ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

Todas las guerras son tecnológicas: la de Ucrania, aún más

Antonio Fonfría
Academia de las Ciencias y las Artes Militares
Sección de Futuro de las Operaciones Militares

21 de abril de 2023

No se descubre nada nuevo si se dice que las guerras poseen un componente tecnológico importante que puede decidir el resultado de las mismas. La Historia así lo muestra desde las guerras más ancestrales hasta hoy. Sin embargo, han cambiado numerosos aspectos que han de tenerse muy en consideración. Hasta los años 80 del siglo XX los mayores generadores de tecnologías de uso militar eran las principales empresas del ámbito de la defensa. Sin embargo, cada vez más, las empresas civiles han desarrollado tecnologías con capacidad para ser utilizadas en los conflictos y, sensu contrario, las firmas que tradicionalmente operaban en el orbe militar han ido generando tecnologías de uso dual dada la estrechez de los mercados militares.

En la guerra de Ucrania se está constatando no sólo la importancia de la tecnología sino algunos hechos que trascienden a la misma pero que se encuentran inextricablemente unidos a ellas. Quizá el primero de ellos es preguntarse cómo un país como Ucrania con un sistema de innovación muy débil que no genera importantes innovaciones tecnológicas, ha sido capaz de hacer frente a una potencia militar como Rusia. La respuesta obvia es el apoyo a través de sistemas de armas –algunos altamente sofisticados, tanto en su tecnología como en su uso–

recibidos de los aliados. Pero, además, hay un factor clave que habitualmente no se tiene en consideración: el aprendizaje.

Así, la capacidad de aprender el manejo de sistemas de armas complejos en tiempos realmente reducidos por parte de los militares ucranianos es una ventaja que muestra sus resultados en el campo de batalla. Si bien la conceptualización de la innovación tecnológica enseña que el aprendizaje es acumulativo, requiere tiempo y esfuerzo, y las fuerzas ucranianas han demostrado ser altamente eficientes en este sentido. Lo cual lleva a una pregunta colateral: ¿podrían ser más eficientes aprendiendo y, por lo tanto, recortar tiempos y costes de enseñanza los países aliados?

Con relación a la sofisticación tecnológica de los sistemas que se están utilizando por parte de Ucrania, es importante distinguir al menos tres niveles de complejidad tecnológica que se han combinado en el conflicto. En primer lugar, Ucrania ha recibido sistemas complejos de alta sofisticación técnica y que requieren un aprendizaje de uso que no es en absoluto obvio y, que demandan ciertas capacidades de aprendizaje previas. Sería el caso de los sistemas HIMARS, los carros de combate Leopardo o de las baterías *Patriot*. En segundo lugar, se encuentran otros sistemas de un nivel de complejidad tecnológica menor, con tiempos y necesidades de aprendizaje más moderados y de más sencilla utilización como los drones turcos -*Bayraktar TB2*-, o el estadounidense *ScanEagle* que ofrecen importantes ventajas tácticas y operativas. Por último, se encuentran sistemas más sencillos -en su uso, que no en su complejidad tecnológica-, como los drones comerciales o los terminales satelitales que se han mostrado muy útiles y necesarios en el mando y control. Pero quizá el nudo gordiano sea la capacidad para poner juntos estos sistemas obteniendo de su uso la mayor «rentabilidad» posible, algo que parece que se está obteniendo por parte de las fuerzas ucranianas.

Una segunda perspectiva relativa al uso de las tecnologías en la actual situación tiene que ver con las grandes empresas tecnológicas multinacionales como Google y algunas más. Comenzando por su propio tamaño, estas empresas facturan anualmente cuantías equiparables al PIB de algunos países pequeños, lo cual les confiere un poder económico que no se había dado hasta hace pocos años. Más aún, su posicionamiento global les permite tener un enorme poder e influencia en términos tanto económicos, como «geopolíticos”. Este último aspecto implica que su posicionamiento en la guerra de Ucrania es decisivo en el desarrollo del conflicto ya que la posibilidad de acceso a sus tecnologías -internet, satélites, etc…-, o su negación a uno de los bandos implicados en la contienda puede cambiar de forma muy sustancial el devenir, incluso el resultado, del conflicto.

