CUMBRE MADRID 2022 · LA OTAN ANTE UN CAMBIO DE ERA

Nº 8 | 13 Julio 2022

Tecnologías emergentes y balance de fuerzas

Jose Luis Calvo Albero

Entre las muchas razones que llevaron a la creación de la OTAN, se encontraba el desigual balance de fuerzas militares, sobre todo terrestres, en la Europa posterior a la Segunda Guerra Mundial. La Alianza nació como el intento de algunos países europeos por neutralizar esa desigualdad mediante la unión y, sobre todo, mediante la voluntad de Estados Unidos de demostrar su compromiso en la defensa de Europa Occidental.

La desigualdad de fuerzas se mantuvo durante gran parte de la Guerra Fría, hasta el punto de que la doctrina OTAN giró durante mucho tiempo sobre la necesidad de utilizar armas nucleares para compensar la debilidad en fuerzas convencionales frente a la Unión Soviética y el Pacto de Varsovia. Esa situación cambió progresivamente a partir de los años 70, cuando se comenzó a hablar de una Revolución en los Asuntos Militares que podría compensar el número con tecnología y procedimientos novedosos.

La caída de la Unión Soviética cambió totalmente el concepto de balance de fuerzas, que en los años 90 se aplicó sencillamente a un equilibrio que resultase cómodo tanto para la OTAN como

para los herederos de la URSS. Ese equilibrio se intentaba alcanzar en un escenario de distensión y reducción de fuerzas que se prolongó hasta los primeros años del siglo XXI.

La actitud progresivamente más asertiva de la Federación Rusa y el crecimiento de su poder militar comenzaron a causar preocupaciones en los círculos de la Alianza, que se convirtieron en una clara sensación de amenaza a partir de la intervención rusa en Ucrania en 2014. Los miembros europeos de la organización se encontraban en una situación especialmente preocupante, pues décadas de distensión y de orientación hacia operaciones de paz y estabilidad habían erosionado muchas capacidades militares básicas. El renacimiento del poder militar ruso y la disposición del Kremlin a utilizarlo provocó una reacción, pero ésta no fue lo suficientemente rápida ni intensa como para evitar la crisis que desembocó en la invasión rusa de Ucrania en febrero de 2022.

En una Europa sacudida por el mayor conflicto en su suelo desde la Segunda Guerra Mundial, el papel de la Alianza Atlántica se ha visto muy reforzado y el concepto de balance y equilibrio de fuerzas ha vuelto a adquirir la máxima actualidad. Las prestaciones de las fuerzas armadas rusas en Ucrania se han mostrado muy pobres, pero eso no borra la certeza de que Rusia se ha atrevido a lanzarse a esa aventura precisamente por la percepción de debilidad política y militar en sus vecinos del Oeste. Surge ahora la idea de una arquitectura de seguridad nueva, que permita ejercer una disuasión eficaz sin que aparezca a la vez como amenazadora.

La tecnología y la capacidad para gestionarla es la clave para lograr ese objetivo, aunque el número sigue teniendo su importancia cuando se trata de utilizar la fuerza militar. En este capítulo se analizará cómo puede conseguir la Alianza esas capacidades que lleven a un balance de fuerzas que garantice la paz en Europa. La guerra en Ucrania está demostrando de manera muy clara por dónde debe ir el futuro de las capacidades, la organización y los procedimientos de los ejércitos europeos y cuáles serán las tecnologías clave en ese futuro.

Tecnología, información y mentalidad. Las capacidades militares clave en el siglo XXI

A lo largo del siglo XX se producen varios momentos clave en los que las experiencias bélicas configuran un modelo militar novedoso, que rompe al menos parcialmente con el modelo

anterior. Uno de esos momentos tuvo lugar en los años 70 y 80, cuando el modelo militar norteamericano intenta recuperarse de una humillante derrota en Vietnam. El análisis de una posible guerra en Europa contra el Pacto de Varsovia llevó a los planificadores norteamericanos a combinar procedimientos relativamente tradicionales con otros muy innovadores. Por un lado, se intentó regresar a la "guerra de maniobra" desarrollada por Alemania en el último conflicto mundial, que requiere rapidez en la decisión y una gran iniciativa en todos los niveles de mando. Por otro, se explotaron las capacidades de una revolución tecnológica entonces en ciernes, que se materializará más tarde en el moderno mundo digital.

