La inteligencia en la guerra de Ucrania Observaciones preliminares

Ángel Segundo Gómez González

«We are witnessing the ways wars will be fought, and won, for years to come»[1]
Gen. Mark A. Milley, chairman of the US Joint Chiefs of Staff

«The power of advanced algorithmic warfare systems is now so great that it equates to having tactical nuclear weapons against an adversary with only conventional ones»[2]
Alex Karp, chief executive of Palantir

Resumen

La invasión de Ucrania por parte de Rusia se presenta como un «escaparate» de tendencias en todos los niveles de conducción de la guerra y en todas sus áreas funcionales y dominios de las operaciones. La inteligencia se está mostrando como una función clave en la que además observamos tendencias e incluso posibles cambios importantes. Su observación y análisis reviste el máximo interés. Es prematuro realizar un análisis profundo acerca de esta materia, pero ya pueden hacerse algunas observaciones que merecerán un análisis más profundo en el futuro. Este es el propósito de este modesto artículo.

Palabras clave

ISR atípico, inteligencia colectiva, X-cueing (activación dirigida de sensores), multidominio, configuración del entorno, disuasión, influencia, disuasión.

Intelligence in the Ukrainian War

Preliminary observations

Abstract

Russia's invasion of Ukraine can be seen as a 'showcase' for trends at all levels of warfare, in all its functional and operational domains. Intelligence is proving to be a key function in which we can observe trends and possibly even major changes. Its monitoring and analysis is of paramount interest. It is still too early to make an in-depth analysis of the subject, but

[1] Ignatus, D. (2022). How the algorithm tipped the balance in Ukraine. *Washington Post.*
[2] *Idem.*

some observations can already be made that will certainly merit further analysis in the future. This is the purpose of this modest article.

Keywords

Non-traditional ISR, crowdsourcing intelligence, X-cueing, multidomain, environment shaping, deterrance, influence, declassification.

1. Introducción

Nadie duda de la importancia de la inteligencia y la contrainteligencia para tener éxito en los ámbitos de la seguridad y la defensa y en particular en la guerra, en sus campañas y en sus batallas. También es conocido que la historia está llena de sonados fracasos político-diplomáticos, estratégicos, operacionales y tácticos que pueden atribuirse a una inteligencia escasa, de mala calidad, mal comunicada y/o mal trasladada a las decisiones de la acción ofensiva o defensiva.

Cuando esto ocurre, cuando puede atribuirse a la inteligencia a cualquier nivel una parte de la «culpa» en el fracaso, el análisis crítico de sus organizaciones, de sus procesos y actividades, de la calidad de sus productos y de cómo y a quién se difunden, es imprescindible para mejorar. Por eso, las organizaciones de inteligencia deben dotarse de mecanismos de control de calidad y valoración del desempeño de sus distintos elementos y componentes, pero también de procesos que permitan medir su efectividad, el grado en que contribuyen a alcanzar el éxito, a reducir el impacto de las situaciones desfavorables o a neutralizar las amenazas. Frecuentemente, hacen lo primero basado en los MOP[3]. Lo segundo (basado en los MOE[4]) es en gran medida una asignatura pendiente. En ambos casos, además de herramientas metodológicas, se requiere una sólida cultura de la autocrítica que no siempre está presente.

En el ámbito académico y profesional anglosajón se usa el término *post mortem* para referirse a los estudios retrospectivos, muy frecuentes y útiles en el ámbito de la inteligencia. Estos estudios se desarrollan cuando teóricamente ya están todas las *cartas sobre la mesa*, una vez pasada la crisis o finalizado el conflicto. Ofrecen grandes posibilidades para el análisis y la identificación de errores y también, en algunos casos, de buenas prácticas que interesa replicar en el futuro. En España tenemos poca tradición de estudios académicos sobre inteligencia. Menos aún de *post mortems*, en el ámbito de las ccomunidades de inteligencia, acerca de nuestras propias crisis u operaciones y, aún menos, sobre aquellas relativamente recientes. Es cierto que estos estudios se ven limitados por el difícil acceso a documentos, a menudo clasificados e incluso no disponibles por haber sido destruidos, pero también —por qué no reconocerlo—, por la falta de espíritu autocrítico. No tan efectivo, pero mucho más fácil, es tratar de aprender de los errores y aciertos ajenos y en esos casos la falta de autocrítica no suele

[3] *MOP: Measures of performance*. Indicadores medibles de la calidad de los procesos y de la de los resultados de los mismos, incluida, especialmente en el caso de la inteligencia, la propia calidad de los productos.

[4] *MOE: Measures of effectiveness*. Indicadores del grado de contribución de nuestros procesos a la consecución de los objetivos de la organización.

ser un factor limitante. La guerra de Ucrania ofrece una magnífica ocasión para ello.

Por definición, un estudio de inteligencia *post mortem* debe realizarse cuando la operación o crisis haya finalizado, cuando el *muerto* ya esté frío, cuando los *futuros* a los que se referían las previsiones y los análisis de inteligencia ya formen parte del pasado.

La guerra en curso en Ucrania puede considerarse un campo de pruebas[5], un *escaparate* de tendencias en muchos aspectos y singularmente en relación con la inteligencia. Su análisis es, por lo tanto, de máximo interés. Los aciertos y errores de los beligerantes y de los que les apoyamos; en general todo lo que observamos en el conflicto y en torno a él, puede enseñar mucho y mostrar elementos de un camino por el que previsiblemente transitaremos en el futuro.

Por desgracia la guerra continúa y es, por tanto, muy prematuro acometer cualquier estudio profundo al respecto. Al intentar un modesto análisis, como el que propone este artículo, debemos asumir que será parcial y muy condicionado por la niebla cognitiva que envuelve, no solo a los beligerantes, sino también a los observadores externos de la guerra. Una *niebla* agravada por el *ruido de fondo* infodémico que limita nuestra capacidad para verlo todo, para identificar qué es lo importante de aquello que vemos y de lo que no vemos y, más aún, para alcanzar una buena conciencia y comprensión de todo ello y de lo que significa.

Sin embargo, y a pesar de las limitaciones citadas, el análisis del papel y de la actuación de la inteligencia en y en torno a la Guerra de Ucrania y en el proceso que llevó a la invasión del 24 de febrero, son del máximo interés. Con todos los reparos que imponen las consideraciones anteriores y con plena conciencia del carácter limitado de este estudio, pueden, no obstante, hacerse ciertas observaciones que ya merecen una reflexión inicial y ese es el propósito de este breve trabajo.

