EL DOMINIO ESPACIAL EN EL CONFLICTO EN UCRANIA

José Maria Martínez Cortés

Analista del Centro de Seguridad Internacional de la Universidad Francisco de Vitoria

INTRODUCCIÓN

Tres décadas después de la Primera Guerra del Golfo, a veces, denominada *primera guerra espacial*, la guerra entre Rusia y Ucrania es quizás, según David Burbach, profesor de la Escuela de Guerra Naval estadounidense, la primera guerra espacial entre dos bandos. Sin embargo, las escaramuzas rusas en la órbita LEO (baja) arrancaron incluso antes de que sus primeros carros de combate pisaran suelo ucraniano. Como ha demostrado este conflicto, tener el control del espacio y de los satélites que permiten la comunicación permanente del adversario es clave para obtener ventajas en los conflictos actuales, y lo será aún más en los del futuro.

En la invasión de Ucrania, antes de que se diera el primer tiro, la dirección de inteligencia militar de la Federación de Rusia lanzaba un ataque que dejó fuera de servicio miles de routers en tierra conectados a la red satelital estadounidense de la empresa de comunicaciones *Viasat*, red que permitía a Zelenski y sus mandos militarse comunicarse con sus soldados. El plan ruso consistía en desplegar una especie de telón de acero digital que dejara aislados a los altos mandos ucranianos, mientras que en tierra los carros rusos avanzaban para capturar la capital, Kiev. A su vez, el ataque fue acompañado de fuego de artillería dirigida a torres de TV y telecomunicaciones. La estrategia era asfixiar al ejército ucraniano en la "niebla de la guerra", según declaraciones de la directora de seguridad y estabilidad espacial del think tank estadounidense *Secure World Foundation*.

Sin embargo, Rusia tuvo poco tiempo para saborear su éxito. El fundador de *SpaceX*, Elon Musk, puso a disposición de Ucrania su red de satélites *Starlink* para restaurar la conexión a Internet, aunque tiempo más tarde la desactivaría para sabotear un ataque naval ucraniano contra la flota rusa. Así mismo, desde el primer momento, satélites de empresas privadas estadounidenses proporcionaron imágenes de alta resolución del conflicto que revelaban con gran precisión los movimientos de las FAS rusas. Tras este apoyo de occidente, el presidente Putin utilizaba a sus enviados a las reuniones de la ONU para amenazar con derribar los satélites estadounidenses que ayudaban a Ucrania, aunque él y los mandos rusos tenían claro que ese objetivo era prácticamente imposible.

Por su parte, el mayor número de actuaciones antisatélite, quizás, los eventos espaciales más significativos, ha estado centrado en Rusia y en actividades vinculadas con la utilización de la guerra electrónica y el ciberespacio. A pesar de que estas actividades son una buena muestra de que las capacidades de control ofensivo del espacio no forman ya parte de la ciencia ficción, también han dejado evidencia de la merma significativa de los últimos años de las capacidades de Rusia a la hora de integrar la tecnología espacial en sus operaciones militares y del hecho de que los estrategas rusos no se habían preparado para un conflicto prolongado contra un adversario que tenía acceso a más información aeroespacial que ellos. Los militares rusos parecían enfrentarse a un vacío de información, debido a los límites de sus constelaciones satelitales y a su falta de acceso a las imágenes comerciales occidentales. Estaba claro que Rusia no previó la cooperación que Ucrania recibiría de los países occidentales y los servicios comerciales.

Merece también especial atención el nivel de transparencia sin precedentes que ha habido en el espacio de batalla: se ha desclasificado inteligencia sensible para revelar los planes e intenciones de Moscú, se han hecho públicas imágenes mostrando la concentración de fuerzas rusas y, a través de las redes sociales, se han transmitido bien de cerca los horrores de la guerra. Además de esta ayuda a la transparencia, las capacidades espaciales están y han tenido una contribución significativa en el conflicto. Los satélites de comunicaciones han estado potenciando las fuerzas ucranianas y conectando al pueblo ucraniano con el mundo exterior. Las imágenes satelitales (algunas capaces de recoger fotografías nocturnas) han estado observando el movimiento de las fuerzas rusas, haciendo un seguimiento de las rutas de evacuación humanitaria y recopilando pruebas sobre potenciales crímenes de guerra. Así mismo, otros satélites han colaborado en detectar y localizar las fuentes de perturbación GPS que están causando que los UAVs ucranianos vean alterado su rumbo. Debido a la prominencia de capacidades industriales espaciales occidentales, que permiten o facilitan la resistencia de Ucrania, algunos observadores han descrito este conflicto como la "primera guerra espacial comercial".