La tecnología ofrecía ya entonces posibilidades inéditas para un nivel de observación, reconocimiento y localización de objetivos en el campo de batalla como no se había conocido anteriormente. Además, ofrecía soluciones para aumentar considerablemente tanto el alcance de las armas como su precisión, mediante sistemas de guía terminal. Por último, también permitía acelerar de manera muy significativa el tiempo que transcurre entre la localización de un objetivo y el momento en el que éste es batido por un arma. Las redes digitales, entonces todavía embrionarias, permitían la difusión casi instantánea de información entre sensores, órganos de decisión y sistemas de armas.

El modelo que surgió de esta reacción norteamericana se denominó <<Batalla Aeroterrestre>> (*Air Land Battle*) y fue adoptado por la OTAN en los años 80 como concepto FOFA (*Follow-on Forces Attack*). Se consagró en el campo de batalla durante la Guerra del Golfo en 1991 y se convirtió desde entonces en el símbolo de la supremacía militar norteamericana.

En los últimos años de la Guerra Fría este concepto cambió radicalmente el balance de fuerzas en Europa. El gran problema estratégico de la OTAN fue siempre la improbabilidad de detener a las abigarradas formaciones blindadas del Pacto de Varsovia utilizando medios exclusivamente convencionales (Pedlow, 1997:XIV). El recurso a armas nucleares tácticas ante un ataque masivo parecía inevitable, pero abría la puerta a una escalada nuclear de consecuencias imprevisibles.

La Batalla Aeroterrestre cambió esa dinámica. Las nuevas tecnologías aplicadas a sistemas militares y el dinamismo que proporcionaba la iniciativa de los mandos permitían dislocar el despliegue enemigo en toda su profundidad antes de que pudiera introducirse en territorio

aliado. La opción nuclear pasaba a ser una respuesta de emergencia caso de que el adversario decidiese hacer uso de ella.

Durante las décadas que siguieron a la Guerra Fría, la Batalla Aeroterrestre, sucesivamente perfeccionada y modificada, fue el modelo vigente en la Alianza Atlántica para un conflicto convencional y se aplicó en mayor o menor medida en las intervenciones de la OTAN en Bosnia Herzegovina (1995), Kosovo (1999) y Libia (2011). No obstante, el modelo era también bastante exigente y requería excelencia tecnológica, mandos muy bien formados y motivados y procedimientos flexibles. La poca probabilidad de un conflicto en Europa hizo que los ejércitos europeos, e incluso el norteamericano se relajasen y dejasen deteriorarse muchas capacidades básicas. La tendencia se orientó a centrarse esencialmente en operaciones aéreas con armas guiadas contra adversarios que no disponían de un sistema avanzado de defensa aérea. Se olvidó con frecuencia toda la compleja acción interarmas e interejércitos que la Batalla Aeroterrestre llevaba asociada, así como la necesidad de mantener unos mandos intermedios muy bien formados para poder utilizar eficazmente su iniciativa (Romjue:1984, 55-59).

Además, tanto Estados Unidos como la OTAN se enzarzaron en conflictos para los que la Batalla Aeroterrestre no funcionaba tan bien. Apareció primero un modelo de conflicto asimétrico muy basado en la guerrilla urbana y el terrorismo, para pasar después al más complejo modelo híbrido, que conjugaba acciones militares irregulares y convencionales con el uso de herramientas no militares (Hoffman, 2009). La generalización de internet primero y de los *smartphones* después, multiplicaba las posibilidades de realizar acciones hostiles no militares, utilizando bien ciberataques, bien campañas de desinformación que utilizaban las redes digitales como vehículo para su rápida difusión. En ese tipo de ataques es muy difícil identificar a su autor y, aunque el daño que consiguen no suele ser decisivo, sí que producen un efecto muy desestabilizador. Además, el exceso de confianza en la tecnología llevó a disfunciones, como que el sistema proporcionaba un constante flujo de información que no se interpretaba adecuadamente (Erwin, 2012).