2. Uso atípico de la inteligencia (audiencias, finalidades)

> «We've been transparent with the world. We've shared declassified evidence about Russia's plans and cyberattacks and false pretexts so that there can be no confusion or cover-up about what Putin was doing. Putin is the aggressor. Putin chose this war. And now he and his country will bear the consequences»[6] president Joe Biden.

[5] Brennan, D. (2022). Russia-Ukraine Cyber War Is 'Test Ground' for NATO. *Newsweek* 90. Disponible en: https://www.newsweek.com/russia-ukraine-war-cyberattack-test-ground-nato-eu-hackers-1745309

[6] *The White House*. (2022). Remarks by President Biden on Russia's Unprovoked and Unjustified Attack on Ukraine. East Room. Disponible en: https://www.whitehouse.

«Over-classification undermines critical democratic objectives, such as increasing transparency to promote an informed citizenry and greater accountability»[7] Avril Haines, directora nacional de Inteligencia EEUU

La inteligencia, como es bien sabido, está primordialmente orientada a la generación y difusión de comprensión acerca del entorno y valoraciones sobre las amenazas que comporta y sobre su posible evolución futura. El destinatario, el consumidor, de dicho conocimiento es normalmente la propia organización o Estado en beneficio de su acción (política, diplomática, militar) en los distintos niveles del diseño, planeamiento y conducción de la acción.

Sin embargo, este modelo no es único. Más aun, como veremos más adelante, en el camino que llevó a la invasión del 24 de febrero y en la subsiguiente guerra de Ucrania, se han podido observar, con gran frecuencia e intensidad, otros patrones que merecen una reflexión. Algunos analistas sugieren incluso que se está produciendo un cambio de paradigma en el uso que hacen los decisores de la inteligencia y en la relación de la inteligencia con el entorno.

La difusión de inteligencia a audiencias distintas de la genérica mencionada en el primer párrafo de este apartado no es nueva[8] [9] [10] [11], pero en torno a la guerra de Ucrania este fenómeno ha alcanzado cotas nunca antes vistas[12]. La difusión citada no tiene como finalidad, en esos casos, que las pro-

---

gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/

[7] *Nextgov*. (2023). The National Intelligence Director: Over-Classification Undermines Democracy. Disponible en: https://www.nextgov.com/cxo-briefing/2023/01/national-intelligence-director-over-classification-undermines-democracy/382367/

[8] *FOIA*. (2016). *The role of intelligence during the Cuban missile crisis*. General CIA Records. Disponible en : https://www.cia.gov/readingroom/document/cia-rdp-85g00105r000100040005-5

[9] SNIE. (1962). *The military build up in Cuba*. Disponible en: https://www.cia.gov/readingroom/docs/DOC_0000242425.pdf

[10] *Timegoggles*. (2019). Photos from history: Presence of Soviet missiles in Cuba triggers crisis. Disponible en: https://timegoggles.com/news/archives/photos-from-history-presence-of-soviet-missiles-in-cuba-triggers-crisis/collection_0fa1acc4-ef67-11e9-8a8f-570537186298.html#10

[11] Dilanian, K. et *al*. (2022). In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid. *NBC news*. Disponible en: https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014

[12] [1]2 *CNAS* (2022). War in Ukraine: Declassifying Intel. «The declassification of intelligence before and after the Russian invasion of Ukraine was unprecedented in its speed, and lauded for its accuracy. Releasing the intel has been credited with stopping the spread of Russia's false justification for launching an invasion, but in the end did not deter Russia from starting a war with its neighbor. A panel of intel experts gather to

pias decisiones sean más correctas para mejorar las opciones de éxito en la acción. Busca, por el contrario, influir en el entorno, configurarlo en nuestro beneficio y en último término, contribuir así también indirectamente al éxito.

Podemos identificar distintas modalidades de esta difusión configuradora del entorno y todas ellas han sido visibles en los últimos meses en torno a la escalada previa, a la propia guerra de Ucrania y al contexto geopolítico en que se desarrolla.

En primer lugar, la difusión puede hacerse para influir en actores amigos o aliados. Esta difusión normalmente busca el acercamiento de las posiciones de otros actores a las propias para recabar apoyos o dar solidez a una posición política o a un planteamiento estratégico común. Así lo hizo la inteligencia norteamericana en 2003 para buscar apoyo a su posición sobre Irak[13] y contribuir a la formación de una gran coalición internacional. Un patrón análogo se ha observado en torno a Ucrania en los últimos meses.

Con la difusión se puede también intentar influir análogamente en actores neutrales externos, buscando su apoyo o el mantenimiento de su neutralidad.

En el marco de la batalla por los *corazones y las mentes*, la difusión también puede dirigirse a la población para conformar el campo de batalla cognitivo y alcanzar no solo la *information superiority* (función clásica de la inteligencia) sino también la *narrative superiority* mediante el reforzamiento de la credibilidad de nuestros mensajes.

Queda por citar en último lugar uno de los casos más interesantes: la difusión dirigida al enemigo, a sus dirigentes, para modelar sus decisiones. En este caso, se trata de configurar la conciencia situacional y las valoraciones del liderazgo adversario con fines disuasorios o bien para intentar que incurra en errores a nuestra conveniencia. El caso más habitual es la difusión disuasoria basada en el simple y poderoso mensaje subyacente de *no hagas lo que estás pensando hacer porque ya sé que estas a punto de hacerlo*[14]. También puede intentar promoverse, mediante un mecanismo análogo, la actuación enemiga en una dirección que pueda llevarle al fracaso o a una sobreactuación de la que se deriven beneficios políticos o militares para el difusor de dicha inteligencia.