Por su parte, lo mismo que ha pasado con otras tecnologías, la Federación Rusa, para contrarrestar esa ventaja, ha llevado a cabo actividades de control del espacio, fundamentalmente, de carácter ofensivo que, aunque no hayan tenido gran visibilidad (por su falta de publicidad), han tenido un papel importante. El empleo ruso de la guerra electrónica y los ataques contra los sistemas espaciales a través del ámbito del ciberespacio, así como la incertidumbre sobre el empleo ruso de armas láser y sobre el comportamiento inusual de los satélites inspectores rusos en la órbita GEO son aspectos reseñables que conviene analizar, y es que los ataques de Rusia contra las capacidades espaciales utilizadas por Ucrania son un ejemplo de cómo las armas de control ofensivo del espacio pueden emplearse, y probablemente serán empleadas, antes y durante futuros conflictos.

ASPECTOS GENERALES. DISPOSICIÓN DE CAPACIDADES ESPACIALES

En lo que respecta a la Federación de Rusia, como uno de los tres actores espaciales estatales dominantes, Rusia mantiene substanciales capacidades y fuerzas espaciales, muchas de ellas de la época de la Unión Soviética. Existe, además, una fuerte evidencia de que, desde 2010, se ha embarcado en un conjunto de programas con la finalidad de recuperar muchas de sus capacidades de control del espacio de la Guerra Fría. A pesar de las sanciones impuestas al Estado agresor, con algunos éxitos y fracasos habidos en el entorno del espacio, la última mayor revelación tiene que ver con las acusaciones estadounidenses en 2024 de que Rusia está desarrollando un arma antisatélite con capacidad nuclear que, según EEUU, violaría el Tratado del Espacio Exterior de 1967. Además de no haberse confirmado estas acusiones, según un portavoz estadounidense, esta capacidad no estaba desplegada y no representaba una amenaza inmediata.

Si bien los funcionarios rusos han esbozado una ambiciosa agenda espacial, las sanciones siguen bloqueando el acceso a tecnología occidental fundamental para la capacidad de Rusia de construir satélites modernos. En estas circunstancias, Rusia tendrá dificultades para ejecutar su estrategia optimista al respecto y menos aún a medida que continúe el conflicto. Por tanto, la base de la fortaleza rusa en el espacio, incluidas sus capacidades contraespaciales, es la tecnología y la infraestructura de la era soviética. Queda por ver cuánto tiempo podrá depender de sistemas y diseños que son, fundamentalmente, de la década de los 80 para mantenerse al día en el espacio y en un nivel de competencia con EEUU.

En este contexto, aunque puede afirmarse que Rusia tiene un conjunto probado y completo de armas para el control del espacio con gran variedad de capacidades para el control ofensivo, en base a unas sofisticadas capacidades de vigilancia y seguimiento espacial (aprovechando su infraestructura de épocas pasadas, para la alerta de misiles y defensa antimisil), Moscú ha continuado desplegando capacidades espaciales y de control de espacio menos avanzadas de lo que se esperaba. A pesar de sus pretensiones, no se han visto en el terreno armas avanzadas[1], tales como los láseres basados en tierra *Peresvet and Sokol-Eshelon,* aunque sí ha utilizado más que nunca capacidades espaciales y armas para el control del espacio, empleo vinculado, sobre todo, con la tensión en Europa del Este y con el conflicto en Ucrania, y ha continuado haciendo un seguimiento de satélites de otras naciones y creando confusión y preocupación sobre la verdadera intención de estas acciones.

Por su parte, en lo que se refiere a Ucrania y a sus FAS, a pesar de carecer de capacidades propias, el apoyo prestado por los países y compañías occidentales en productos y servicios, relacionados con las comunicaciones, las funciones ISTAR (vigilancia, inteligencia, reconocimiento y localización, designación y ataque de objetivos) y la inteligencia de señales, ha tenido un papel tremendamente relevante como vemos a continuación.

UCRANIA Y EL APOYO EN ISR, COMUNICACIONES Y TELEDETECCIÓN

Aunque Ucrania no dispone de capacidades nacionales espaciales, el gobierno y las FAS ucranianas han recibido y están recibiendo un apoyo con un papel significativo en el esfuerzo bélico, en forma de activos occidentales comerciales y gubernamentales (estadounidenses y europeos), apoyo que, en algunos aspectos, puede calificarse de decisivo cuando se plantea abiertamente la pregunta de cómo el gobierno y las FAS ucranianas pueden, a pesar de este apoyo, continuar resistiendo la envestida de un país agresor con el hipotéticamente segundo ejército más poderoso del mundo[2], al menos, en el momento de la invasión y en los análisis más prestigiosos internacionales.