Hay numerosos ejemplos de lo anterior, sin embargo, esto posee igualmente un coste para las empresas que, es de suponer, estén dispuestas a soportar hasta cierto punto, por lo que en algún momento -si no a priori-, habrán de negociar con determinadas administraciones de varios países para el reparto de dichas cargas económicas o para resarcirse de ellas. Obviamente, posee igualmente un coste reputacional que ha sido considerado por las firmas y que condiciona su desarrollo futuro en numerosos países.

Sin embargo, surgen algunas cuestiones que no están claras y que requieren de un cierto análisis. Entre ellas cabría destacar durante cuánto tiempo van a estar estas empresas aportando sus tecnologías en un conflicto que posiblemente les supongan ciertas pérdidas económicas, como ya se ha constatado con el caso de algunas empresas y que puede alargarse en el tiempo. En otras palabras, el grado de compromiso puede depender de la cuenta de resultados. Una segunda cuestión es la dependencia que este conflicto -y los que vengan después-, está generando en empresas privadas que pueden o no compartir visiones o perspectivas sobre determinados asuntos internacionales con distintos países, es decir, hoy se encuentran a favor de uno de los contendientes, pero en un hipotético conflicto futuro se pueden posicionar de forma distinta. Cierto es que lo mismo ocurre con los países y que sus estrategias geopolíticas, económicas y militares cambian a lo largo del tiempo, pero al incluir actores empresariales en el desarrollo de los conflictos -algo que ha ocurrido en numerosas ocasiones-, con un poder tecno-económico sin parangón en la historia, se abren un conjunto de interrogantes que, al menos, es necesario considerar.

De hecho, uno de los más relevantes es la gran dependencia que tienen los países de esas tecnologías, en las cuales se basan las puramente militares cada vez en mayor medida -véase el ejemplo del *Future Combat Air System* (FCAS) o de numerosas aplicaciones basadas en tecnologías de satélites-. Eso otorga un poder muy elevado a las empresas, poder que no tienen los propios países, lo cual les hace vulnerables y dependientes de decisiones empresariales. ¿Cómo deberían actuar los países ante esta nueva situación? No hay una respuesta clara a esta cuestión, aunque una de las enseñanzas que nos provee la guerra de Ucrania es que la colaboración público-privada llevada a cabo de manera formal y la implicación empresarial moderada en la gestión de actividades públicas basadas en tecnologías de estas grandes corporaciones, junto con políticas que tiendan a atenuar dicho poder, son ingredientes básicos para cualquier país. Sin embargo, en el ámbito de la defensa no es posible dejar de contar con estas empresas.

Se abre aquí una situación de muy compleja gestión, en cuya base se encuentra la ciberseguridad. Desde una perspectiva internacional, los Estados se consideran unidades comparables y es el equilibrio de poder lo que los conduce a actuar de

manera específica en este ámbito. La capacidad ciber ofensiva de un Estado es un instrumento abstracto de poder que puede utilizarse con diversos fines, tanto en tiempos de paz como durante los conflictos. Sin embargo, los Estados son también actores llamados a restablecer el control del uso indebido del ciberespacio mediante las normas internacionales, a menudo buscando lecciones aprendidas de anteriores problemas y soluciones en materia de seguridad. En su papel de garantes de la seguridad, los Estados actúan o bien maximizando el poder o la seguridad o bien minimizando las amenazas.

Timeframe	Technological Capability of State	Coping Strategy and Tactics		Explanation
Before embargo	Basic		Stockpile	Stockpile spares prior to the embargo
During embargo		Dependency: Continued dependency on foreign design, development, manufacturing, and supply	Cannibalise	Cannibalise older and damaged airframes
			Procure	Look for new suppliers for spare parts
				Bring in expertise by enticing foreign technicians
				Scour black or grey markets for spares
				Look for new suppliers for aircraft
		Self-sufficiency? Development of enhanced capabilities domestically	Maintain	Develop (or use) the capability to produce spares domestically
			Replicate	Develop (or use) the capability to replicate existing designs
	Sophisticated		Innovate	Develop (or use) the capability to design and produce new aircraft

Figure 1: How do Air Forces Respond to Embargoes?