---

discuss the process of declassification, and the impact it has played in the Russian war». Disponible en: https://conference.cnas.org/session/declassifying-intel/

[13] *History* (2023). Secretary of State Colin Powell speaks at UN, justifies US invasion of Iraq. Disponible en: https://www.history.com/this-day-in-history/secretary-of-state-colin-powell-speaks-at-un-invasion-of-iraq

[14] Nowroozi, K. (2022). Intelligence Sharing as A Deterrent and A Method of Warfare. *Security and Politics*. Disponible en: https://kavon.substack.com/p/intelligence-sharing-as-a-deterrent

No hay duda de que en las semanas anteriores al inicio de la invasión y también después de la misma, las distintas inteligencias nacionales — la norteamericana, británica, rusa y ucraniana—, han hecho un amplio uso de estas metodologías. Lo han hecho para, según los casos, buscar el apoyo de aliados, recabar apoyo de la propia población rusa a la invasión, fortalecer el espíritu de resistencia de la población ucraniana, fomentar el apoyo militar y otros tipos de ayuda a Ucrania, disuadir a Rusia de actuar militarmente contra Ucrania (antes de la invasión) y a China y a otros estados de dar una apoyo abierto e incondicional a Rusia —sobre todo después de la invasión y hasta la fecha—, contribuir a la cohesión de la posición europea y de su convergencia con la anglo-norteamericana, etc.

Es cierto que la difusión de inteligencia de acuerdo con estos modelos no es nueva. Resulta fácil identificar ejemplos de ello en el pasado. Sin embargo, no es menos cierto que nunca antes en la historia se había producido un volumen de desclasificación de inteligencia para su difusión comparable al de la guerra de Ucrania[15].

Se puede decir que en torno a la guerra de Ucrania se está observando un uso muy abundante de la inteligencia con fines que se podrían llamar «atípicos» y quizás se esté consolidando una tendencia de cambio de paradigma en la difusión de la inteligencia. Una tendencia que acerca la inteligencia al ámbito de la comunicación estratégica, que sustituye, en ciertos casos, las paredes blindadas de los archivos de inteligencia por *escaparates transparentes*. Una tendencia que vincula la búsqueda de la superioridad en el conocimiento de la situación a la superioridad en la confrontación de narrativas.

Estos *usos atípicos* de la difusión de inteligencia e incluso de su producción *ad hoc* en beneficio de la influencia orientada a la decepción, a la disuasión, al fortalecimiento de la cohesión o a cualquier otra finalidad, no deben desdeñarse. Probablemente han llegado para quedarse. Sin embargo, este asunto requiere reflexión, desarrollo conceptual y procedimental. Cuando se acometa esta tarea deberán considerarse, entre otros aspectos, los riesgos colaterales de la sobredifusión que también se recogen de forma superficial más adelante en este documento y que se deben aprender a valorar adecuadamente[16] [17].

---

[15] Harrington, J. (2022). Intelligence disclosures in the Ukraine crisis and beyond. *War on the rocks*. Disponible en: https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/

[16] CIA. Conferencia de Marzo de 1954 sobre «Dissemination of intelligence» (Approved for release CIA-RDP78-033662A0007000330001-8). Disponible en: https://www.cia.gov/readingroom/docs/CIA-RDP78-03362A000700030001-8.pdf

[17] *Firstpost*. (2022). Explained: The risks countries are facing for sharing intelligence inputs over the Ukraine war. Disponible en: https://www.firstpost.com/explainers/explained-the-risks-countries-are-facing-for-sharing-intelligence-inputs-over-the-ukraine-war-11341881.html

Una variante a esta difusión atípica de inteligencia producida con rigor sobre la base de las informaciones obtenidas y evaluadas con los procesos y los estándares de calidad requeridos, es la *fabricación* de *inteligencia* completamente desvinculada de la realidad, de la verdad. Esta *fabricación* puede hacerse con algunos de los fines mencionados anteriormente: influir en aliados, disuadir a enemigos, configurar el entorno cognitivo para alcanzar la superioridad en la narrativa,... Es cierto que en sentido estricto esa *inteligencia* no merece siquiera tal denominación, pero no deja de tener relación con el tema de este artículo. Además, esta práctica más allá de si encaja taxonómicamente o no en esta categoría, o si más bien debemos considerarla solo como desinformación, ha sido ampliamente empleada por Rusia, y probablemente no solo por Rusia en este conflicto[18] [19]. Lo cierto es que esta *fake intelligence* contamina e interactúa —distorsionándolo— con el ciclo de inteligencia del adversario y, en todo caso, añade *niebla* a la *niebla de la guerra*.

3. Los vectores de la difusión

Cuando hablamos del uso habitual, canónico, de la inteligencia, no tiene mucho sentido utilizar el término vectores que aparece en el título de este párrafo. Los sistemas nacionales de inteligencia y de seguridad nacional, así como las organizaciones de inteligencia internamente, disponen de canales para ordenar sus flujos de trabajo y de difusión de inteligencia.

Cuando hablamos del resto de los casos, sí que se observa una variedad de canales e incluso vectores indirectos de difusión que merecen un comentario.

El proceso parte siempre de una decisión de difundir algo con una finalidad y para ello, se deben desclasificar o reclasificar productos de inteligencia o de la información que contienen. A partir de ahí, por supuesto, existen canales formales, y en muchos casos permanentemente operativos, para el intercambio bilateral o multilateral de inteligencia entre países y también existen herramientas para los intercambios discretos. En el caso de los países aliados que comparten pertenencia a organizaciones internacionales de seguridad y defensa, este intercambio es rutinario y se apoya en mecanismos muy sólidos y permanentes.

En otros casos, los productos de inteligencia y más frecuentemente la información que contienen, o parte de ella, es transferida a los canales de

[18] *Felgenhauer*, P. (2017). Russian Military Spreads Fake Intelligence. The Jamestown Foundation. Disponible en: *https://jamestown.org/program/russian-military-spreads-fake-intelligence/*

[19] *Ukrinform*. (2022). Russian intelligence creates fake website to discredit Zelensky. Disponible en: https://www.ukrinform.net/rubric-polytics/3566988-russian-intelligence-creates-fake-website-to-discredit-zelensky.html

la comunicación pública a través de las notas o declaraciones oficiales de los departamentos de comunicación u oficinas de prensa de los organismos gubernamentales.

