

El papel de la tecnología en los recientes conflictos de Ucrania y Gaza. Una valoración inicial

Carlos Martí Sempere | Experto en asuntos de seguridad y defensa

Tema

La tecnología y la capacidad de producción del armamento afectan a los recientes conflictos de Ucrania y Gaza.

Resumen

En los recientes conflictos bélicos en Ucrania y Gaza se puede observar la importancia de la explotación tanto de nuevas tecnologías, como del mantenimiento de capacidades militares esenciales, como la reposición de medios, munición y repuestos para enfrentarse con éxito al adversario. Este documento analiza en qué medida la tecnología ha mejorado las capacidades militares en aspectos como la movilidad, el enfrentamiento, la inteligencia y la logística, examinando su empleo, sus ventajas y, en su caso, sus posibles limitaciones.

Análisis

La [invasión de Ucrania](#) por la Federación Rusa, el 24 de febrero de 2022, así como [los ataques de Hamás sobre Israel](#), el 7 de octubre de 2023, han mostrado el importante papel, por no decir esencial, desempeñado por algunas tecnologías sobre el resultado de las acciones llevadas a cabo por las partes enfrentadas. Mientras que algunas han mejorado los métodos y tácticas empleados, favoreciendo el éxito de la operación, otras han demostrado tener una eficacia relativamente baja.

Este trabajo analiza en qué medida la tecnología ha mejorado las capacidades militares en aspectos como la movilidad, el enfrentamiento, la inteligencia y la logística, examinando su empleo, sus ventajas y, en su caso, sus posibles limitaciones. Aunque en estos conflictos se han usado métodos tradicionales de probada madurez, este documento explora los más afectados por estas nuevas tecnologías. Para ello, se han usado inteligencia de fuentes abiertas, lo que ha limitado su evaluación al ser insuficientes los datos sobre la tecnología y el contexto particular donde se ha empleado para evaluar sus efectos y su impacto. Además, la ausencia de una verificación independiente hace factible que la información publicada esté sesgada u oculte datos especialmente relevantes.

Gran parte de la nueva tecnología usada en Ucrania ha sido facilitada por Occidente. Sus prestaciones han sido fruto de largos y costosos procesos de investigación y desarrollo, aunque su empleo operativo eficaz ha recaído fundamentalmente sobre las Fuerzas Armadas ucranianas. Estados Unidos (EEUU) y los aliados de la Organización del Tratado del Atlántico Norte (OTAN), han proporcionado esta tecnología en forma de

datos, equipos, capacidades tecnológicas y otros recursos al Gobierno ucraniano que han sido claves para evitar su derrota. Empresas privadas como SpaceX, Microsoft, Palantir, Planet Labs, Capella Space, Maxar Technologies y muchas otras han colaborado en este proceso, tanto de forma desinteresada como para evaluar sus soluciones tecnológicas y comercializarlas cuando han tenido éxito. En cualquier caso, la ayuda prestada se ha centrado en medios defensivos, evitando armas ofensivas que pudieran escalar el conflicto.¹

Por el contrario, las menores capacidades industriales y tecnológicas de la Federación Rusa, el menor apoyo de otras naciones (China, Corea del Norte), así como las sanciones económicas, financieras y tecnológicas impuestas por su ilegal invasión han mermado su capacidad de avituallar a sus Fuerzas Armadas con los medios que precisan en este conflicto, como es el caso del dron de espionaje ruso Orlan-10.²

En el conflicto en Gaza, Israel dispone de tecnología avanzada para hacer frente al ataque de Hamás que ha mostrado habilidad para explotar militarmente tecnologías civiles, aunque sus capacidades para hacer frente a Israel, incluidos algunos apoyos externos (Hizbullah, los huzí, Irán), es muy limitada.

Vehículos autónomos y robótica

El empleo de vehículos autónomos y la robótica en estos conflictos está siendo extensivo por dos razones básicas. Por una parte, los espectaculares avances en prestaciones, así como la significativa caída del precio de esos sistemas en los últimos años, lo que ha permitido desplegarlos rápidamente y usarlos en un entorno bélico con alteraciones mínimas. Y, por otra, su capacidad de realizar misiones sobre el adversario de forma remota, lo que reduce el riesgo de pérdidas humanas, un coste especialmente alto que los políticos desean evitar. Esta también ha sido la preferencia de Israel con cuatro semanas de continuos bombardeos aéreos y ataques con misiles y granadas de mortero guiadas sobre Gaza antes de comenzar la batalla terrestre. No obstante, la Federación Rusa ha mostrado una menor sensibilidad a estas pérdidas humanas, una de las causas de la rebelión del grupo Wagner en junio de 2023.³

