2020. Disponible en: https://www.rand.org/pubs/research_reports/RR3161.html (Fecha de la consulta: 28/1/2021).
[18] POMERLEAU, Mark. «Special Forces to build "influence artillery" for online campaigns». Disponible en: https://www.c4isrnet.com/information-warfare/2021/02/18/special-forces-to-build-influence-artillery-for-online-campaigns/ (Fecha de la consulta: 18/2/2021).

deberán revisarse buscando la sinergia eficiente entre ambas comunidades. En este caso, como ocurre en general entre áreas y procesos confinantes, sus límites borrosos e imprecisos plantean un gran reto. Un doble reto: deben evitarse duplicidades de esfuerzo y también el riesgo de desatender ciertas áreas o aspectos. La coordinación, división de funciones, intercambio fluido de información y la evitación de planteamientos de competencia entre ambas comunidades deben ser la base de la cooperación sinérgica entre las comunidades operativas de inteligencia e influencia/información.

La explotación, fusión y producción de inteligencia. Los procesos analíticos

Nadie duda que la computación cuántica y la inteligencia artificial sacarán buen provecho del flujo masivo de datos procedentes de la obtención en JISR y de otras muchas fuentes. Los procesos de correlación, fusión y análisis se verán transformados, automatizados. Los servicios funcionales avanzados para apoyar los procesos analíticos y la nueva relación, cada vez más próxima al lenguaje natural, entre el analista y los repositorios de información llevarán a un nuevo modo de producir inteligencia. Se configurarán verdaderos equipos hombre-máquina en los que la base de datos, más que una herramienta, será un compañero del ser humano, la mitad de ese binomio[19].

Un aspecto interesante a este respecto tiene que ver con la función predictiva de la inteligencia y la capacidad de anticiparse. Nuestros algoritmos serán capaces de predecir la acción enemiga mejor que los métodos analíticos analógicos que conocemos. Como contrapartida, nuestros oponentes y también nosotros mismos, desarrollaremos mecanismos de «camuflaje algorítmico». Así, de modo análogo a como nos ocultábamos de las vistas en el mundo físico, trataremos también de ocultarnos de la predicción algorítmica en el mundo de los datos. La sorpresa se buscará mediante las actuaciones tan irracionales o lejanas de los patrones al uso, que resulten impredecibles para el algoritmo.

[19] «Human-machine teaming (JCN 1/18)». Disponible en: https://www.gov.uk/government/publications/human-machine-teaming-jcn-118.(Fecha de la consulta: 25/1/2021).

La difusión

Las fases de difusión del ciclo de inteligencia o del proceso JISR ya están en pleno proceso de modernización. Los cambios continuarán en este campo.

La difusión es y será una de las grandes beneficiarias de los avances en sistemas de información y telecomunicaciones. Los más veteranos en las Fuerzas Armadas recordamos una difusión basada en la remisión de productos de inteligencia que incluso se explotaban en papel en la mayor parte de los casos. Además, se distribuían con criterios bastante rígidos, a través de la cadena de mando. Las cosas han cambiado y lo harán mucho más aún para esta fase final del ciclo de inteligencia y del proceso JISR, una fase de apariencia banal, pero mucho más importante y compleja de lo que a menudo se pueda pensar.

La difusión evoluciona hacia un nuevo paradigma. La distribución de los datos, de la información explotada, de los productos de inteligencia y también de los objetos para enriquecer la representación del entorno operativo en las COP y en los sistemas de mando y control, los llamados *battle space objects* (BSO), serán objeto de atención y tratamiento automático, pero singularizado. La difusión se adaptará cada vez más a las necesidades singulares de cada usuario y de cada proceso consumidor, y se gobernará en base a perfiles que contemplen sus necesidades (no solo su necesidad genérica de conocer), así como su capacidad de ingestión de inteligencia o de información explotada del proceso JISR.

Uno de los grandes retos en la difusión es la extensión de los servicios avanzados de Intel y JISR a los niveles tácticos inferiores, por ejemplo, los servicios de vídeo *streaming*. En el futuro, las pequeñas unidades en el nivel táctico tendrán acceso a muchos de los repositorios de datos y a la parte de la COP que sea relevante para la ejecución de su operación. Las gafas con *display* holográfico y otros dispositivos tecnológicos permitirán tener acceso, en una sola mirada, al terreno real, a los elementos del planeamiento y a la inteligencia relevante para la operación, así como a las notificaciones urgentes recibidas durante la conducción, incluida la llamada *time sensitive intelligence*.