Además del apoyo recibido por la empresa estadounidense *Space X* y su red de satélites Starlink para restaurar la conexión a internet (y mantenerse conectados), por parte de la población, el gobierno y las FAS ucranianas, éstas hacen un uso extensivo de las comunicaciones satelitales comerciales. En particular, conjuntamente con el apoyo suministrado por las señales de GPS, estas capacidades resultan críticas para la transmisión y compartición de datos que se ha convertido en un aspecto crítico y fundamental en el actual espacio de batalla, aunque este empleo sea más desconocido por ser menos publicitado. Estas capacidades satelitales posibilitan compartir datos entre los diferentes usuarios de una nube con objeto de disponer de una conciencia situacional en tiempo real, en base al sistema ucraniano Delta, sistema que ha resultado crucial en la eficaz ejecución de operaciones de las FAS ucranianas. Este sistema, desarrollado bajo la cobertura del Centro de Innovación y Desarrollo de Tecnologías de Defensa del MoD ucraniano, fue iniciado en 2017 con la intención de dotar a las FAS ucranianas de un sistema compatible con los estándares y

[1] Existen, además, informes de que la base industrial espacial rusa está sufriendo por las sanciones, posee una población envejecida y padece de corrupción. Todo ello, unido al actual conflicto en Ucrania, conforma un entorno complejo y difícil para intentar mantenerse en el nivel deseado de competencia con EEUU.

[2] Al menos, por el momento, Global Fire Power considera el ejército de la Federación de Rusia en segunda posición, con el mismo índice que el de la República Popular de China.

protocolos de la OTAN y vivió un impulso con la participación en los ejercicios «Sea Breeze» y «Rapid Trident», que permitieron validar algunas de las soluciones en él recogidas.

Sin embargo, el momento clave para Delta sería en 2021, cuando Ucrania tomó la decisión de pasar a operar el software (que da vida a Delta) desde la nube, en lugar de ejecutarlo desde servidores físicos en el país, que podían ser atacados cinéticamente. De hecho, se temía que la oleada inicial de ataques rusos, si llegaba a producirse, fuese dirigida directamente contra las capacidades de mando y control ucranianas, algo que se produjo, aunque finalmente con un éxito bastante escaso. Es más, se cree que el sistema Delta fue fundamental durante las primeras semanas de conflicto al brindar a los comandantes sobre el terreno «inteligencia en el campo de batalla en tiempo real recibida de drones y observadores».

La compartición de datos e información también forma parte esencial del sistema de gestión táctica automática del campo de batalla *Kropyva*, una aplicación de inteligencia cartográfica que se ejecuta en Android y que permite a un usuario con un terminal (generalmente una tableta) marcar fácilmente una posición enemiga, en base a la conexión con la red GPS (aunque puede emplear datos de Galileo), y generar automáticamente soluciones de tiro para la artillería o introducir correcciones si es necesario hacerlo[3].

En base a la adaptación realizada a la red *Starlink*, la información es posteriormente transmitida a las piezas de artillería cercanas, al tiempo que permite la coordinación de su fuego, lo que resulta en un fuego sincronizado contra el mismo objetivo desde varias posiciones separadas. Funcionando en forma de *Uber* para artillería, mediante la integración en red de distintos medios de reconocimiento (como radares de artillería o UAS), *Kropyva* ha permitido mejorar drásticamente el tiempo de reacción del fuego de artillería, al tiempo que ha reducido su vulnerabilidad. El tiempo medio necesario para desplegar piezas de artillería ucranianas (obuses o MLRS) y para abrir fuego de contrabatería se ha reducido drásticamente. Además, combinado con el uso sistemático de drones (como medios de observación, detección y corrección de fuego), *Kropyva* ha aumentado la efectividad de la artillería ucraniana de forma muy significativa, acelerando su *kill-chain* y actuando como un multiplicador de fuerza, obteniendo así una importante ventaja táctica que, en muchos casos, ha sido determinante.

Así mismo, en base a capacidades satelitales, la compartición de datos ha permitido también alimentar otro sistema de artillería en red, *GIS Arta* (*GIS for Artillery*), un software militar que se utiliza para coordinar ataques de artillería. Con una rápida determinación de objetivos en el ciclo de selección y determinación de objetivos (un minuto), no requiere que las unidades de reconocimiento utilicen dispositivos especializados (emplean *smartphones*) ni que las piezas de artillería estén agrupadas. De un nivel comparable, por ejemplo, con el *software* de la artillería alemana, su programación fue desarrollada por programadores ucranianos, con la participación de empresas británicas de mapas digitales. Una vez recopila la información sobre los objetivos (procedente de drones, fuentes de inteligencia u observadores avanzados), la aplicación de *Android* distribuye órdenes de disparo entre múltiples unidades de artillería. Este sistema ha venido utilizándose en las FAS ucranianas desde 2014 y ha demostrado ser muy eficaz en comparación con los métodos tradicionales de gestión y control de fuegos. Aunque ha demostrado ser un buen instrumento para

[3] Para ello, tiene en cuenta no solo las posiciones relativas del sistema al que se asigna el ataque y del objetivo, sino también muchos otros parámetros, como la propia forma del terreno o la información meteorológica.

diferentes actividades de control e inteligencia, debido a sus peculiaridades, su uso más extendido es en unidades de artillería.