El uso de drones ha sido masivo, pero también se han usado motos acuáticas dotadas de un sistema de guiado y cargadas de explosivos para atacar a la flota rusa en Crimea⁴, o vehículos terrestre autónomos en tareas de desminado. La principal misión de los drones es capturar información de inteligencia, para disminuir el riesgo de la operación al conocer con más precisión la situación del adversario y sus intenciones, así como facilitar la coordinación de las propias fuerzas. Su capacidad de observación avanzado permite localizar objetivos o corregir el tiro de artillería, identificar los sistemas de

¹ Sobre ayudas, ver https://en.wikipedia.org/wiki/List_of_military_aid_to_Ukraine_during_the_Russo-Ukrainian_War.

² Bendett, S. y J. Edmonds (2022), "Russian Military Autonomy in Ukraine: Four Months In", *CNA Occasional Papers*, Center for Naval Analysis, julio.

³ Jones, S. G., McCabe R. y Palmer A. (2023), "Ukrainian Innovation in a War of Attrition", *CSIS Briefs*, Center for Strategic and International Studies, febrero.

⁴ Jones, G., Egan J. y Rosenbach E. (2023), "Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S." Belfer Center, Harvard Kennedy School, 31/VII/2023.

defensa aérea del adversario actuando como señuelo o bien encontrar brechas desde las que efectuar posibles ataques.

Aunque el *software* de estos aparatos puede realizar muchas funciones autónomamente, no se puede hablar todavía de que actúen sin autorización previa humana, una cuestión especialmente preocupante desde el punto de vista del derecho bélico, dada la posibilidad de que cometan errores.

Los modelos más avanzados pueden portar armas y explosivos para realizar ataques desde la distancia. Algunos tienen un comportamiento suicida, es decir, merodean en busca de un objetivo de oportunidad, en cuyo caso caen en picado sobre el mismo detonando la carga explosiva que portan. Ejemplos de estos aparatos son el Switchblade Tactical y el Phoenix Ghost norteamericanos o el Warmate polaco.⁵ Para ataques más estratégicos se han empleado aparatos con mayores prestaciones como el turco Bayraktar TB2 con una autonomía de 300 km o 27 horas vuelo y capaz de portar cuatro municiones guiadas por láser. Su precio se sitúa en torno a los cinco millones de dólares. Ucrania los ha usado con éxito para atacar lanzadores de misiles tierra-aire, depósitos de munición, rutas de suministro y convoyes armados e incluso para ayudar al hundimiento del *Moskvá*, buque insignia de la flota rusa del mar Negro. El dron Tu-141 Strizh también se ha usado para atacar bases rusas. Otro modelo autóctono, el UJ-22, ha logrado aproximarse a Moscú.

Los modelos usados son muy variados. Los más sencillos son pequeños aparatos comerciales con capacidad de transmitir imágenes video de alta resolución como el cuadróptero DJI Mavic 3 chino que se controla desde un *smartphone* o una *tablet* y con un precio en torno a los 2.000 dólares. Otros modelos usados por Ucrania son el A1-CM Furia, el Spectator M-1, el Leleka-100 "Stork", el Punisher, el People's Drone (PD-1) o el R18 octocóptero. La Federación Rusa tiene también una larga lista como el Orlan-10, Orlan-30, Eleron-3, Takhion, Zastava y el modelo Lancet y Kub-Bla de Zala, junto con modelos tipo helicóptero, así como el Forpost-R y el Orión de combate. La lista se ha completado con unidades adquiridas a Irán como el Shahed 136 y el Mohajer-6. Israel también dispone de drones como los modelos IAI Heron, Elbit System Thor y Magni que se han usado contra líderes de Hamás y objetivos bajo tierra.

Rusia ha usado, además, el misil hipersónico Khinzal (velocidad superior a 5 *mach*) lanzado desde el aire, al menos en tres ocasiones, sobre Ucrania para golpear objetivos protegidos. La combinación de velocidad, maniobrabilidad, sigilo y habilidad para evadir los sistemas de defensa, lo convierte en un sistema único. A pesar de ello, su uso no parece haberle otorgado una ventaja estratégica significativa.⁶ Para ataques contra objetivos de alto valor ha empleado misiles crucero (KA-101 y KH-555) y misiles balísticos como el Iskander, todos ellos dotados de guiado terminal.⁷

⁵ En algunos casos, se ha reportado el uso de granadas anticarro modificadas con aletas estabilizadoras, impresas en 3D, para impactar sobre el débil techo de los vehículos acorazados rusos.

