

El teatro de operaciones ucraniano se ha convertido en un banco de experimentación de armas y procedimientos con especial relevancia para la valoración del impacto de las nuevas tecnologías y la digitalización en las operaciones militares presentes y futuras. Este artículo trata de identificar aspectos notorios en relación con la digitalización que, en la práctica, han tenido grandes consecuencias en el devenir del conflicto y que afectan a las capacidades de inteligencia, vigilancia y reconocimiento y al empleo de la denominada «guerra de la información».

Con la digitalización de los sistemas de inteligencia, los aliados han posibilitado que la OTAN —principalmente los Estados Unidos— apoyase de manera directa el intercambio de información tanto en la defensa contra la invasión como en posteriores operaciones ofensivas de reconquista del territorio ocupado. Igual de importante es la utilización por parte de Ucrania del ciberespacio y del entorno de la información para potenciar y difundir *urbi et orbi* la narrativa de apoyo a su causa, un factor estratégico fundamental para conseguir y mantener el apoyo de Europa y Estados Unidos. La potenciación de la recopilación y el intercambio de información, junto con su distribución sencilla y oportuna a los receptores, ha puesto claramente de manifiesto el valor multiplicador de las capacidades de inteligencia mediante la digitalización.

Hay que admitir que las operaciones de inteligencia iniciales de Rusia contra las estructuras políticas y económicas de Ucrania fracasaron en lo más básico: la información precisa sobre la voluntad de resistir de Kiev. Si los rusos hubieran dispuesto de un mejor conocimiento, podrían haber efectuado una ofensiva completamente diferente, sustentada por una mejor preparación de la fuerza y una adecuada selección de las direcciones de ataque.

En Occidente, la inteligencia sobre la guerra ha sido abundante, precisa y públicamente difundida. Por ejemplo, el Ministerio de Defensa del Reino Unido ha publicado resúmenes diarios en su página de Facebook. Además, en los días previos a la entrada de Rusia en Ucrania, anuncios norteamericanos y británicos adelantaron con bastante acierto las acciones rusas. La evidencia demuestra que Rusia fue incapaz de proteger su proceso de planificación y deliberación, ya que las operaciones de inteligencia de los Estados Unidos penetraron completamente el liderazgo político, el aparato de espionaje y el

Ejército de Rusia¹. Los desmentidos rusos realizados en el momento resultaron ser falsos, lo que afectó a la credibilidad de posteriores declaraciones, al tiempo que reforzó la legitimidad de la información publicada por la OTAN.

Se ha escrito relativamente poco sobre las operaciones de inteligencia cibernética contra Rusia por parte de Ucrania y sus aliados, aunque han circulado suposiciones sobre la contribución de las fuerzas de la OTAN mediante datos de orientación para marcar objetivos de alto valor, como depósitos de municiones y centros de mando. El empleo de lanzacohetes de campaña HIMARS y del cohete guiado de largo alcance GMLRS — superior a los 70 kilómetros— produjo un gran efecto destructivo en depósitos de municiones². Esta información sobre los blancos podría haberse obtenido a través de medios cibernéticos, pirateando y rastreando teléfonos celulares o incluso pinchando las redes de mando rusas a través de operaciones de inteligencia concernientes a señales más tradicionales —por ejemplo, la triangulación de las ubicaciones de radares y radios— y reconocimiento de satélites, además del empleo de observadores y drones en la línea del frente.

Visión digital

El empleo en el conflicto de nuevas tecnologías como *driver* para el conocimiento de la situación y la coordinación de acciones ha concedido libertad de acción a las fuerzas ucranianas y ha permitido el apoyo de Estados Unidos y otros países simpatizantes. Ucrania ha hecho de las capacidades digitales un elemento imprescindible para la planificación de sus acciones a nivel táctico y estratégico. La oportunidad y fiabilidad de la inteligencia ha sido esencial para aportar la precisión necesaria en acciones como las emboscadas, la selección de blancos y el empleo eficaz de armas contracarro.