Además, en el contexto de la función ISR, las imágenes satelitales han colaborado en la observación del movimiento de las fuerzas rusas, en el seguimiento de las rutas de evacuación humanitaria y en la recopilación de pruebas sobre potenciales crímenes de guerra. Empresas como *Maxar News Bureau, Planet y BlackSy* han proporcionado imágenes electroópticas a los clientes de defensa y a los medios de comunicación, y otras empresas como *Iceye y Capella Space* han recibido una gran demanda de sus imágenes radáricas SAR (radar de apertura sintética), al disponer de la capacidad de penetrar densas capas de nubes en Ucrania.

Por otra parte, los satélites no solo han permitido nuevos usos en el campo de los conflictos, también han facilitado nuevas estrategias en el ámbito de la diplomacia y la coerción, mediante la difusión pública de imágenes satelitales que, constituyendo una verdadera fuente de inteligencia, han obstaculizado las operaciones de propaganda rusas (mostrando públicamente las imágenes terribles de la realidad vivida en territorio ucraniano ocupado por el agresor) y han ayudado a construir la narrativa occidental sobre el conflicto que impera en Europa y, al menos, hasta la llegada de Trump, en EEUU. De alguna manera, estos nuevos empleos contribuyen a la reconfiguración del dominio espacial que estamos viviendo con nuevos actores y nuevas estrategias.

En este mismo contexto, otras empresas estadounidenses de análisis geoespacial, como *Spire Global y HawEye 360*, proveedoras de datos de radiofrecuencia, han utilizado sus satélites para rastrear, detectar y localizar perturbadores rusos de señal GPS que están causando, por ejemplo, que los UAVs ucranianos vean alterado su rumbo. Así, debido a la prominencia de capacidades industriales espaciales occidentales que posibilitan la resistencia de Ucrania, algunos observadores han descrito el conflicto como la "primera guerra espacial comercial". Estos ejemplos evidencian que tanto las empresas como los Estados han aprovechado esta crisis para implementar nuevos desarrollos y transformar con ello el dominio espacial.

EMPLEO RUSO DE CAPACIDADES DE CONTROL OFENSIVO DEL ESPACIO

Antes de comenzar este apartado, hemos de recordar primero que el control del espacio consiste en el empleo de capacidades para asegurar el acceso y para alcanzar y mantener un grado suficiente de libertad de acción en el espacio. Es evidente que, por el momento, la naturaleza del dominio espacial es tal que un control total no es viable por parte de ningún actor; sin embargo, ello no descarta la exigencia de proteger los satélites y actividades espaciales propias y aliadas para asegurar la continuidad de los servicios y productos que obtenemos a través del espacio. Conviene recordar, asimismo, que el control del espacio puede incluir actividades de control del espacio ofensivas, las denominadas OCS (del inglés, *Offensive Counter-Space*), también llamadas de respuesta en el entorno europeo, y actividades de control del espacio defensivas, las denominadas DCS (del inglés, *Defensive Counter-Space*), excluidas éstas del presente apartado por su total desconocimiento. Por tanto, ciñéndonos al contexto de las OCS rusas contempladas en este conflicto, se resaltan los siguientes aspectos:

(a) **Efectos no-físicos. Guerra electrónica y empleo del ciberespacio**

Rusia otorga una alta prioridad a la integración de la guerra electrónica en las operaciones militares y ha estado invirtiendo fuertemente en la modernización de esta capacidad con el ambicioso objetivo de incorporar capacidades EW en todo su ejército. En este contexto, tiene experiencia operativa con multitud de sistemas que pueden bloquear receptores GPS dentro de un área local, pudiendo interferir potencialmente el guiado de sistemas aéreos a control remoto, misiles y PGMs, capacidades que también utiliza en su territorio para proteger instalaciones estratégicas y personal seleccionado[4]. Así mismo, alguno de sus sistemas EW móviles puede bloquear terminales de usuarios de comunicaciones satelitales específicas dentro de rangos tácticos y es probable que, desde estaciones terrestres fijas, pueda bloquear enlaces ascendentes de comunicaciones satelitales en una amplia área. En lo que respecta al ciberespacio, Rusia ha demostrado capacidades significativas para negar los sistemas de mando y control, como demostraba poco antes de la invasión en Ucrania (como se detalla más adelante) y, según informes, mantiene operativo un grupo de piratas informáticos *Fancy Bear*[5] que se habría infiltrado con éxito, durante meses, en una red comercial estadounidense de satélites de comunicaciones.

En el contexto del conflicto en Ucrania, el mayor número de actuaciones antisatélite están vinculadas con la utilización de la guerra electrónica y el ciberespacio. Durante marzo/abril de 2021, más del 60 % de los vuelos de UAVs de la OSCE[6] afrontaron perturbación de señal GPS, incluso en áreas cercanas a la base de la OSCE (aproximadamente a 25 kms del frente), hechos corroborados por una empresa espacial comercial que detectó la señal de perturbación GPS. Así mismo, el día antes de la invasión, fuentes del gobierno ucraniano declaraban que un dron *Bayraktar* (TB-2) había experimentado una perturbación significativa de GPS provocando una pérdida de su control temporal.