⁶ Favaro, M. y Williams H. (2023), "False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation", *Journal for Peace and Nuclear Disarmament*, 6:1, pp. 28-46.

⁷ Irán ha utilizado también misiles balísticos Fateh-110 con guiado terminal contra la supuesta base del Mossad en Irak.

Uno de los principales problemas de los drones es su gran merma, por su uso incorrecto o por la facilidad con la que pueden ser abatidos, bien físicamente, bien usando sistemas de guerra electrónico que interfieren las señales GPS y comunicaciones, como el Krashukha-2 o el R-330 Zhitel rusos o los equipos usados por las Fuerzas Armadas israelíes⁸, lo que reduce sus posibilidades de éxito. Las pérdidas de drones ucranianos han crecido hasta situarse en torno a las 10.000 unidades mensuales, una cifra solo admisible gracias a su bajo coste.⁹

Defensa aérea

La capacidad de ataque desde el aire mediante vehículos autónomos, bien sean drones, misiles aire-tierra, o balísticos hace esencial el uso de medios de defensa aérea. Ucrania ha contado con el empleo de misiles Patriot, Norwegian Advanced Surface-Air Missile System (NASAMS), IRIS-T (una versión europea del Sidewinder) y Flakpanzer Gepard¹⁰, mientras que Rusia cuenta con los sistemas de defensa aérea SA-21 y SA-23 basados igualmente en radares y misiles tierra-aire. El empleo de estas tecnologías por ambas partes ha impedido que su adversario domine el espacio aéreo. Su elevado nivel de riesgo ha reducido considerablemente este tipo de ataques. Esta falta de claro dominio ha hecho que se usen con frecuencia ataques de saturación empleando una combinación elevada de estas armas para tener un cierto éxito.

Israel dispone de uno de los sistemas de defensa aérea más avanzados del mundo. Esta defensa se ha focalizado en la protección de los cohetes y granadas de morteros disparados desde la franja de Gaza, capaces de alcanzar Tel Aviv. Para ello, utiliza el sistema móvil de misiles tierra-aire denominado Iron Dome, desplegado desde 2011 que se complementa con el denominado Iron Beam que utiliza un láser de energía dirigida para destruirlos. Estos sistemas sufrieron un ataque de saturación el 7 de octubre con el lanzamiento coordinado de entre 2.200 y 3.000 cohetes. La protección frente a aviones y misiles balísticos y de crucero denominado “David’s Sling” que sustituye al antiguo Patriot, se puso en servicio en 2017, y se complementa con el sistema Arrow destinado a interceptar misiles balísticos de largo alcance. La protección del tráfico marítimo en el mar Rojo contra los ataques de drones y misiles huzí lanzados desde el Yemen, de procedencia iraní, está siendo soportada por EEUU y el Reino Unido con sus sistemas defensa aérea naval, aunque el coste de abatirlos es especialmente alto.

Artillería de precisión

Las piezas de artillería con capacidad de guiado terminal son también especialmente útiles para destruir objetivos de gran valor como puestos de mando radares o material logístico. Ucrania se ha beneficiada de esta artillería de precisión de largo alcance, como los 20 sistemas High Mobility Artillery Rocket System (HIMARS) suministrada por EEUU. Las brechas creadas con esta artillería le han permitido su explotación ulterior.

⁸ Scharf A, y Kubovich Y. (2023), “Israel Ramps up GPS Jamming to Thwart Hezbollah, Hamas Drone Attacks”, *Haaretz*, 16/X/2023.

⁹ Watling, J. y Reynolds N. (2023), “Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine”, *RUSI*, 19/V/2023.

¹⁰ Boot, M. (2023), “The Ukraine war is revolutionizing military technology. Whoever masters it wins”, *The Washington Post*, 18/IX/2023.

Rusia también dispone de este tipo de artillería como es el 2K25 Krasnopol con un alcance de 20 km y guiado terminal mediante un haz láser, aunque se dispone de menos información sobre su uso operativo, frente a su empleo tradicional.⁹

Satélites

El papel de los satélites desde el punto de vista estratégico ha sido también muy importante. Aunque Ucrania carece de ellos, ha contado con las imágenes proporcionadas por satélites de observación civiles y militares de Occidente, incluyendo la OTAN, así como herramientas automáticas de análisis, pudiendo así anticiparse y hacer frente a las acciones de la Federación Rusa. Entre ellos, se pueden citar las imágenes de alta resolución bajo cualquier condición meteorológica de los radares de apertura sintética (SAR) de empresas como la norteamericana Maxar o la finesa ICEYE. Estas imágenes alertaron de la invasión rusa al detectar movimientos de sus tropas cerca de la frontera antes de comenzar la guerra, a pesar de las declaraciones y desmentidos de Putin. También parecen haberse usado para destapar crímenes de guerra, como la localización de fosas comunes.