El paradigma que describe el párrafo anterior lleva la difusión al ámbito resbaladizo en el que las acciones de influencia encuentran sus *municiones* cognitivas en la inteligencia. Ese es también es el caso que observamos cuando se utilizan vectores de difusión no convencionales ni formales al servicio del propósito de esas acciones difusoras *atípicas*. Un caso paradigmático, y sin duda el más frecuente en este ámbito, es el del periodista que publica sus crónicas o valoraciones empezándolas con la clásica frase: «según fuentes de la inteligencia de...»[20]. A veces esta transferencia, aunque sea intencional, se disfraza de fuga de información o de indiscreción. Puede ocurrir que esos periodistas sean conscientes de ser una pieza de un mecanismo atípico de difusión de inteligencia para la influencia. Sin embargo, en muchos otros casos. quizás sean completamente inconscientes de ello y se sientan afortunados de la ocasión de *brillo* profesional que les brindan *sus fuentes*. El resto del *trabajo* lo harán los medios de comunicación y su habitual tendencia a la redifusión con efecto de eco multiplicador en esa caja de resonancia mediática que es el entorno de la información.

4. Los riesgos de la sobredifusión

El citado uso atípico de la inteligencia tiene mucha capacidad para la configuración del entono del conflicto, pero, sin duda, comporta también riesgos que pueden llegar a desaconsejarlo y que, en todo caso, deben ser valorados convenientemente.

En primer lugar, hay un riesgo evidente: la transferencia de productos de inteligencia de los canales reservados al acceso público, los pone en conocimiento de nuestros oponentes que pueden adaptar en consecuencia sus *modus operandi*, sus técnicas, tácticas y procedimientos. El impacto de este fenómeno es especialmente importante en relación con las acciones de nuestros enemigos o competidores para protegerse de nuestras actividades de obtención. En algún caso, puede llegar a resultar en la neutralización de fuentes de obtención de información o en la reducción de la eficacia operativa de determinadas técnicas, tácticas y/o procedimientos de obtención.

La difusión de lo que sabemos acerca de los planes del enemigo realizada con intención disuasoria pudiera también, en algún caso, generar paradójicamente el efecto contrario. Producir una aceleración de su acción al verse apremiado por el aparente buen progreso de nuestra conciencia situacional

[20] Marinho, J. (2016). Journalists and Intelligence Services. *Marinho Media Analysis*. Disponible en: http://www.marinho-mediaanalysis.org/articles/Sep-02-2016/journalists-and-intelligence-services

acerca de sus intenciones. Esta dinámica de respuesta en nuestro adversario, que responde a la lógica «cuanto más esperemos, peor será», puede en ciertos casos desencadenar inmediatamente aquello que se estaba tratando de impedir mediante la difusión disuasoria de inteligencia.

Otro riesgo tiene que ver con la lógica de que cuando ya se han mostrado las cartas no hay margen para elegir cómo continuar la partida. Hacer público el propio conocimiento sobre ciertos aspectos de nuestro oponente y de sus planes o sus acciones reprochables, condiciona a nuestro enemigo, pero también puede limitar nuestras propias opciones de negociación, de desescalada, de disuasión ulterior, de decepción... En ciertos casos podemos llegar a ser esclavos de nuestra propia difusión.

Por último, hay un riesgo relacionado con el conocido fenómeno de la *self negating prophecy*, versión en negativo del aún más famoso *self fulfilling prophecy*[21].

En ocasiones la difusión disuasoria («no lo hagas, ya sé lo que estas preparando») puede alcanzar el efecto que busca, que, sin duda, puede considerarse un éxito operativo. Sin embargo, a los efectos de la valoración *post mortem* de la efectividad de la inteligencia y su impacto en su prestigio y credibilidad, los vaticinios incumplidos podrían simplemente ser vistos como predicciones excesivamente desfavorables («veis como no ha pasado nada»), un caso más del *típico* exceso de dramatismo de la comunidad de inteligencia en sus estimaciones sobre la amenaza y las líneas de acción del enemigo.

Tristemente, serán pocos los que piensen que esa difusión en concreto pueda haber sido la que haya evitado que ocurriera aquello de lo que se alertaba. La mayoría tenderá a creer que se ha tratado de un simple vaticinio que no se ha cumplido, con la erosión que esto tiene siempre sobre el prestigio y credibilidad de las organizaciones de inteligencia. Se trata de un dilema en el que deberán valorarse beneficios y perjuicios para buscar soluciones de compromiso y, en algún caso, aceptar posiciones extremas si el balance ventajas-inconvenientes resulta favorable.

5. El prestigio y la credibilidad

> «Mistrust in intelligence has serious consequences for the effectiveness of intelligence agencies[22]».

[21] Cole, N. L. (2019). Definición de profecía autocumplida en sociología». *Greelane*. Disponible en: https://www.greelane.com/es/ciencia-tecnolog%C3%ADa-matem%C3%A1ticas/ciencias-sociales/self-fulfilling-prophecy-3026577/

[22] Matei, F. C. y Halladay, C. (2019) The conduct of intelligence in democracies: Processes, practices and cultures. ISBN 978-1-62637-769-1. Disponible en: https://www.tandfonline.com/doi/full/10.1080/23800992.2019.1695719

Uno de los procesos más importantes y conocidos del ciclo de inteligencia es el de valoración de la credibilidad de las informaciones obtenidas y de la fiabilidad de las fuentes de información.

Hay otro asunto que normalmente no se considera de manera sistemática, ni lo recogen nuestros procedimientos ni hay métodos para su cuantificación, pero que también merece ser considerado. El prestigio y credibilidad de los analistas, de los oficiales responsables de inteligencia, y hasta el de cada organización de inteligencia en su conjunto, es asimismo objeto de valoración, aunque sea de manera espontánea e informal. Esta valoración se basa en la calidad del desempeño, pero, sobre todo, en lo que mejor puede observarse, su historial de éxitos o fracasos.

La credibilidad que se dé —en su propia organización— a los asesoramientos, a las valoraciones, juicios y recomendaciones de la inteligencia procede, sin duda, de lo que contengan los productos de inteligencia y del rigor en la aplicación de las metodologías de valoración de credibilidad y fiabilidad. Sin embargo, también depende, en gran medida, de algo tan subjetivo como es el prestigio y la credibilidad del propio analista y del oficial responsable de inteligencia. Este prestigio, y el crédito asociado al mismo, pueden atribuirse asimismo a las organizaciones o estados y de él depende, en gran medida, que las valoraciones y los consejos que explícita o implícitamente contengan dichos productos sean considerados y trasladados a la acción.