Además, a lo largo de todo el conflicto y en varios lugares, se ha observado perturbación adicional de los Sistemas de Navegación Global por Satélite. En marzo de 2022, la Agencia de Seguridad Aérea de la UE informaba que la perturbación y/o posible engaño de dichos sistemas se había intensificado en áreas geográficas aledañas a la zona de conflicto y otras áreas. Así mismo, en base a diferentes fuentes, añadía que, desde el 24FEB2022, había cuatro áreas geográficas clave aledañas a la zona de conflicto en las que la interferencia de estos sistemas se había intensificado[7]. Todos estos lugares han experimentado una interferencia significativa en sistemas como el GPS y Galileo (corroborada por empresas de análisis de datos) que ha continuado a lo largo del conflicto, interferencias que hay que añadir a las detectadas en satélites occidentales con otras funciones, como la observación y la teledetección (como ha sido el caso de la perturbación experimentada por el radar Sentinel-1 del programa *Copernicus* de la UE en noviembre de 2023).

Más allá de la guerra electrónica contra diferentes servicios satelitales, en lo referente al ciberespacio, Rusia ha demostrado capacidades significativas para negar los sistemas de mando y control de Ucrania habilitados por satélites de comunicaciones comerciales, como

[4] Según fuentes abiertas, alrededor de Moscú se está llevando a cabo una perturbación del GPS; se especula que es para protegerla de ser atacada por drones ucranianos. Rusia habría estado instalando perturbadores de señales GPS en infraestructura doméstica (como torres de telefonía móvil) y en las cercanías del Kremlin. Así mismo (informado en 2020), dispositivos móviles en vehículos de perturbación de señal GPS acompañan al presidente Putin para garantizar su seguridad personal.

[5] *Fancy Bear* es un grupo amenaza persistente patrocinado por Rusia que es rastreado por el gobierno estadounidense y que se ha confirmado forma parte del antiguo Directorio Principal de Inteligencia del Estado Mayor General de la Federación de Rusia.

[6] Meses antes de la invasión, la OSCE se encontraba monitoreando la frontera entre Ucrania y Rusia con UAVs en misiones de sobrevuelo, sistemas que emplean la señal GPS civil sin protección para ayudar en su navegación

[7] A saber: la región de Kaliningrado, mar Báltico circundante y Estados vecinos; el este de Finlandia; el mar Negro; y el área del Mediterráneo Oriental cerca de Chipre, Turquía, Líbano, Siria e Israel, así como el norte de Irak.

muestra su actividad de "hackeo" de 24FEB2022. Una hora antes de invadir Ucrania, realizaba un ciberataque para negar la conectividad de la red KA-SAT de comunicaciones de la empresa *Viasat* y sus miles de terminales terrestres, introduciendo [en la red] el *malware wiper* y bloqueando los módems terrestres vía enlace descendente satelital[8]. Tras este exitoso ciberataque y la entrega de miles de terminales *Starlink* de la empresa *Space X* a Ucrania para solventar sus consecuencias (reconectando gobierno y civiles ucranianos a internet), Rusia intentó perturbar de nuevo los terminales terrestres para interrumpir las comunicaciones ucranianas. Sin embargo, según el DoD estadounidense, *SpaceX* pudo contrarrestar rápidamente los efectos de la perturbación arreglando líneas de código, de tal forma que los servicios no fueron gravemente interrumpidos desde este primer intento de perturbación a la red *Starlink* en marzo de 2022, intentos que han continuado con un éxito limitado.

Por último, aunque está claro que la perturbación electrónica contra este tipo de sistemas o productos ha sido generalizada y frecuente, en base a informes sobre vehículos y sistemas rusos capturados durante el conflicto, o de vídeos o imágenes publicados en redes sociales, existe poca confirmación concreta sobre qué dispositivos de perturbación de señales GPS o comunicaciones satelitales ha sido realmente utilizado.

(b) **Efectos físicos. DEW-ASAT-RPO**

En lo que se refiere a armas físicas, específicamente a la capacidad DA-ASAT (del inglés, *Antisatellite Direct Ascent*), demostrada con éxito en noviembre de 2021[9] (tras más de una década de desarrollos y pruebas), además de mantener sus capacidades existentes, en febrero de 2024, el gobierno estadounidense confirmaba que Rusia estaba desarrollando una nueva capacidad ASAT. Según un portavoz de la Casa Blanca, esta capacidad no estaba desplegada y no representaba una amenaza inmediata, afirmando que no podía atacar seres humanos ni causar destrucción física en la Tierra, pero que violaría el Tratado del Espacio Exterior de 1967[10]. Así mismo, aunque es posible que Rusia haya desarrollado un nuevo sistema láser antisatélite DEW (del inglés, *Directed Energy Weapon*) basado en tierra, apodado *Kalina*[11] (que podría deslumbrar o cegar satélites), no está claro que esté operativo, o sea capaz de realizar ataques para el control del espacio, no habiéndose detectado ninguna actividad sobre ninguna de estas dos capacidades en el conflicto actual.