El empleo de satélites rusos en el conflicto parece haber sido más modesto, a la luz de los errores observados en sus sistemas de guiado preciso de misiles. No hay constancia de que haya empleado su arma antisatélite Perevest, tal vez por no inaugurar una nueva forma de combate, o quizá por el elevado número de satélites de observación, tanto civiles como militares, desplegados que hace poco efectiva esta arma, teniendo en cuenta que hay más de 500 satélites civiles de observación de la tierra.¹¹

Sistemas de información y comunicaciones

Los sistemas de información y comunicaciones conservan su papel esencial en estos conflictos, ya que permiten gestionar mejor las operaciones al reducir riesgos, disminuir la carga física y cognitiva de los combatientes, aumentar la velocidad de proceso de información, de toma de decisiones y de ejecución de la operación. Estos sistemas requieren disponer de redes de comunicación seguras y sistemas capaces de procesar grandes volúmenes de información. Un ejemplo son las aplicaciones Kropyvya o Delta desarrolladas por Ucrania que permite conocer sobre un *tablet* la situación de fuerzas amigas y enemigas. La transformación digital ha favorecido el desarrollo de aplicaciones (Apps) de uso general para apoyar la defensa, como por ejemplo la de Ucrania para proporcionar información de inteligencia vía internet, o recibir la alarma de un ataque aéreo ruso, o la de Israel, denominada Red Alert, para avisar del lanzamiento de cohetes desde Gaza.

El carácter vital de estos sistemas ha provocado múltiples intentos de atacarlos e inutilizarlos que no se han centrado exclusivamente en los militares, sino también en los civiles que soportan infraestructuras críticas, lo que incluye tanto ataques físicos como ciberataques, siendo la ventaja de este último la dificultad de identificar al atacante y

¹¹ Borowitz, M. (2022), "War in Ukraine highlights the growing strategic importance of private satellite companies, especially in times of conflict", <https://theconversation.com/war-in-ukraine-highlights-the-growing-strategic-importance-of-private-satellite-companies-especially-in-times-of-conflict-188425>

responder adecuadamente. Aunque los ciberataques rusos se iniciaron con la invasión de Crimea en 2014, éstos se intensificaron con el inicio del conflicto, en el que los rusos consiguieron deshabilitar los módems del sistema KA-SAT de Viasat Inc. bloqueando por un tiempo el acceso a internet a miles de ciudadanos ucranianos. Igualmente, se han efectuado ataques distribuidos de denegación de servicio (DDoS), secuestro de datos (*ransomware*), limpiadores (*wiper*) que han continuado durante el conflicto, muchos de ellos realizados por hackers con lazos con el gobierno ruso (v.g. Killnet)¹², aunque Ucrania también ha empleado estos métodos contra Rusia. También hay constancia de que Hamás, posiblemente con apoyo externo, realizó ciberataques el 7 de octubre sobre la administración israelí, aunque con resultados poco efectivos, quizá porque estaba mejor preparado en este asunto.¹³ Los ciberataques para espiar están menos documentados, aunque parece que Hamás ha logrado hackear teléfonos de soldados israelíes que podrían haberle facilitado su ataque inicial.

Los apoyos occidentales para defender a Ucrania en esta materia han sido vitales. La administración ucraniana, con el apoyo de empresas como Microsoft y Google, ha logrado trasladar a la “nube” un gran volumen de información, estimada en unos 10 petabytes, lo que ha garantizado su supervivencia.¹⁴ Por otra parte, la prestación de servicios de internet de banda ancha y baja latencia, resistente a interferencias electromagnéticas, a través de la red Starlink compuesta por 2.500 satélites de baja órbita, perteneciente a la empresa de Elon Musk SpaceX, ha permitido mantener su infraestructura de comunicaciones, gracias a los 30.000 terminales portátiles civiles suministrados en los primeros 15 meses de la guerra (la Unión Europea, UE, pretende desplegar una red similar denominada IRIS²).