La velocidad de los ciclos de decisión, el requerimiento de inmediatez en los procesos operativos urgentes (*time sensitive targeting*, *time-sensitive-actionable-intelligence driven operations*) requerirá de concisión en la difusión. La nueva cultura de la brevedad y la inmediatez que está configurando el intelecto de las nuevas generaciones subrayará

más aún, si cabe, esta necesidad. Las infografías, la realidad aumentada o los hologramas darán posibilidades inimaginables a la fase de difusión del ciclo de inteligencia y del proceso JISR.

El viejo cajón de arena será sustituido por realidades virtuales altamente inmersivas para los ensayos de misión. Las sorpresas y la incertidumbre ante la entrada en terrenos o infraestructuras desconocidas se reducirán al máximo.

Control de calidad y análisis de efectos

Los procesos en inteligencia y JISR deberán establecer mecanismos para la valoración de la calidad de la producción y su impacto en los procesos consumidores de la misma. La evaluación de la «estrategia» en Intel y JISR —de los fines, de los modos y de los medios— debe permitir mejorar su contribución a los procesos operativos apoyados, a las autoridades que deciden en base a dicha inteligencia y, en ultimo término, al éxito de la acción militar. Dicha evaluación deberá ser continua y alimentarse de numerosos indicadores que serán procesados con las nuevas herramientas proporcionadas por la ciencia de los datos, la computación avanzada y la inteligencia artificial.

Contrarrestando la asimetría legal y ética

Sin menoscabo del respeto del Estado de derecho y, singularmente, de la salvaguarda de los derechos individuales de los ciudadanos, nuestra sociedad, y en particular nuestra inteligencia militar, deberá dotarse del marco normativo adecuado para el conflicto multidominio. No hay duda de que en el manejo de datos y en la actuación sobre los vectores del ámbito cognitivo, nuestros enemigos previsibles tendrán menos limitaciones éticas y legales que nosotros. Esta situación podría llevar a perder las batallas antes de librarlas si no nos dotamos de las adecuadas herramientas legales.

Capacidad de adaptación frente al futuro VUCA[20]

El desarrollador de software Eric S. Raymond formuló en su libro *The Cathedral & the Bazaar*[21] una atractiva teoría en relación con su trabajo. Sostiene Raymond que los grandes proyectos deben concebirse, diseñarse y ejecutarse más como un bazar árabe, turco o persa que como una catedral gótica.

La catedral gótica se diseña y después se inicia su construcción, para finalizarla mucho tiempo después. El diseño es sólido, bello y adaptado al requerimiento inicial, pero normalmente la propia perfección y rigidez del proyecto impide su modificación cuando, con el proyecto ya en ejecución, el tiempo nos lleva a desear que el resultado final sea distinto del originalmente concebido[22]. Un bazar, por el contrario, se establece en base a unas pocas líneas organizativas y urbanísticas generales que permiten añadir y quitar, modificar y reconfigurar la idea inicial según continúa el establecimiento del bazar e incluso cuando ya está en funcionamiento.

Esta filosofía de adaptabilidad a los cambios debe también regir el proceso de modernización de nuestra inteligencia militar. El postulado de Raymond, concebido para los desarrollos de software, pudiera y debiera aplicarse también a la redefinición de nuestros procesos operativos y de nuestras arquitecturas organizativas y de sistemas. Solo así podremos satisfacer con éxito los nuevos requerimientos que traerá el futuro. Estos requerimientos no serán inmutables porque, como todos sabemos, el futuro es un objetivo en movimiento.

*Ángel Segundo Gómez González**
Cor. ET. Director Departamento de Inteligencia
Escuela Superior de las FAS

[20] VUCA: *volatility, uncertainty, complexity and ambiguity*. Acrónimo propuesto por el US Army War College para recoger las características de los entornos como al que nos enfrentamos actualmente, y más aún a su previsión de evolución futura.
[21] ISBN 1-565-92724-9.
[22] Disponible en: https://www.ileon.com/actualidad/101091/la-cupula-que-casi-derrumba-la-catedral-de-leon-y-la-convirtio-hace-175-anos-en-el-primer-monumento-nacional-de-espana (Fecha de la consulta: 20/2/2021).