A partir de 2006 la actitud de Rusia se hizo cada vez más agresiva. La primera advertencia se produjo en 2008 en la guerra contra Georgia y en 2014 el Kremlin mostró su voluntad de utilizar la fuerza para mantener su influencia sobre Ucrania. Al mismo tiempo, el crecimiento económico y militar de China se veía también como una amenaza, no tanto en la OTAN como en

Estados Unidos. En 2011, el presidente Obama señaló ya a China como el competidor económico y geopolítico más peligroso para Washington y lanzó la idea de reforzar la presencia y el esfuerzo económico y militar norteamericano en el Pacífico (Lieberthal, 2011).

Ante este nuevo desafío, la reacción de la Alianza Atlántica fue desigual, pero adquirió una fuerza notable en Estados Unidos. Los pobres resultados en conflictos como Iraq o Afganistán y el renacimiento de la amenaza militar en Europa y el Pacífico llevaron a buscar una solución militar que, como la Batalla Aeroterrestre treinta años atrás, permitiese recuperar la hegemonía militar norteamericana.

A esta reacción se la denominó *third offset strategy* o <<Tercera estrategia de compensación>> (Colom, 2015). El nombre derivaba de lo que se consideraban conceptos estratégicos previos para compensar la inferioridad militar norteamericana. La primera fue la respuesta nuclear masiva de la era Eisenhower en los años 50, y la segunda la modernización y deriva tecnológica del arsenal militar norteamericano que culminó esencialmente en la Batalla Aeroterrestre. Tras la decepción de la guerra contra el terrorismo y la pérdida de capacidades convencionales era el momento de reaccionar de nuevo.

Dentro de este impulso, aparecieron conceptos como la <<Batalla Multidominio>>, que buscaba la sincronización de acciones en los diferentes dominios del campo de batalla (aire, tierra, mar, espacio exterior, ciberespacio y entorno cognitivo) o la <<Guerra Mosaico>> (Grayson, 2018), que buscaba la sinergia de múltiples acciones simultáneas de sistemas en su mayoría no tripulados para desarticular el despliegue enemigo y romper la coherencia de su acción. Lo cierto es que la importancia de los sistemas no tripulados aumentó exponencialmente, sobre todo de los aéreos que se habían diversificado para cubrir funciones que iban desde el reconocimiento al ataque a tierra, pasando por la guerra electrónica o la alerta temprana. Una novedad en la evolución de estos sistemas fue que su desarrollo siguió dos líneas diferentes. Por un lado, la tradicional de diseñar plataformas cada vez más sofisticadas, complejas y caras. Por otro, y liderada por potencias pequeñas y medias, e incluso milicias y grupos terroristas, la tendencia que buscaba emplear un gran número de plataformas sencillas, baratas y flexibles (Marcus, 2022).

En este proceso se demostró que la aplicación práctica de nuevas tecnologías a sistemas de armas y equipos militares es un proceso complejo. Tan importante resulta el grado de desarrollo tecnológico como el acierto a la hora de diseñar una doctrina de empleo apropiada para un nuevo sistema o ser capaz de integrar los materiales "nuevos" y "viejos" en un sistema coherente (Eaglen & Ferrari, 2020). Se ha comprobado, por ejemplo, el buen resultado de integrar sistemas de fuego en principio anticuados (artillería de la Guerra Fría) con sistemas de dirección de fuego que combinan la acción de drones equipados con cámaras de alta resolución y de sistemas de posicionamiento global que transmiten inmediatamente la situación exacta de la pieza y el objetivo. El resultado es un arma con prestaciones considerablemente incrementadas a un coste mucho más asumible que la producción de un sistema completamente nuevo.