En resumen, la creciente digitalización de la sociedad y la dependencia de los servicios que ofrece hace especialmente atractivo hostigar las infraestructuras civiles en esta materia para debilitar al adversario, e impedir su empleo con fines militares. Se trata de una forma de actuar un tanto gris que puede incumplir las normas del derecho de guerra sobre la separación entre combatientes y no combatientes. Un caso particularmente relevante es la restricción de servicios de internet provocada por Israel en la Franja de Gaza que está dificultando la provisión de ayuda humanitaria a los palestinos.

La guerra de la información

En un mundo crecientemente globalizado donde la información es fácilmente accesible a través de internet, esta red se está usando de forma extensiva por todas las partes para publicitar, justificar y legitimar sus acciones, así como ganar adeptos a su causa. Además, este medio se emplea para realizar campañas de desinformación, publicando falsas narrativas o distorsionando los hechos, para destruir la confianza en la información pública y en las instituciones, crear confusión y desacreditar a los

¹² Ver entre otros, Lewis J.A. (2022), “Cyber War and Ukraine”, CSIS, 16 de octubre; Digital Security Unit (2022), “Special Report Ukraine”, Microsoft, 27/IV/2022.

¹³ Mimran, T. (2023), “The hidden aspect of the conflict. Israel-Hamas”, 30/XI/2023, <https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict/>

¹⁴ Franke, U. y Söderström J. (2023), “Star tech enterprise: Emerging technologies in Russia’s war on Ukraine”, *Policy Brief*, European Council on Foreign Relations, 05/IX/2023.

beligerantes y sus aliados. Para ello se ha usado el amplio elenco de tecnologías civiles en esta materia, así como las redes sociales más importantes.

El papel de la Inteligencia Artificial¹⁵

La Inteligencia Artificial hace referencia al conjunto algoritmos cuyo propósito es imitar la inteligencia humana para realizar tareas que pueden mejorar conforme recopilan información, es decir, disponen de capacidad de aprendizaje. Se trata, pues, de una tecnología con un espectro de métodos y aplicaciones considerablemente amplio.

Es difícil determinar su escala de empleo en estos conflictos con la información disponible. En Ucrania, parece que se ha utilizado *software* para el análisis y explotación de grandes volúmenes de información (*Big Data*) como las imágenes de satélites, para soportar la toma de decisiones o para informar de posibles objetivos. Igualmente se ha utilizada para detectar con rapidez y evitar ciberataques, mediante la identificación de ciertos patrones asociados a un ataque.

La herramienta MetaConstellation proporcionada por la empresa Palantir a Ucrania es capaz de agregar datos procedentes de satélites comerciales para crear un modelo digital del campo de batalla que ayude a los mandos a evitar la “niebla de la guerra” de Clausewitz. Este sistema puede analizar la información de sensores para identificar posiciones enemigas, estimar las armas más apropiadas para destruirlas y evaluar los daños después de los ataques lo que permite mejorar la fiabilidad y precisión de sus predicciones.

Los algoritmos de la empresa norteamericana Primer se han usado para capturar, transcribir, traducir y analizar las comunicaciones militares rusas interceptadas sobre canales inseguros o no cifrados. El uso de las tecnologías de procesamiento del lenguaje natural para analizar las comunicaciones militares es un claro ejemplo del carácter dual de esta tecnología y de la relativa facilidad con la que algunas aplicaciones comerciales pueden reusarse con fines militares.

Tres agencias gubernamentales ucranianas declaran haber usado el reconocimiento facial proporcionado por la empresa Clearview AI para identificar soldados rusos fallecidos, prisioneros de guerra, o confirmar la identidad de los viajeros a través del país ante el temor de espías y saboteadores. Ucrania también ha desarrollado *chatbots*, aplicaciones diseñadas para conversar mediante texto, y que emplean métodos de Inteligencia Artificial, para que los ciudadanos puedan informar sobre la posición y el movimiento de tropas enemigas, denominadas eVorog y STOP Russian War.

Menos información existe sobre el empleo ruso de esta tecnología, aunque parecen haberse usado, al menos, en campañas desinformativas de creación de contenidos empleando técnicas como la denominada *Generative Adversarial Network* (GAN). El

¹⁵ Konaev, M. (2023), “Tomorrow’s Technology in Today’s War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability”, *CAN Occasional Paper*, septiembre.

caso más significativo ha sido la publicación de un video falso del presidente Zelenski rindiéndose a Rusia.¹⁶

Conclusiones

Los dos conflictos analizados muestran muchos aspectos de carácter convencional, sobre los que se yuxtaponen novedades significativas que hay que analizar para evaluar su impacto sobre la doctrina y los medios que conviene disponer para ejecutar misiones militares.