Por otra parte, desde 2010 la Federación rusa ha estado probando tecnologías RPO (del inglés, *Rendez-vous Proximity Operations*) para operaciones de encuentro coorbital y de aproximación a otros satélites[12]. y Esta tecnología también podría utilizarse para aplicaciones no agresivas, incluida la vigilancia e inspección de satélites extranjeros (actividad que puede calificarse como espionaje espacial), en las que se incluye la mayoría de las actividades en órbita de este tipo (RPO)

---

[8] Además del gobierno y ejército ucranianos, este ciberataque existoso afectó a otros usuarios de Internet en toda Europa Central. Causó importantes daños materiales a civiles en países aliados (lo que obligó a reemplazar decenas de miles de terminales) y provocó importantes interrupciones, como la desconexión de miles de turbinas eólicas de la red eléctrica europea durante días.

[9] En este lanzamiento destruyó parcialmente un satélite fuera de servicio de la era soviética mediante un misil interceptador *Nudol*, siendo ésta su primera interceptación en órbita que creaba basura espacial.

[10] Al respecto, algunos han teorizado que Rusia está considerando un arma nuclear en el espacio, mientras otros sugieren que está desarrollando un satélite de guerra electrónica con propulsión nuclear. En cualquier caso, si se confirmara el programa de desarrollo de tal arma, ésta constituiría una forma eficaz de amenazar a un gran número de satélites, como las constelaciones de satélites que proliferan en la actualidad.

[11] Como parte de una estación de vigilancia espacial cerca del mar Negro.

[12] Además, existen evidencias que sugieren que Rusia puede haber comenzado un nuevo programa antisatélite coorbital llamado *Burevestnik*. Aunque poco o ningún detalle se ha confirmado sobre esta capacidad antisatélite, no es nueva. En septiembre de 2018, un MiG-31 modificado ruso fue fotografiado llevando un misil no identificado que supuestamente era una "maqueta" de un misil antisatélite ASAT lanzado desde el aire, sistema que, posteriormente, fue sugerido como el sistema de misiles *Burevestnik*.

realizadas hasta la fecha. En este sentido, aunque difíciles de identificar, un comportamiento inusual o amenazante de un satélite puede proporcionar información sobre capacidades e intenciones en este ámbito y, en ese tipo de comportamiento, Rusia tiene una larga historia, habiendo realizado actividades similares a lo largo de 2022 y 2023.

En cuanto a los efectos físicos referidos al conflicto en Ucrania, en lo que respecta a sistemas láser y de deslumbramiento DEW, es sorprendente que Rusia no haya conseguido emplear más armas de control ofensivo del espacio para erosionar la ventaja que ha supuesto la disponibilidad, por parte Ucrania, de productos de los satélites ISR comerciales que han permitido sus operaciones tácticas. Así mismo, a pesar del alto volumen de satélites de teledetección y otras plataformas que han estado y están proporcionando datos e inteligencia sobre las posiciones de las tropas rusas al ejército ucraniano, no existen informes independientemente verificados sobre que Rusia haya desplegado este tipo de capacidades DEW contra satélites en el conflicto en Ucrania. Y ello, a pesar de la importante propaganda rusa desplegada sobre esta capacidad; funcionarios rusos habrían exhibido en los últimos años el sistema *Peresvet* (un láser contra satélite basado en tierra) y Putin, en 2021, anunciaba que dicho sistema sería adaptado para ser empleado desde una plataforma aerotransportada.

En lo referente a operaciones RPO, en los últimos años, los satélites rusos vienen llevando a cabo conductas hostiles en el espacio, aunque es difícil afirmar de manera concluyente si estas actividades tienen como objetivo apoyar o probar armas ASAT orbitales o constituyen simplemente actividades de espionaje, o ambas cosas. En este sentido, el satélite inspector ruso *Luch* podría haber estado/estar apoyando la guerra de Rusia en Ucrania, recopilando señales de inteligencia, mediante la realización de maniobras de aproximación y merodeo de larga permanencia, cerca de satélites occidentales europeos[13]. Estas actividades, que se han visto incrementadas en los últimos cinco años, se han venido desarrollando también con el satélite *Luch 2* (lanzado en marzo de 2023) cerca de satélites occidentales, en este caso, estadounidenses y europeos.