Pese a las novedades, el aspecto principal de las operaciones sigue siendo la interconexión entre los diferentes elementos del sistema formado por las fuerzas militares. Las comunicaciones fiables y rápidas dentro de una red compuesta por sensores, centros de decisión, elementos de fuego, unidades de maniobra y apoyos logísticos constituyen la clave del sistema. La adición de nuevos elementos tecnológicos, como el 5G, la inteligencia artificial o, en el futuro, la computación cuántica, pueden permitir superar los cuellos de botella que se generaban con los primitivos sistemas digitales utilizados durante la Batalla Aeroterrestre. En definitiva, lo más importante de una fuerza armada es, como lo ha sido siempre, su sistema nervioso. La red que permite que la información fluya con rapidez, las decisiones sean oportunas y la capacidad de reacción del adversario se vea reducida al mínimo.

Las lecciones de Ucrania

La invasión rusa de Ucrania en 2022 fue una sorpresa en muchos aspectos. El primero de ellos que la propia invasión llegase a producirse, abriendo con ello el mayor conflicto convencional en Europa desde 1945. El segundo fue la forma en la que se produjo, con un peso abrumador de las fuerzas convencionales en detrimento de otros instrumentos híbridos, como la desinformación o los ciberataques, que, aunque se han manifestado durante el conflicto, han tenido una importancia más bien complementaria (Fendorf & Miller, 2022). Por último,

sorprendió también el bajo rendimiento de las fuerzas armadas rusas, de las que se esperaba mucho más, sobre todo de sus capacidades para integrar las nuevas tecnologías en el uso de los fuegos, los sistemas no tripulados o el mando y control[1].

La primera lección que puede extraerse del conflicto reitera lo expuesto sobre la importancia de la actuación en red y el carácter esencial de los sistemas de mando y control. Ucrania sobrevivió como Estado independiente porque su sistema de dirección política y de mando y control militar sobrevivió a la primera embestida rusa. En los ocho años en los que las fuerzas armadas ucranianas habían recibido asistencia militar de Estados Unidos y Gran Bretaña no se le había proporcionado al país ningún sistema de armas pesadas, pero si se habían mejorado considerablemente sus procedimientos administrativos, de gestión de la información, producción de inteligencia, reconocimiento y mando y control (Friedman, 2019). La mejora en la gestión produjo también un cierto cambio de mentalidad que se mostraría decisivo en el enfrentamiento contra el ejército ruso. En la incertidumbre y la confusión de los primeros días de la invasión, los mandos intermedios ucranianos utilizaron su iniciativa para atacar los puntos vulnerables del despliegue ruso, incluso en pequeños grupos de combatientes.

También se mostraron muy competentes en el uso de modernas tecnologías con un impacto considerable en el campo de batalla, como los drones (en muchos casos modelos comerciales adaptados a usos militares) o la ciberdefensa. Además, los apoyos recibidos de algunas compañías privadas en el campo de la información y la conectividad tuvieron también un papel muy destacado en el éxito ucraniano. Cabe destacar la conexión a internet mediante los satélites *Starlink* o las imágenes de satélite proporcionadas por la compañía *Maxar* (Feldscher, 2022).

Por el contrario, las fuerzas armadas rusas mostraron carencias considerables. Su sistema de mando y control sufrió aparentemente fallos tan graves que obligaron a utilizar redes de comunicaciones no protegidas, lo cual tuvo como consecuencia la localización y destrucción de múltiples puestos de mando y la muerte de varios generales (Beaumont & Borger, 2022). El efecto sobre las operaciones fue devastador, con dificultades evidentes para coordinar la

[1] Por ejemplo, las fuerzas armadas rusas se consideraban líderes en el uso integrado de la artillería con drones de observación y guerra electrónica, dentro del concepto RUK (Complejo de fuego y reconocimiento) (Grau & Bartles, 2018). Sin embargo, poco de esto se ha visto en el campo de batalla.

actuación de las numerosas unidades rusas en una compleja maniobra que se desarrollaba a través de no menos de once ejes de penetración.