En Ucrania, se observa el empleo de carros de combate, barreras de artillería, obstáculos anticarro (zanjas, dientes de dragón), campos de minas, o aviones de combate y bombarderos, que difieren poco de su modo de empleo en la Segunda Guerra Mundial. Las fortificaciones, trincheras y campos de minas rusos que han detenido la contraofensiva ucraniana¹⁷, nos retrotraen al estático frente Occidental de la Primera Guerra Mundial y la petición de aviones F-16 del presidente Zelenski a EEUU para recomponer su deteriorada flota aérea, sugiere que los aviones tripulados mantienen todavía un considerable valor operativo. En este contexto, el efecto multiplicador de algunas armas ha tenido un papel vital para detener el avance ruso como el misil Javelin norteamericano, en producción desde 1996, que, se estima, destruyó 1.500 carros rusos o los 1.400 misiles Stinger que han evitado el dominio ruso del aire (estos misiles con guiado infrarrojo son del tipo “dispara y olvida” porque no precisan mantener la designación del objetivo durante su vuelo).

A pesar de las ventajas que aporta la tecnología, [la transformación de este conflicto en una guerra de desgaste](#) hace que la logística y la capacidad de reponer personal, medios, munición y repuestos sean tan importantes como en el pasado. En este sentido, las limitadas capacidades industriales de Ucrania hacen necesario el apoyo externo, pues, por ejemplo, sus necesidades de munición en un mes pueden consumir la que Europa produce en un año (no son menores las rusas: entre 12.000 y 38.000 durante el primer trimestre de 2023).

Lo que sí parece evidente es la necesaria integración de estas tecnologías con la forma de operar militarmente para extraer su máximo potencial, lo que incluye su empleo combinado con otros medios. En este contexto, la estrecha colaboración entre las Fuerzas Armadas y la industria resulta clave para tener éxito, como la rápida modificación del *software* de los sistemas ante las deficiencias observadas o mejoras operativas necesarias.¹⁸ Esto obliga a revisar el papel de la industria y su forma de colaborar con las Fuerzas Armadas, así como una nueva especialización del personal militar para aprovechar estos nuevos medios. Por otra parte, el papel estratégico de los productos y servicios que proporcionan algunas empresas plantea cuestiones

¹⁶ Youtube, Euronews, (16/03/2022), https://www.youtube.com/watch?v=TWS8_7HWMYA

¹⁷ Massicot, D. (2023), “Russian Military Operations in Ukraine in 2022 and the Year Ahead”, CT-A2646-1. Testimony presented before the U.S. Senate Committee on Armed Services, 28/11/2023, <https://doi.org/10.7249/CTA2646-1>

¹⁸ Un ejemplo de ello ha sido la dificultad de adaptar el misil anti-radiación HARM norteamericano a los aviones Su-29 ucranianos.

especialmente difíciles de resolver porque los intereses empresariales pueden diferir de los geoestratégicos nacionales, siendo necesario establecer normas que garanticen la disponibilidad de los medios y servicios prestados. Este es el caso de la red Starlink de SpaceX que Ucrania ha declarado usar en operaciones ofensivas de sus drones, por lo que Rusia podía considerar esta empresa como un objetivo militar.

Estos conflictos también han puesto de relieve la propia fragilidad de la tecnología como se ha visto en el deficiente funcionamiento del sistema de protección activa de vehículos de combate Trophy contra granadas y munición guiada contracarro¹⁹, en los drones cuando la autonomía de sus baterías cae sensiblemente con las bajas temperaturas invernales o en la vulnerabilidad de las torres de comunicación y los sensores avanzados ubicados en la valla de Gaza neutralizados por los drones de Hamás. En este sentido, las limitaciones de la tecnología son patentes en zonas densamente pobladas donde resulta especialmente difícil combatir a un adversario encubierto entre la población que utiliza las infraestructuras civiles y red de túneles como escudo para actuar, lo que conduce a operaciones especialmente sangrientas y destructivas, con daños inevitables sobre la población civil. En este marco, el propio concepto de una guerra altamente tecnificada que requiere poco personal queda en cuestión, como demuestra la precautoria movilización de cientos de miles reservistas israelíes tras el ataque de Hamás.

¹⁹ Frantzen, S.J. (2023), "New tech plays role in Gaza war, but not to level Israel once envisioned", *Breaking Defense*, 13/XI/2023.