Es por ello que el prestigio de las organizaciones de inteligencia y el de sus componentes individuales debe cuidarse como un valioso bien a proteger. La guerra de Ucrania y las fases anteriores al inicio de la invasión ha dado ejemplos de lo difícil que resulta *limpiar* las manchas del pasado en el *expediente*, en el *historial* de los estados y de sus organizaciones de inteligencia y como estas afectan a su credibilidad en el presente. La dificultad encontrada por la inteligencia norteamericana y británica para que sus valoraciones fueran compartidas por algunos aliados en las semanas anteriores a la invasión, a pesar del gran flujo de difusión de productos que las apuntalaban, puede haberse debido a la erosión de su prestigio por graves fallos con trascendencia global cometidos en el pasado.

6. Contar tanques es fácil, predecir intenciones es difícil

En inteligencia normalmente diferenciamos las necesidades de la conducción de las que tiene el diseño y planeamiento de las operaciones. Efectivamente, la conducción es ávida consumidora de conciencia situacional y el planeamiento requiere estimaciones sobre el futuro. En ambos casos se deben hacer valoraciones sobre lo que significa lo que *vemos*, en un proceso para el que en lengua inglesa se emplea la atractiva secuencia de verbos: *sense-make sense*.

De ambos procesos lo verdaderamente difícil es el *make sense*. Observar disposiciones de unidades militares y geolocalizarlas es relativamente fácil si se dispone de medios de vigilancia y reconocimiento. No es difícil, y cada vez lo será menos, detectar y *contar* buques, aviones, vehículos de combate y situar esos objetos (Battle Space Objects, BSO) en el mapa de situación con el valor añadido de un cierto análisis y etiquetado.

Por el contrario, anticipar intenciones para configurar la propia acción ofensiva o defensiva en base a estimaciones de calidad sobre las intenciones y los conceptos de operaciones del enemigo es mucho más difícil. Valorar la magnitud de la potencia de combate de las unidades que se observan y, por tanto, sus opciones de éxito en los enfrentamientos militares es extremadamente difícil, como se ha señalado con insistencia. Este problema afecta a la inteligencia militar en todos los niveles de la conducción de la guerra y de las operaciones.

La derivada de todo esto —para el asunto que interesa aquí—, es la dificultad, pero también la importancia, de la evaluación de esos elementos no físicos y también de su detección, lo que representa un reto mayúsculo para la inteligencia de los *corazones y las mentes*, la inteligencia del ámbito cognitivo.

Análogamente podríamos añadir que los aspectos culturales de las organizaciones militares pudieran ser susceptibles de evaluación como catalizadores o como inhibidores de su éxito en el diseño, planeamiento y ejecución de las actividades militares. Aun a falta de un estudio sistemático, resulta, no obstante, evidente que las FAS rusas padecen el efecto de su propia y fuertemente arraigada cultura de freno sistemático a la iniciativa y de su modelo de liderazgo rígido y autoritario[23]. Esta cultura, que es conocida y cuyo impacto en los fracasos tácticos ha sido ya suficientemente señalada[24], puede estar también detrás de una de las posibles causas del grave error estratégico que cometió el presidente de la Federación Rusa cuando invadió Ucrania. Sus asesores, como quedo de manifiesto en una famosa grabación de su jefe de inteligencia, más que aumentar la comprensión y conciencia

[23] Watling, J. (2022). Russia's underperforming military capability may be key to its downfall . *The Guardian*. «Fear of punishment has created a military in which soldiers will doggedly implement orders even when they no longer make sense. For example, Russian artillery units routinely prosecute targets in the order that they receive fire missions, with no contextual prioritisation. Even when new intelligence indicates a target has moved, Russian units will often engage the previous location and then the new one, giving the target time to move once more». Disponible en: https://www.theguardian.com/world/2022/sep/18/russia-military-underperforming-ukraine

[24] Frías, C. J. (2022). Ucrania y el Ejército ruso: primeras impresiones (II). Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO71_2022_CARFRI_Ucrania.pdf

situacional de Vladimir Putin, parecían ser una caja de resonancia de sus ideas sesgadas y preconcebidas evitando desagradar al *Jefe*[25].

Análogamente al razonamiento de la potencia de combate y la capacidad de combate de párrafos precedentes, nadie duda que la cultura de las organizaciones puede ser *lubricante* o puede ser *arena* en sus engranajes. Entre otros *pecados* de su acervo organizacional, la cultura ruso-soviética de la jerarquía rígida contraria la iniciativa parece que ha sido y está siendo una rémora. A pesar de la enorme dificultad para el manejo de elementos intangibles en los juicios y valoraciones predictivas en inteligencia, debemos mejorar nuestra manera de medirlos, evaluarlos e integrarlos en nuestros estudios y *wargamings* para evitar sonados fracasos como los cometidos por casi todas las inteligencias estatales, multinacionales y por muchos *think tanks* en Occidente en la evaluación de la potencia de combate, de la verdadera magnitud de la capacidad militar rusa.

Un análisis cargado de la inteligencia actual y sustentado en la inteligencia básica es importante y es una de las bases de la conciencia situacional y sobre ella se construyen las estimaciones de evolución de la situación. Sin embargo, aún más importante que tener la *fotografía* de la disposición física de los elementos, incluso de la fotografía anotada y etiquetada, es poder valorar adecuadamente esos elementos subjetivos en los que radica la verdadera naturaleza de la amenaza y el efecto de esos BSO en nuestra potencial actuación y opciones de éxito. Conocer, anticipar, entender las intenciones, voluntades de resistencia, previsibles reacciones de los comandantes ante la presión y otros elementos abstractos e intangibles es mucho más importante y supone un gran reto para la inteligencia. Un reto difícil de superar con éxito. Algo que ya sabíamos y que Ucrania nos ha recordado.

Casi todo el mundo reconoce los graves errores cometidos en relación con las estimaciones sobre la posible invasión rusa de Ucrania y, una vez producida, acerca de la evolución posterior de la misma. Por los motivos mencionados, ha habido errores en la evaluación de las capacidades de las Fuerzas Armadas rusas y también en la de las ucranianas.