La presunta excelencia rusa en el uso de su artillería no se puso en evidencia hasta la segunda fase de las operaciones en Ucrania, ya a mediados de abril, y solo en algunos sectores del frente en lo que fue posible conseguir una concentración suficiente de estos medios. Además, al contrario que en el bando ucraniano, la iniciativa y la capacidad de liderazgo de los mandos intermedios se mostró muy pobre.

Por otro lado, quedó también en evidencia que el esfuerzo en un conflicto armado, especialmente en uno de intensidad media, excede con mucho el ámbito puramente militar y necesita de un grado considerable de movilización ciudadana y de uso de todos los instrumentos del Estado. En Ucrania, junto a la actuación de sus fuerzas militares resultó esencial el buen funcionamiento de su red de ferrocarriles, tanto para apoyar la logística militar como para atender al enorme flujo inicial de refugiados. Las fuerzas de seguridad y los servicios de inteligencia tuvieron también un papel destacado neutralizando grupos de saboteadores en los primeros días del conflicto. La defensa civil consiguió reducir las consecuencias de los daños producidos por los bombardeos rusos y el gobierno activó un auténtico ejército de “hackers” centrados tanto en la ciberdefensa de las redes del Estado como en el ataque contra intereses rusos en la red (Shore, 2022). Asimismo, muchos voluntarios jugaron un papel destacado, tanto en el apoyo a la evacuación de personas vulnerables como en la gestión de refugiados o incluso en el campo de batalla, como la improvisada unidad de expertos en drones que contribuyó a frenar el avance ruso sobre Kiev (Shoaib, 2022). La seguridad y la defensa son actividades en las que el Estado debe actuar de forma integral, gestionando y coordinando todos los recursos disponibles, e incluso generando recursos nuevos. Para ello, como se ha señalado anteriormente, la existencia de un sistema de mando, control y comunicaciones seguro, fiable y flexible resulta esencial.

En definitiva, las lecciones aprendidas de la guerra en Ucrania se orientan por un lado hacia la necesidad de reforzar los elementos centrales de todo sistema de defensa, en especial el sistema nervioso constituido por los sistemas de mando y control, comunicaciones e inteligencia, integrados en redes digitales y gestionados con una mentalidad proactiva y abierta. Por otro lado, se apunta también a la necesidad de consolidar sistemas de seguridad integrales que

permitan combinar las capacidades puramente militares con el resto de los instrumentos del Estado con aplicaciones en seguridad, desde las fuerzas de policía hasta el sistema de protección civil, pasando por las redes de comunicaciones, la ciberseguridad o el sistema sanitario. Integración e interconexión, impulsadas por las posibilidades de las nuevas tecnologías, son los conceptos clave en cuanto a capacidades de seguridad y defensa en el siglo XXI.

¿Qué necesitará la OTAN en 2050?

Para conseguir una disuasión creíble y un balance de fuerzas sostenible y eficiente siempre hay que combinar de alguna manera cuatro factores esenciales: número, organización, tecnología y motivación. Es muy difícil disponer siempre de una proporción adecuada de cada uno de estos factores, por lo que normalmente hay que compensar las carencias en algunos con la excelencia en otros. Entre los miembros de la OTAN resulta evidente que hay más posibilidades de contar con una buena organización y una tecnología puntera que con fuerzas numerosas o una motivación excepcional.

La consecuencia es que hay que reforzar lo que ofrece mayores posibilidades de éxito, pero sin olvidar lo que resulta más débil ya que existen umbrales que, una vez traspasados en sentido descendente, pueden provocar el colapso de todo el sistema. Por ejemplo, una motivación claramente insuficiente puede anular totalmente los efectos de la excelencia tecnológica, llevando a una sociedad a darse por vencida antes de que su superioridad en tecnología tenga ocasión de manifestarse en el campo de batalla.

En cualquier caso, el esfuerzo de la Alianza para mejorar su organización y desarrollar su nivel tecnológico debería orientarse a reforzar los dos factores claves que se han mencionado anteriormente: la interconexión y la integración.