Fuente: Salisbury, D. "Clipped wings? The impact of arms embargoes on Russian air power in Ukraine and beyond" Freeman Air & Space Institute. King´s College, London (2023).

Históricamente, se observa una evolución en las funciones del Estado que coincide con tres fases de la política de ciberseguridad. En una primera función, el Estado aparece como propietario de redes o sistemas de información que pueden estar en peligro. En una segunda función, es el actor que debe resolver el problema desde el punto de vista de la política de seguridad. En tercer y último lugar, el Estado -o ciertas unidades individuales del Estado- aparece como causante del problema. Es importante destacar que esta evolución es aditiva: se asumen nuevas funciones mientras se mantienen las antiguas, lo que aumenta la complejidad del ámbito de la política de ciberseguridad. Esta mutación en los roles y en la orientación de la

política de ciberseguridad la revela como una cuestión transversal, que requiere la cooperación de una amplia variedad de agentes que proceden no solo de diversas autoridades públicas, sino también de las empresas y de la sociedad civil.

En caso de conflicto, la posible regulación que hayan planteado los Estados pasa a un segundo plano y los objetivos son muy diferentes. Si a ello se une la dificultad para establecer el origen de un ciberataque, en muchas ocasiones esta parte de la amenaza en la zona gris pasa a ser un riesgo mucho más real que cualquier ataque cinético. En el caso de la guerra de Ucrania, la capacidad de ciberataque de Rusia a Ucrania se ha visto contrarrestada por las aportaciones occidentales, no sólo a través de los sistemas militares, sino también a través de las mencionadas empresas privadas especializadas en este tema y la sociedad civil, en muchos casos a través de las redes sociales.

La tecnología se ha mostrado como caballo de batalla desde el principio del conflicto y no sólo en el teatro de operaciones, sino también como instrumento debilitador de las actividades rusas tanto de producción, como de generación de nuevas tecnologías y conocimientos. Es a través de las sanciones como se ha utilizado. Así, desde el comienzo de la guerra, se endurecieron las sanciones a la exportación de productos de doble uso, se prohibió el suministro a Rusia de productos y tecnologías aptos para el refinado de petróleo, se prohibió igualmente la financiación pública del comercio con Rusia y, más importante, se prohibió la exportación de productos y tecnologías para la industria aeronáutica, espacial y de navegación marítima.

No obstante, el efecto de las medidas relacionadas con el control del comercio de tecnologías con Rusia posee un impacto mayor a largo plazo, cuando se comiencen a notar problemas de abastecimiento de sistemas de alta tecnología a través de las importaciones o, en el caso de que los costes de desarrollo de tecnologías sean mucho más elevados que hasta antes de la guerra. A ello es necesario unir la práctica desaparición de las relaciones científicas internacionales de Rusia, ya que los países occidentales han cortado básicamente todo intercambio con aquel país. Más aún, tal y como expresa el gráfico adjunto a modo de ejemplo, a medida que la sofisticación tecnológica es más acusada y cuanto menor sea la autosuficiencia del país, mayor será el impacto de las sanciones. Esto choca con el apoyo, bien directo, bien indirecto que recibe Rusia de otros países y con cierto grado de flexibilidad que las propias sanciones han mostrado, por lo que su impacto ha sido muy moderado. Este contexto enlaza con el concepto de autonomía estratégica que la UE viene desarrollando últimamente.

En definitiva, la tecnología está conduciendo a una situación que hasta hace unos pocos años no era ni tan siquiera presumible o no se encontraba en los más

avanzados análisis de prospectiva e inteligencia. Su papel en la guerra de Ucrania está siendo decisivo, pero no sólo desde la perspectiva de su uso en las operaciones, sino mucho más allá y desde muy diversas perspectivas como se ha expuesto. Su consideración de manera conjunta expone un lienzo complejo que conduce al concepto de interdependencia de forma inexorable.