Sin duda, lo que falló en ese cálculo, no se debió a un *recuento* incorrecto de los medios militares de los beligerantes, sino que tuvo que ver con los citados aspectos intangibles, y por tanto, difícilmente cuantificables. La voluntad de resistir, la conciencia de estar *haciendo lo correcto*, la confianza en el mando o la disciplina en todas sus dimensiones son clave en esta ecuación. En esa categoría de elementos, mencionada de forma repetitiva en las líneas precedentes, radica la explicación a la inesperada resiliencia del

[25] *La Vanguardia*. (2002) Putin humilla a su jefe de inteligencia en una reunión de alto nivel sobre Ucrania: «¡Habla claro!». Disponible en: https://www.youtube.com/watch?v=z0ZWg-FFkVRQ

pueblo ucraniano y también en ellos hay que buscar algunas de las debilidades incomprensibles de la maquinaria militar rusa. Podríamos decir que «el mejor *hardware* no sirve de nada sin un buen *software* cultural y moral».

Los sistemas de indicadores de alerta estratégicos pueden establecer multitud de parámetros a monitorizar, medir y trasladar a sistemas complejos de integración para su análisis. No obstante, la emisión, o no, de alertas derivadas de ese estudio de indicadores tiene mucho de valorativo, de subjetivo. No siempre la concentración de tanques anticipa la voluntad de usarlos en una acción ofensiva. No hay duda de que debemos aprender a parametrizar e integrar mejor los intangibles culturales y morales mencionados, en nuestros sistemas de la inteligencia de alertas en beneficio de la anticipación estratégica u operacional.

Una prueba de las limitaciones de estos sistemas fue el mantenimiento de la posición de la *Direction du Renseignement Militaire* (DRM) francesa y de algunas otras organizaciones, que consideraron poco probable la invasión hasta las vísperas mismas de su inicio. Como es sabido, esta situación provoco el cese, pocos días después, del Director de la DRM, General Eric Vidaud[26].

Es cierto que nada de lo dicho en los párrafos precedentes es una novedad, pero también lo es que la guerra de Ucrania ha sido un recordatorio de hasta qué punto toda la tecnología, todos los sensores, todo el *hardware* y *software*, toda la analítica avanzada acaban chocando con nuestra incapacidad para obtener y descifrar nuestras más deseadas y necesarias necesidades de inteligencia: lo que piensan, lo que pretenden y lo que asusta a los comandantes adversarios.

7. La tecnología y la democratización de la inteligencia

La ciencia y la tecnología han sido históricamente una constante configuradora de la actividad militar. Las tecnologías han ido desarrollándose como soluciones ofensivas o defensivas contra otras tecnologías defensivas u ofensivas existentes. Su aparición ha sido casi siempre un catalizador de cambios en las doctrinas, los procedimientos y en las organizaciones. A veces, no siempre, estas novedades hacen su aparición como *huracanes* disruptivos que cambian las *reglas del juego* y provocan grandes modificaciones en el modo de hacer la guerra o de evitarla.

La guerra de Ucrania ha sido el escenario de muchas novedades tecnológicas ya intuidas o anticipadas en nuestras previsiones, pero que en pocas ocasiones habíamos visto materializarse hasta ahora en un contexto real

[26] *Midi Libre* (2022). Pourquoi le directeur du renseignement militaire français va-t-il quitter son poste ? Disponible en: https://www.midilibre.fr/2022/03/31/pourquoi-le-directeur-du-renseignement-militaire-francais-va-t-il-quitter-son-poste-10205898.php

de acción militar. Algunas de estas novedades, también en el ámbito de la inteligencia, han tenido un impacto muy significativo en el desarrollo de los acontecimientos.

La inteligencia de fuentes abiertas y de redes sociales (RR.SS.) no es nueva para las comunidades de inteligencia, pero ambas, y especialmente esta última, han tenido una importancia nunca antes vista en anteriores conflictos bélicos. Las herramientas analíticas y de rastreo disponibles han convertido a las RR.SS. en una valiosa fuente de información[27]. Su contribución a la inteligencia militar, y a través de ella, a la acción operativa ha sido muy importante en la guerra de Ucrania y se ha materializado en innumerables facetas entre las que se pueden mencionar las siguientes:

- Identificación de personas fallecidas.
- Identificación positiva de individuos de alto valor susceptibles de ser objetivos.
- Geolocalización de personas y/o unidades.
- Identificación de materiales significativos.
- Captura de imágenes o videos para su uso en el ámbito de las acciones de influencia.

En el campo de la identificación biométrica de personas o la identificación de objetos a partir de sus elementos físicos reflejados en imágenes o video, los avances de los últimos años han puesto en manos de los beligerantes (especialmente de Ucrania) herramientas de *software* que han sido usadas con gran éxito. Han sido empleadas en el análisis, valoración y preparación de la acción (letal o no letal) sobre objetivos, lo que conocemos como *targeting*. También han contribuido a la generación y mejora del llamado orden de batalla (identificación y disposición) de las fuerzas adversarias, así como a las acciones de guerra psicológica, algunas marcadamente agresivas, en el contexto del cruento enfrentamiento que ha venido librándose en el ámbito cognitivo[28].

En el campo de la inteligencia de imágenes, esta guerra ha puesto de manifiesto el papel de los proveedores comerciales de imágenes e incluso de aquellos que, quizás con fines muy lejanos a la inteligencia militar, las proporcionan con carácter libre y gratuito[29].

---

[27] *The Economist* (2022). The invasion of Ukraine is not the first social media war, but it is the most viral. Disponible en: https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456

[28] Weiss, Michael. (2022). Inside Ukraine's Psyops on Russian and Belarusian Soldiers. *New Lines Magazine*. Disponible en: https://newlinesmag.com/reportage/inside-ukraines-psyops-on-russian-and-belarusian-soldiers/

[29] Ignatus, D. (2022). How the algorithm tipped the balance in Ukraine. *Washinton Post*. «In our Kherson example, Palantir assesses that roughly 40 commercial satellites will pass over the area in a 24-hour period». Disponible en: https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

No hay duda de que uno de los protagonistas de esta guerra han sido las aeronaves tripuladas remotamente. La guerra de Nagorno-Karabaj[30] fue, probablemente, la primera guerra en la que este tipo de medios tuvieron un papel importante, en algún caso decisivo, pero Ucrania está siendo la consolidación del *reinado* de los RPAS en las actividades de ataque y desde luego también de ISR[31]. Un reinado previsible y previsto, que no sorprende a nadie y que estamos observando con nitidez.

En definitiva, la tecnología al servicio de la obtención y el análisis de inteligencia no solo ha avanzado, sino que se ha hecho accesible, se ha *democratizado* hasta el punto, como se analizará en el próximo apartado, de estar disponible en manos incluso privadas.