CONCLUSIONES

Las capacidades espaciales han tenido una contribución significativa en este conflicto. El empleo de estas capacidades para comunicaciones, ISR y teledetección de señales de perturbación, así como para el ciclo de selección y ataque a objetivos, ha tenido un elevado impacto, fundamentalmente en el bando ucraniano, gracias al apoyo recibido por los países occidentales. Ello es así, en la medida, que han potenciado las comunicaciones de las fuerzas ucranianas y conectado al pueblo ucraniano con el mundo exterior; han proporcionado información sobre el movimiento de fuerzas rusas y sobre rutas de evacuación humanitaria; han permitido, en base a la compartición de datos, operar en red de forma eficaz; y han posibilitado recopilar pruebas sobre potenciales crímenes de guerra (mediante las imágenes satelitales) o detectar y localizar fuentes de perturbación de los sistemas de navegación satelital.

Así mismo, se ha detectado una prominencia de capacidades industriales civiles espaciales, en apoyo a la resiliencia, que puede marcar pautas para futuros conflictos. El incremento del apoyo, por parte de capacidades del sector civil, constituye un reflejo del aumento significativo de satélites lanzados al espacio en los últimos años. No obstante,

[13] Entre ellos, varios satélites *Intelsat* empleados para comunicaciones comerciales o militares seguras.

debido a la falta, en general, de información al respecto, resulta difícil de medir el nivel del impacto que dicho apoyo haya podido tener en la ejecución de las operaciones.

Este apoyo satelital de terceros, - actores estatales y no-estatales -, ha permitido además un nivel de transparencia sin precedentes en el espacio de batalla, desclasificando inteligencia sensible (al desvelar planes e intenciones de Moscú previas a la invasión), publicando imágenes sobre la concentración de fuerzas rusas (previas también a la invasión) y transmitiendo, a través de las redes sociales, los «horrores de la guerra» a la opinión pública. Este apoyo ha facilitado también nuevas estrategias en diplomacia y coerción, mediante la difusión pública de imágenes satelitales que, como verdadera fuente de inteligencia, han obstaculizado operaciones de propaganda rusas (mostrando la realidad vivida en territorio ucraniano) y han ayudado a construir la narrativa occidental sobre el conflicto. Estos nuevos empleos contribuyen, sin duda, a la reconfiguración del dominio espacial a la que estamos asistiendo con nuevos actores y nuevas estrategias.

En lo que respecta a la Federación Rusa, el empleo de capacidades de control ofensivo en el espacio, relacionado con el conflicto, es una buena muestra de que estas capacidades no forman parte, desde hace tiempo, de la «ciencia ficción». Los empleos más significativos han estado y están relacionados, fundamentalmente, con el empleo del ciberespacio o de la guerra electrónica. El empleo de ambos, guerra electrónica y ataques en el ciberespacio, contra los sistemas espaciales, así como la incertidumbre sobre el empleo ruso de armas láser y sobre el comportamiento inusual de los satélites inspectores rusos *Luch* y *Luch 2,* alertan sobre los efectos posibles en el espacio ultraterrestre. Y es que los ataques de Rusia contra las capacidades espaciales utilizadas por Ucrania son un ejemplo de cómo pueden emplearse, y probablemente serán empleadas, las armas de control ofensivo del espacio (llamadas actividades o misiones de respuesta en el entorno europeo) antes y durante futuros conflictos. No obstante, es sorprendente que Rusia no haya conseguido emplear más armas de control ofensivo del espacio para erosionar la ventaja que ha supuesto la disponibilidad ucraniana de productos procedentes del espacio.

LECCIONES IDENTIFICADAS, Y ALGUNAS APRENDIDAS

A modo de preludio de futuros conflictos, del empleo observado de las capacidades espaciales, por parte de ambos bandos, podemos extraer algunas lecciones, alguna ya previamente aprendida.

(a) Puede confirmarse la **contribución significativa y crucial de los productos y servicios obtenidos desde el espacio** en el planeamiento y ejecución de operaciones militares. Aunque la importancia de este apoyo ya es lección aprendida desde hace tiempo, este conflicto ha puesto de manifiesto, más aún si cabe, la relevancia de la integración de capacidades en la eficacia del ciclo de selección y ataque de objetivos y de la famosa *kill-chain,* en base al apoyo de activos satelitales. Este apoyo, en algunos aspectos, puede calificarse de decisivo; su ausencia difícilmente hubiera permitido al gobierno y a las FAS ucranianas seguir resistiendo la agresión del ejército de la Federación Rusa.

(b) **La mayor utilización del apoyo desde el espacio**, en actividades adicionales a las ya conocidas, parece estar **reconfigurando el espacio como dominio operativo**. En base a nuevas posibilidades de actuación, permitidas por el apoyo desde el espacio, podemos estar asistiendo a una reconfiguración del espacio como dominio operativo.

Este conflicto ha demostrado igualmente la posibilidad de emplear productos rerivados del espacio no sólo para contrarrestar la narrativa del adversario, sino también para construir la propia. Esta capacidad puede resultar crucial en el empleo de capacidades militares y no-militares como instrumento fundamental de poder de los Estados y de actores no-estatales, más aún si cabe, en el actual entorno multi-dominio que precisa, sí o sí, de un enfoque integral cuando se contemplan todo tipo de capacidades.