En cuanto a la interconexión, hay dos nichos tecnológicos que probablemente se convertirán en decisivos durante el siglo XXI. El primero de ellos es el desarrollo de la inteligencia artificial que, combinada con el 5G y 6G, permitirán una autonomía cada vez mayor de vehículos y sistemas militares robotizados, mejorarán la rapidez y precisión de los procesos de decisión en operaciones y revolucionarán actividades como la ciberdefensa, imprimiendo un ritmo a las

acciones en este dominio que resultaría imposible para operadores humanos. El segundo nicho tecnológico se centra en la computación cuántica que, como primera consecuencia, modificará dramáticamente la seguridad de las comunicaciones militares, ofreciendo a quien domine primero esta tecnología la posibilidad de disfrutar de códigos cifrados impenetrables y, a la vez, la capacidad para romper los códigos enemigos. Como segunda consecuencia, la computación cuántica contribuirá de manera decisiva al desarrollo de una inteligencia artificial más capaz y con mayor grado de autonomía.

La interconexión debe facilitar el desarrollo de un modelo que amplíe las posibilidades de la tradicional Batalla Aeroterrestre a un escenario en el que debe actuarse simultáneamente en múltiples dominios y utilizando un número cada vez mayor de plataformas no tripuladas. De nuevo hay que recordar que no se trata solo de la tecnología sino de la mentalidad a la hora de utilizarla. La excelencia tecnológica sirve de poco sin el adecuado componente de capacidad de decisión, imaginación e iniciativa en los operadores de los sistemas.

También hay que recordar que las consecuencias de una revolución tecnológica no se hacen del todo patentes hasta que el avance en tecnología no se traduce en productos sencillos, sostenibles y fáciles de utilizar. Aunque en algunos casos las plataformas de combate complejas y caras seguirán siendo necesarias, el futuro está probablemente en productos más sencillos, accesibles y baratos. Los enjambres de pequeños drones, por ejemplo, pueden tener un futuro más prometedor que complejos sistemas tripulados.

En cuanto a la integración, la OTAN debe ser capaz de dar el salto desde la mera defensa hacia la seguridad. Este es un paso complicado porque implicaría que la organización se dotase de capacidades civiles de las que ahora mismo no dispone o no tiene capacidad para gestionar, aunque sus Estados miembros sí que dispongan de ellas. La solución más realista no es probablemente convertir a la OTAN en una organización más compleja de lo que ya es, sino mejorar su capacidad para interactuar con actores que sí dispongan de este tipo de capacidades civiles, bien aliados y socios, o bien organizaciones supranacionales como la Unión Europea. De hecho, la cooperación entre la OTAN y la Unión Europea, que posee capacidades diplomáticas, legislativas (firma de tratados, promulgación de leyes) y financieras de las que la Alianza carece, se presenta como una de las posibilidades más prometedoras para la futura seguridad europea. La necesidad de integración en seguridad y defensa no se limita solamente a las estructuras

internas de cada Estado, sino que se amplía a la colaboración multinacional o entre organizaciones internacionales.

Aunque la excelencia tecnológica y una reforma organizativa que permita aprovechar al máximo sus posibilidades son las áreas de desarrollo más prometedoras para la Alianza, conviene mantener un nivel al menos aceptable en otros factores más débiles. Quizás el más sensible es la motivación. Los miembros de la Alianza son países desarrollados con unos estándares de vida más que aceptables y unas sociedades poco proclives a afrontar los sacrificios propios de un conflicto armado. Esto tiene una influencia importante en la eficacia de la disuasión. De poco sirve disponer de fuerzas militares poderosas si la sociedad que las sostiene no dispone de un mínimo grado de resiliencia.

En los países de la OTAN esta resiliencia social es variable, pero en ningún caso es excepcional. Una de las tareas fundamentales de la Alianza es reforzarla o, al menos, evitar que se deteriore todavía más. Una vía para lograrlo es mejorar la capacidad para afrontar estrategias precisamente diseñadas para romper la resiliencia de la sociedad. Cabe destacar entre ellas los ciberataques, las campañas de desinformación o los ataques terroristas, que tienen a la sociedad civil como objetivo.