Uno de los aspectos más divulgados de la actuación de la inteligencia ucraniana es el uso extensivo de la interceptación de las comunicaciones rusas. Debe admitirse que esto ha sido posible, en parte, por su insuficiente protección. Otro aspecto que se ha de

¹ HARRIS, Shane y LAMOTHE, Dan. «Intelligence-sharing with Ukraine designed to prevent wider war», *The Washington Post*. 11 de mayo de 2022. Disponible en: <https://www.washingtonpost.com/national-security/2022/05/11/ukraine-us-intelligence-sharing-war/>

² REUTERS. «Ukrainian military strikes with Western arms disrupt Russian supply lines - general». 14 de julio de 2022. Disponible en: <https://www.reuters.com/world/europe/ukrainian-military-strikes-with-western-arms-disrupt-russian-supply-lines-2022-07-14/>

considerar es el eficaz empleo de sistemas no tripulados de bajo coste en espacios aéreos en disputa, siempre y cuando se disponga de la capacidad de inteligencia necesaria.

Si hay un aspecto en el que se estimaba que Rusia presentaba deficiencias, este eran las operaciones de influencia a través del ciberespacio. La combinación de piratería informática y propaganda dirigida empleada por Rusia tanto en el referéndum del Brexit en el Reino Unido como en las elecciones presidenciales de Estados Unidos en 2016 constituía una referencia para evaluar la habilidad y sofisticación de sus servicios de inteligencia a la hora de socavar las instituciones democráticas de los aliados de la OTAN.

En las operaciones de información, Ucrania ha sido capaz de verter todo el material disponible —desde comunicaciones rusas filtradas e inseguras hasta videos de emboscadas a vehículos blindados— en una narrativa de triunfo sobre un oponente desafortunado. Ucrania ha librado una guerra mediática que efectivamente retrata al país como la víctima que es y que muestra que Rusia ha pagado un alto tributo por la invasión.

Pero lo importante es que Ucrania ha podido apoyarse en las capacidades de Estados Unidos y la OTAN, perfeccionadas durante años de conflicto de baja intensidad y que pueden contribuir a la obtención de ventajas adicionales en una guerra convencional. Se estima que, para ayudar a las operaciones de Ucrania, la Alianza Atlántica ha proporcionado una gran cantidad de información sin procesar procedente de diferentes plataformas, así como análisis de inteligencia. Si bien estas plataformas no son necesariamente digitales en sí mismas, la recopilación, el análisis y, lo que es más importante, la difusión de la inteligencia se han acelerado a través de la digitalización.

La revolución digital también ha creado nuevos actores en la búsqueda de información que Ucrania ha aprovechado: empresas privadas de satélites comerciales e inteligencia de código abierto (OSINT) con efectos operativos e incluso estratégicos. Estos recursos son especialmente importantes para Estados como Ucrania, que carecen de las capacidades espaciales que poseen Estados Unidos, Rusia o China. Se conoce que Ucrania ha utilizado imágenes proporcionadas por Maxar y BlackSky³ para documentar

³ ERWIN, Sandra. «Commercial spy satellites put Russia's Ukraine invasion in the public eye», *Space News*. 27 de febrero de 2022. Disponible en: [Commercial spy satellites put Russia's Ukraine invasion in the public eye - SpaceNews](#)

los daños e identificar las unidades rusas. Estas aumentarían el tesoro de imágenes satelitales recibido de gobiernos simpatizantes.

Asimismo, ha quedado comprobada la relevancia de la inteligencia OSINT. Al menos al comienzo de la guerra, parecía que cualquier ucraniano con una cámara que filmara un ataque a un vehículo blindado ruso publicaba el material en internet. Estas imágenes en conjunto y los videos publicados por los militares ucranianos y rusos —a menudo captados desde vehículos aéreos no tripulados— se suman a una visión sorprendentemente completa de la contienda. En las redes sociales circulan multitud de datos. Su actividad, que tiene antecedentes próximos, ha aportado un factor ocasional de guerra sin pertenecer a un bando en particular. El cúmulo de información que se puede obtener a través de los medios digitales parece indicar que el factor limitante de la inteligencia probablemente resida en la capacidad de análisis, y no tanto en la obtención de datos.

Se trata de enviar un mensaje

Sin embargo, las capacidades digitales no solo tienen aplicaciones militares. También son muy útiles como herramienta política internacional y de apoyo a la diplomacia pública. Las informaciones disponibles constatan que Estados Unidos, Francia y el Reino Unido hicieron públicas sus evaluaciones de inteligencia antes de la invasión rusa en un intento de cambiar el comportamiento del Kremlin, preparar a Ucrania para la batalla e influir en la opinión pública mundial. Es resaltable la ausencia de Alemania en esta actuación. La importancia de dichas actividades y de otras que se han ido conociendo a lo largo del desarrollo de la guerra es difícil de conceptualizar. No obstante, existe la posibilidad de que con el apoyo de la tecnología digital y un modo estratégico adecuado se influya en la audiencia global casi a tiempo real.