8. Multidominio, ISR atípico[32], *crowdsourcing intelligence*[33]

La noción de entorno operativo multidominio y operaciones militares que integran acciones en los dominios físicos y no físicos no es estrictamente nueva, se lleva hablando de ella casi una década[34]. Sin embargo, la guerra de Ucrania la está mostrando en su máxima expresión. Los proyectiles físicos y la destrucción que provocan, conviven con la batalla en el ciberespacio y también con las bombas cognitivas portadoras de *submuniciones* generadoras de confusión y desmoralización. Hace algunos años que las Fuerzas Armadas occidentales, incluidas las españolas, hemos empezado a aproximarnos al ámbito cognitivo, considerándolo ya sin paliativos un espacio de confrontación, quizás ni siquiera secundario[35].

---

[30] Dyxon, R. (2022). *The Washington Post*. Disponible en : https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441b-cbd2-193d-11eb-8bda-814ca56e138b_story.html

[31] JISR: Joint intelligence, surveillance and reconnaissance, actividades conjuntas de Inteligencia, Vigilancia y Reconocimiento. En general el concepto de ISR o Joint ISR-JISR nace para poner el énfasis en la agilidad del apoyo a las operaciones y al ciclo de targeting (análisis, valoración, ataque a objetivos, con acciones físicas o no físicas, letales o no letales).

[32] Conocido como *non-traditional ISR*.

[33] McCabe, M. (2019). What is Crowdsourcing Intelligence? *Intelligence Fusion*. Disponible en: https://www.intelligencefusion.co.uk/insights/resources/article/what-is-crowdsourcing-intelligence/

[34] McCoy, K. (2017). The road to multi-domain battle: an origin story. *Modern War Institute*. Disponible en: https://mwi.usma.edu/road-multi-domain-battle-origin-story/#:~:text=The%20origins%20of%20Multi-Domain%20Battle%20can%20be%20traced,will%20create%20and%20the%20solutions%20it%20will%20require.

[35] Goldstein, Simon (2020). A British Perspective On Information Manoeuvre. *Defstrat*. Disponible en: https://www.defstrat.com/magazine_articles/a-british-perspective-on-information-manoeuvre/

Las operaciones multidominio requirieren, como resulta evidente, inteligencia (y por ende ISR) multidominio[36]. La máxima expresión de la inteligencia multidominio son los episodios, cada vez más frecuentes, de lo que podríamos llamar *cross domain cueing* [37] y del apoyo a las acciones letales mediante la obtención y el procesamiento de inteligencia en los ámbitos no físicos del entorno operativo.

Ucrania ha mostrado casos de éxito en los procesos mencionados, en la inteligencia de redes sociales, en el análisis de sus flujos, de sus mensajes y en el procesamiento de sus materiales gráficos con fines de inteligencia. Una inteligencia con efecto en la conciencia situacional acerca de los ámbitos no físicos, pero también en la comprensión holística del entorno en sus múltiples dimensiones. Una inteligencia que cataliza acciones en el mundo físico desde la inteligencia en los ámbitos no físicos.

Otro aspecto significativo, otra tendencia en curso, es el llamado ISR atípico o *non-traditional ISR* (NTISR)[38]. Este concepto nació en referencia a los sensores no específicos de inteligencia de plataformas y sistema de armas, pero puede ahora aplicarse a sensores de toda índole, como las cámaras de los teléfonos móviles[39], de los sistemas seguridad de edificios o de los sistemas de control de tráfico que son valiosos contribuyentes potenciales a la obtención ISR.

Por otra parte, en la guerra Ucrania, y en torno a ella, está brillando como nunca antes la creciente facilidad para que ciudadanos normales puedan realizar el seguimiento y análisis de la guerra desde el salón de su casa. Se puede decir que la guerra de Ucrania está ofreciendo a los analistas *freelance* un festín de fuentes abiertas[40] e incluso de información del entorno que pueden consumir en tiempo real o casi real. Esta facilidad de acceso a la información en fuentes abiertas, favorecida por el cambio de paradigma en la difusión citado

[36] Atkins, S. A. (2018). Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace. *OTH Over The Horizon*. Disponible en: https://overthehorizonmdos.wpcomstaging.com/2018/09/12/multidomain-observing-and-orienting-isr-to-meet-the-emerging-battlespace/

[37] Pang, C. et *al*. (2017). Multi-Sensor Cross Cueing Technology and Its Application in Target Tracking. *ResearchGate*. Disponible en: https://www.researchgate.net/publication/317750654_Multi-Sensor_Cross_Cueing_Technology_and_Its_Application_in_Target_Tracking

[38] Deway, D. (2022). Here are 4 ways Non-traditional ISR can accelerate time to insight. *C4ISRnet*. Disponible en: https://www.c4isrnet.com/cyber/2022/10/31/here-are-4-ways-non-traditional-isr-can-accelerate-time-to-insight/

[39] Brodsky, S. (2022). How mobile phones are changing war in Ukraine. *Digitaltrends*. Disponible en: https://www.digitaltrends.com/mobile/ukraine-phones-warfare/

[40] *The Conversation* (2022). Open-source intelligence: how digital sleuths are making their mark on the Ukraine war. *The conversation*. Disponible en: https://theconversation.com/open-source-intelligence-how-digital-sleuths-are-making-their-mark-on-the-ukraine-war-179135

en párrafos precedentes, unida a la disponibilidad de *software* de explotación y análisis —en algunos casos incluso gratuito— proporciona capacidades nunca antes vistas fuera de las agencias oficiales o grandes *think tanks*. Cualquier persona con interés y una mínima formación puede ahora hacer aportaciones significativas al seguimiento y análisis de la guerra que hacen las agencias oficiales o los grandes operadores privados de inteligencia.

Como resulta evidente, lo mencionado en los párrafos anteriores subraya la magnitud de las capacidades privadas, tanto en obtención como en elaboración, que pueden ponerse al servicio del esfuerzo colectivo de inteligencia. La *crowd intelligence/crowdsourcing intelligence* (inteligencia colectiva) que aparece en el título del párrafo es, sin duda, una tendencia y una dimensión novedosa del concepto clásico del *pueblo en armas*, aplicado específicamente al campo de la inteligencia.