Otro aspecto que debe tomarse en consideración es el número, referido a la cantidad de capacidades militares disponibles. La tecnología y la buena organización pueden compensar la limitación de fuerzas, pero solo hasta cierto punto. Hay niveles críticos por debajo de los cuales la capacidad operativa se desmorona. En la guerra de Ucrania se ha demostrado la importancia de las reservas, la movilización y la disponibilidad de stocks de abastecimientos y munición suficientes. El campo de batalla moderno es muy letal y consume cantidades extraordinarias de municiones, combustibles y equipos por lo que la cantidad sigue importando, especialmente en un conflicto que se prolongue más allá de unos días. Aunque pueda parecer un recuerdo de la estrategia militar del siglo XIX, la capacidad de movilización sigue contando bastante a la hora de ejercer una disuasión creíble y de lograr un balance de fuerzas equilibrado.

Conclusiones

Es muy probable que al final de la Guerra en Ucrania se asista a un renovado esfuerzo por construir una nueva arquitectura de seguridad en Europa. Ese esfuerzo incluirá una parte "blanda" centrada en la distensión, el desarme y las medidas de confianza y una parte "dura" enfocada a la disuasión. La mala experiencia del conflicto ucraniano, producto en parte de un fallo en la disuasión, llevará a prestar más atención hacia este aspecto de la seguridad.

La disuasión debe ser creíble pero no amenazante. Suficiente para evitar tentaciones de utilizar la fuerza militar, pero también contenida y limitada, para evitar la impresión de que se está preparando una agresión. Un balance de fuerzas equilibrado y razonable es una de las condiciones esenciales para mantener la paz en cualquier lugar del mundo que albergue varias potencias con intereses diversos.

Desde los años 70 del pasado siglo, la capacidad de disuasión de la Alianza se ha basado en la superioridad tecnológica, una organización militar más eficiente y unos procedimientos más modernos. En el siglo XXI parece lógico continuar en esta línea, aunque la experiencia de los últimos conflictos nos recuerda la necesidad de no olvidar otros aspectos de la seguridad, como la resiliencia de la sociedad o un volumen suficiente de fuerzas y suministros para alimentarlas.

Para mantener la excelencia tecnológica, la OTAN debe trabajar esencialmente en mejorar la interconexión de sus fuerzas, que tradicionalmente ha sido un factor decisivo en las operaciones militares y aún lo es más en la era digital. La adecuada aplicación de nuevas tecnologías como la inteligencia artificial, el 5G y 6G o la computación cuántica permitirán disminuir los tiempos de transmisión de datos, acelerar las decisiones, batir objetivos con mayor oportunidad y precisión, disminuir la vulnerabilidad de las redes propias y, finalmente, conseguir un efecto de desintegración de la coherencia del adversario, consecuencia de la actuación de múltiples sistemas en red, muchos de ellos no tripulados.

En el aspecto de la organización, el mayor reto de la Alianza es avanzar hacia un sistema de seguridad más integral, que amplíe los aspectos puramente militares que hasta ahora han sido la piedra angular de la organización. Es difícil que la OTAN evolucione hacia una organización más compleja, con capacidad y competencia para gestionar otros instrumentos de seguridad más propios de los Estados, pero puede adaptar sus estructuras y procedimientos para una

mejor interacción. La colaboración con la Unión Europea, un actor con múltiples instrumentos de seguridad que la OTAN no posee, aparece como una de las posibilidades más prometedoras tanto para la propia Alianza como para la futura arquitectura de seguridad europea.