Ucrania no ha actuado como un receptor pasivo de la ayuda occidental. El Gobierno ucraniano aprovechó y aprovecha la información y las plataformas digitales para elaborar una narrativa propia y llevarla a audiencias nacionales y globales. Además, el Gobierno ucraniano ha utilizado con éxito las plataformas digitales para levantar la moral de su pueblo, dar cuenta del progreso de la guerra y establecer un enlace activo con otros gobiernos. La tecnología digital permitió al presidente Zelenski pronunciar discursos ante

organismos legislativos extranjeros para cosechar el apoyo internacional al tiempo que permanecía en Kiev para mantener la moral y demostrar simbólicamente la capacidad de resistencia de Ucrania ante el ataque ruso. Los hechos demuestran de manera concluyente que Zelenski personalizó la guerra de la información utilizando la tecnología digital para obtener efectos bélicos tangibles.

Estos esfuerzos en la guerra de la información han sido particularmente exitosos para contrarrestar la desinformación rusa en Ucrania, Europa y los Estados Unidos y también para tomar la iniciativa en dicho ámbito desde el comienzo del conflicto. Antes de la invasión, el consenso general era que Rusia tenía una capacidad única para contaminar los discursos y los espacios informativos al servicio de sus fines. Al igual que ha sucedido con las predicciones sobre el poder militar ruso, esta evaluación ha demostrado estar lejos de la verdad.

Evolución más que revolución

La llamada «revolución digital» ha generado todo tipo de conjeturas sobre cómo se verán afectadas las guerras futuras, pero hay que ser conscientes de que esta también ha modificado y, en ciertos aspectos, afectado las funciones de guerras existentes. Al igual que ha sucedido con otras innovaciones militares, se ha predicado que la digitalización cambiaría fundamentalmente el carácter de la guerra. Un ejemplo común son las operaciones de efectos cibernéticos. La exageración nos hacía creer que Rusia podía anular los sistemas antiaéreos e incluso cierto armamento e interrumpir el suministro eléctrico en vastas franjas de Ucrania, pero nada de esto ha ocurrido.

La guerra en Ucrania debería obligarnos a centrarnos en el valor más mundano de la tecnología en los conflictos modernos. En lugar de una verdadera revolución en los asuntos militares (RMA), la tecnología está catalizando una evolución más pausada. Las capacidades interoperables de los aliados, impulsadas cibernéticamente mediante la «actuación en red», han generado un mayor volumen de información mucho más accesible debido a la potenciación de la capacidad para procesar a alto ritmo aportaciones de diferentes fuentes y difundirlas globalmente. También han aportado elementos cognitivos esenciales para la concepción estratégica, la planificación operativa y el empleo táctico.

Ucrania demuestra que se debe adoptar una perspectiva holística sobre el papel de la tecnología en la guerra. El empleo de la tecnología digital para mejorar las capacidades de producción de inteligencia ofrece un retorno significativo de la «inversión», que proporciona protección contra sorpresas estratégicas y facilita la ejecución táctica. También puede servir de vehículo para difundir narrativas informativas que obtengan resultados favorables constatables. La guerra de la información no consiste solo en la utilización de sus «armas», se trata de emplear las capacidades disponibles para construir las narrativas adecuadas en la conquista de los objetivos establecidos. Vale la pena financiar estas capacidades tecnológicas —en el caso de las plataformas de inteligencia— y perfeccionarlas —en el caso de las tácticas de guerra de la información—. Las promesas de las nuevas capacidades y tecnologías militares, como las operaciones de efectos cibernéticos y la inteligencia artificial (IA), nos distraen en el empleo de las capacidades presentes.

El poder de las capacidades digitales ha quedado probado en Ucrania y proporciona una enseñanza importante: es necesario pensar sobre los «revolucionarios» cambios que la tecnología producirá en la conducción de la guerra, sin dejar de considerar la «evolución» de las formas, aparentemente normales pero impactantes, en las que cambiará las actuales funciones bélicas.

*Enrique Fojón**

Coronel de Infantería de Marina (Ret.)