9. Obtención en entornos degradados

En la guerra de Ucrania hemos observado como las acciones de ISR han sido frecuentemente precedidas por acciones degradadoras del entorno para favorecer el efecto de determinadas disciplinas de obtención. Un caso paradigmático ha sido el recurso frecuente y fatal de los jefes militares rusos a las comunicaciones no seguras e incluso a la telefonía GSM ante la degradación de sus redes tácticas de sus comunicaciones militares[41] [42]. En muchos casos sus vulnerabilidades materiales y/o procedimentales preexistentes se han visto intensificadas por la acción de la guerra electrónica ucraniana preparando así el terreno a una efectiva obtención en inteligencia de comunicaciones (COMINT). Estos éxitos en COMINT han llevado, como ha sido ampliamente comentado, a éxitos importantes en la destrucción o neutralización de elementos de mando y control e incluso a la efectiva acción letal contra los propios jefes militares usuarios de medios de comunicación no seguros. Estos casos de uso han sido ejemplos paradigmáticos de la interacción sinérgica entre la guerra electrónica, la inteligencia de comunicaciones y las acciones de destrucción física de objetivos.

10. Debilidades de Rusia, oportunidades para Ucrania

La superioridad en conciencia situacional, en comprensión del entorno, la llamada *information superiority* es un pilar clave del éxito militar. Rusia

[41] Frías, C. J. (2022). Ucrania: la guerra de los teléfonos móviles. Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO112_2022_CARFRI_Ucrania.pdf

[42] Frías, C. J. (2022). Ucrania y el Ejército ruso: primeras impresiones (II). Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO71_2022_CARFRI_Ucrania.pdf

parece haber tenido y estar teniendo dificultades en ese ámbito, tanto por sus limitadas capacidades de obtención como en relación con el procesamiento-fusión, y probablemente, también en la alimentación de sus decisiones relativas al diseño y la conducción de la guerra. Precisamente en este campo, con un gran apoyo[43] exterior, recibido antes y durante la guerra, Ucrania ha sustentado, sin duda, una gran parte de sus éxitos.

En relación con la inteligencia militar de las fuerzas rusas en los niveles operacional y táctico, parecen observarse deficiencias en su ciclo de obtención en apoyo al análisis y valoración objetivos y en la acción sobre ellos (el llamado ciclo de *targeting*). Es cierto que su Fuerza Aérea ha mostrado limitada capacidad, pero sigue siendo sorprendente como ejemplo en este sentido, como señala el general de brigada Carlos Frias[44], el poco éxito a pesar de su capacidad artillera, en la destrucción de los RPAS BAYKTAR cuyas pistas normalmente se encontraban sobradamente dentro del alcance de la artillería rusa y en zonas que, teóricamente, no debieran haber presentado dificultades graves a la obtención ISR rusa [45].

De forma análoga, hay ciertos éxitos ucranianos en el este del país (Jerson, Jarkov) que difícilmente podrían entenderse sin la aparente sorpresa operacional y táctica que alcanzaron frente a las Fuerzas rusas lo que indica, una vez más, la debilidad de su ISR táctico y operacional y de su sistema de indicadores de alerta a esos niveles.

Otro aspecto en el que las deficiencias rusas han propiciado oportunidades a Ucrania han sido los problemas con el sistema de C2 y la debilidad de los escalones Brigada y División[46] [47]. Es en esas deficiencias, unidas quizás a aspectos relativos a la cultura militar rusa, donde hay que buscar la razón de la frecuente presencia de comandantes de los niveles tácticos superiores en los primeros escalones. En su intento de alcanzar conciencia situacional de primera mano y tratar de *conducir* fases principales de la maniobra táctica desde la proximidad de grupos tácticos de 1.º escalón, han ofrecido, en ocasiones, grandes oportunidades para la obtención ISR y el *targeting* ucraniano.

---

[43] Grady, J. (2022). Intel Sharing Between U.S. and Ukraine 'Revolutionary' Says DIA Director. *USNI News*. Disponible en: https://news.usni.org/2022/03/18/intel-sharing-between-u-s-and-ukraine-revolutionary-says-dia-director

[44] Frías, C. J. (2022). Ucrania y el ejército ruso: primeras impresiones. Instituto Español de Estudios Estratégicos (*ieee.es*). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO33_2022_CARFRI_Ucrania.pdf

[45] *Idem.*

[46] *Idem.*

[47] Ripley, T. (2022). Ukraine conflict: Russian military adapts command-and-control for Ukraine operations. *Janes*. Disponible en : https://www.janes.com/defence-news/news-detail/ukraine-conflict-russian-military-adapts-command-and-control-for-ukraine-operations

La debilidad de las comunicaciones tácticas rusas explotada adecuadamente por las Fuerzas ucranianas, unida a una conciencia y disciplina inadecuada en el uso de los teléfonos móviles, ha expuesto a las fuerzas rusas a una vulnerabilidad que ha sido, de nuevo, una oportunidad de oro para la Inteligencia/ISR ucraniana[48].

11. Epílogo

Como quedó advertido en las primeras líneas de este texto, resulta evidente que aquí no se ha hecho un análisis exhaustivo y sistemático del asunto. Sí se apuntan ciertas observaciones preliminares que, sin duda, merecerían un estudio más profundo y riguroso.

Entretanto propongo algunos aspectos acerca de los que la observación inicial de lo ocurrido sugiere una reflexión:

- La inteligencia como modelador del entorno y no solo como herramienta para su comprensión, así como la relación de la inteligencia desclasificada con la influencia, y en particular, con la acción disuasoria.
- La necesidad de mejorar los sistemas de indicadores de alerta estratégicos y de wargaming.
- La creciente dificultad para sustraerse a la obtención ISR enemiga en lo relativo a la disposición de elementos físicos en el entorno operativo y la necesidad de un nuevo modo de alcanzar la sorpresa.
- Los métodos de parametrización y medida de los elementos intangibles que configuran la potencia de combate y la eficiencia de organizaciones y procesos.
- Los mecanismos para mejorar la contribución del ISR atípico y de los contribuyentes externos (privados o corporativos) al esfuerzo de inteligencia (crowdsourcing intelligence).
- La mejora de los mecanismos de ISR multidominio y en particular del X-domain cueing.

[48] Frías, C. J. (2022). Ucrania y el Ejército ruso: primeras impresiones (II). Instituto Español de Estudios Estratégicos (ieee.es). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO71_2022_CARFRI_Ucrania.pdf