No hay que olvidar, por último, que la eficacia de toda estructura de seguridad y defensa descansa en la competencia y la motivación de las personas que la gestionan. La excelencia tecnológica y organizativa, así como la integración de múltiples elementos de seguridad, requiere no solo equipos, procedimientos y técnicas novedosas, sino de una mentalidad nueva, capaz de extraer el máximo rendimiento de los nuevos sistemas. La OTAN se creó para proteger una cultura que prioriza la libertad personal, la iniciativa y la creatividad como cualidades esenciales de una sociedad. Esas fueron sus mejores armas en el duro periodo de la Guerra Fría y lo seguirán siendo en el incierto siglo XXI.

Referencias

Beaumont, Peter & Borger, Julian, (2022) "US intelligence helping Ukraine kill Russian generals, report says", *The Guardian*, 5 mayo de 2022, https://www.theguardian.com/world/2022/may/05/us-intelligence-helping-ukraine-kill-russian-generals-report

Colom. Guillem (2015), "Rumsfeld revisited: La tercera estrategia de compensación estadounidense", *Revista UNISCI / UNISCI Journal* , Nº 38 (Mayo / May 2015), https://www.ucm.es/data/cont/media/www/pag-72452/UNISCIDP38-3COLOM.pdf

Eaglen, Mackenzie & Ferrari, John, (2020), "Use Legacy Systems as Tech Playgrounds for Innovation", *Breaking Defense*, November 19, 2020, https://breakingdefense.com/2020/11/use-legacy-systems-as-tech-playgrounds-for-innovation/

Erwin, Sandra I., "Too Much Information, Not Enough Intelligence", *National Defense*, 05-01-2012, https://www.nationaldefensemagazine.org/articles/2012/5/1/2012may-too-much-information-not-enough-intelligence .

Feldscher, Jacqueline (2022) "The Ukraine War Is Giving Commercial Space an 'Internet Moment'", *Defense One*, 7 abril de 2022, https://www.defenseone.com/technology/2022/04/ukraine-war-giving-commercial-space-internet-moment/364101/

Fendorf, Kyle & Miller, Jessie, (2022), "Tracking Cyber Operations and Actors in the Russia-Ukraine War", *Council on Foreign Relations*, March, 24, 2022, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

Friedman, Uri, (2019), America Hasn't Always Supported Ukraine Like This, *The Atlantic*, November 21, 2019, https://www.theatlantic.com/politics/archive/2019/11/how-vital-us-military-aid-ukraine/602407/

Grau, Lester W. & Brtles Charles K. (2018), "The Russian Reconnaisance Fire Complex comes of age", *Oxford Changing Character of War Centre*, May 30, 2022, http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age

Hoffman, Frank G.(2009), "Hybrid Warfare and Challenges*", JFQ* / issue 52, 1st quarter 2009, https://smallwarsjournal.com/documents/jfqhoffman.pdf

Grayson, Timothy, (2018), "Mosaic Warfare and Multi-Domain Battle", Youtube video, DarpaTV, https://www.youtube.com/watch?v=33VAnIEjDgk

Lieberthal, Kenneth, G. (2011), "The American Pivot to Asia", *Brookings Institution*, December 21, 2011, https://www.brookings.edu/articles/the-american-pivot-to-asia/

Marcus, Jonathan (2022), "Combat drones: We are in a new era of warfare - here's why", *BBCNews*, 4 February 2022, https://www.bbc.com/news/world-60047328

Pedlow, Gregory W. (1997) "NATO Strategy Documents 1949-1969" Supreme Headquarters Allied Powers Europe, 1997, https://www.nato.int/docu/stratdoc/eng/intro.pdf

Romjue, John L. (1984), *From Active Defense to Air Land Battle: The Development of Army Doctrine 1973 – 1982*, United States Army Training & Doctrine Command, Fort Monroe, Virginia.

Shoaib, Alia (2022) "Inside the elite Ukrainian drone unit founded by volunteer IT experts: 'We are all soldiers now.", *Insider*, 9 abril de 2022, https://www.businessinsider.com/inside-the-elite-ukrainian-drone-unit-volunteer-it-experts-2022-4?r=US&IR=T

Shore, Jennifer (2022), "Don't Underestimate Ukraine's Volunteer Hackers*", Foreign Policy*, April 11, 2022, https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army