(c) **Sin poseer activos espaciales**, los combatientes **pueden realizar operaciones habilitadas por el espacio**. Este conflicto demuestra que lo importante es tener acceso a los productos de los sistemas espaciales, no poseer satélites. Con la explosión de las comunicaciones comerciales y los servicios de imágenes, muchos combatientes tendrán acceso a esos productos. Sin embargo, el acceso no será universal; las empresas occidentales están muy por delante en sus capacidades y están sujetas a límites formales e informales sobre los clientes a los que venden datos. Facilitar el acceso comercial, proporcionar financiación y ofrecer formación y entrenamiento en el uso de productos espaciales comerciales (o compartir productos clasificados) puede afectar, en gran medida, las actuaciones en el espacio de batalla. Además, esos esfuerzos son relativamente de bajo coste y, tal vez, visiblemente menos provocativos que los envíos de armas.

(d) Las operaciones o actividades contra espaciales tienen **más probabilidades de ser cibernéticas o electrónicas** (efectos no-físicos) que cinéticas (basadas en efectos físicos). Independientemente de que la demostración ASAT rusa de noviembre de 2021 fue pensada como una advertencia a la OTAN con respecto a Ucrania, no ha habido informes sobre el conflicto de que se hayan intentado ataques espaciales físicos. Sin embargo, aunque después del ataque a la red de Viasat *SpaceX* recuperó la conexión de comunicaciones satelitales, el ciberataque ruso, previo a la invasión, resultó exitoso. Las interferencias cibernéticas y electrónicas son más probables que los ataques espaciales físicos, por varias razones: no generan escombros, son menos costosos, ofrecen la posibilidad de negar el ataque y es menos probable que estimulen una represalia armada.

Así mismo, los acontecimientos en Ucrania también demuestran el valor de la redundancia contra las armas antisatélite; es decir, depender de una gran cantidad de satélites[14] (constelación), en lugar de unos cuantos satélites grandes, tendencia a la que parecen derivar los servicios de comunicaciones y teledetección. Cierto es, sin embargo, que un ciberataque exitoso puede perjudicar las terminales terrestres y el acceso de los usuarios, haciendo irrelevante la existencia de una flota de satélites (megaconstelación).

(e) Las **empresas comerciales como actores importantes, y ¿objetivos?** El conflicto ucraniano pone de relieve el crecimiento explosivo del sector espacial comercial. Aunque el ejército estadounidense lleva mucho tiempo alquilando ancho de banda en satélites comerciales, la integración de *Starlink* en el espacio de batalla y el uso táctico de la teledetección comercial ha sido innovador. No sorprende que Rusia señalara que los satélites de las empresas que trabajaban directamente con el ejército

[14] Starlink tenía, al principio, dos mil quinientos satélites en servicio, demasiados para que Rusia los derribara con sus pocos y costosos interceptores.

ucraniano eran objetivos militares legítimos[15]; es probable que los rusos tengan razón en virtud del derecho internacional. La comunidad internacional acepta el principio de que se puede atacar a terceros que contribuyan directa y conscientemente al esfuerzo bélico de un combatiente, dentro de los límites de la proporcionalidad y cuando causen mínimos daños colaterales. Lo que no está claro es cómo se respondería a los ataques a sistemas espaciales comerciales, ya sea por medios físicos o a través del ciberespacio.

(f) **Evaluación de las capacidades espaciales rusas**. A pesar de la larga historia de los vuelos espaciales soviéticos y rusos, no es obvio que las FAS rusas se hayan beneficiado más del espacio que el bando ucraniano. Las dificultades rusas de mando y control, la ausencia de una aparente ventaja en ISR y los errores sorprendentemente grandes detectados en el lanzamiento de municiones de precisión (presumiblemente guiadas por el sistema de navegación satelital ruso GLONASS) son indicios de un empleo menos eficaz de los sistemas espaciales que el que realizan EEUU o sus aliados, lo que no resulta sorprendente. De hecho, los satélites militares rusos de comunicaciones y vigilancia están muy por detrás de los estadounidenses en número y tecnología; las sanciones en tecnología impuestas desde 2014 han retrasado el desarrollo de las capacidades espaciales rusas, entre otras razones, por la falta de componentes electrónicos específicos para ello. Ello, sumado a la probable disminución de ingresos del gobierno ruso, hacen dudoso que Rusia pueda disminuir la brecha espacial.

[15] El subdirector del departamento de no proliferación y armas del ministerio de exteriores ruso, *Konstantin Vorontsov*, advertía el 26 de octubre de 2022 en la Asamblea General (NNUU) que la infraestructura casi civil podía convertirse en un objetivo legítimo de represalia, indicando que Moscú consideraba a las empresas comerciales proveedoras de servicios a gobiernos y militares como objetivos legítimos en tiempos de conflicto.