



Facultad de Ciencias Humanas y Sociales
Grado en Relaciones
Internacionales

Trabajo Fin de Grado

Naturaleza híbrida y tecnología
militar moderna: Un análisis
comparativo del uso de vehículos no
tripulados de combate aéreo y
acciones en el ciberespacio en la
guerra de Nagorno-Karabaj (2020) y
en la guerra de Rusia contra
Ucrania (2014-actualidad)

Estudiante: Martín Fernández Martínez

Director: Dra. Sonia Alda Mejías

Madrid, abril 2024

Resumen

En un mundo progresivamente digitalizado y tecnológicamente avanzado, la dinámica y la conducta de los actores en los conflictos bélicos está evolucionando, incorporando características de las guerras híbridas mediante la mezcla de tácticas militares tradicionales y no tradicionales. Este estudio se enfoca en la adopción de tecnologías emergentes, como los vehículos no tripulados de combate aéreo y las operaciones en el ciberespacio, con el objetivo general de identificar si la implementación de estas tecnologías fue similar en ambos conflictos, si estas tecnologías han reemplazado o complementado el armamento convencional y determinar si permiten alcanzar la victoria por las partes. A través de un análisis comparativo entre la guerra de Nagorno-Karabaj del 2020 y la guerra de Rusia contra Ucrania a partir del 2014, se busca dilucidar estas dinámicas y determinar su impacto. Estos conflictos no solo fueron seleccionados por su relevancia reciente sino también por la notable implementación de tecnologías avanzadas. Estos conflictos presentan un contraste intrigante: mientras que el uso de tales tecnologías fue percibido como un factor de éxito en Nagorno-Karabaj, la situación en Ucrania permanece estancada. En definitiva, este análisis pretende explorar si las maneras de implementar estas nuevas tecnologías fueron similares en ambos conflictos y hasta qué punto el empleo de estas herramientas asegura una ventaja decisiva que conduce a la victoria.

Palabras clave: Guerra híbrida, Nuevas Tecnologías, Drones, Ciberataques, Rusia, Ucrania, Nagorno-Karabaj

Tabla de contenidos:

I.	Introducción	1
A.	La relevancia de las innovaciones tecnológicas en el ámbito militar: Las Revoluciones de los Asuntos Militares (RAM)	1
B.	Relevancia de estas nuevas tecnologías en conflictos recientes: El caso de la guerra de Rusia contra Ucrania y la guerra de Nagorno-Karabaj	3
II.	Objetivos de estudio	6
III.	Estado de la cuestión	7
A.	La percepción de la evolución lineal de la implementación de tecnología: entre el estado embrionario y la madurez	7
B.	La revolución percibida por la implementación de drones	8
C.	Reevaluación y cuestionamiento de la eficacia de los VNTC	11
D.	La importancia del contexto para la eficacia militar	12
E.	La percepción de las acciones en el ciberespacio como limitadas	13
IV.	Marco teórico	15
A.	La relevancia del realismo	15
B.	Definición y evolución del concepto de guerra híbrida	17
1.	Surgimiento del término	17
2.	Críticas y debates sobre el concepto	18
V.	Metodología	19
VI.	Desarrollo y Discusión	22
A.	CAPÍTULO 1: Vehículos no tripulados de combate aéreo (VNTC)	22
1.	VNTC con capacidad ISR (Inteligencia, Vigilancia, Reconocimiento)	23
a)	<i>Diferencias de clases utilizadas</i>	23
b)	<i>Uso combinado de drones y coordinación con sistemas lanzacohetes múltiple</i>	26
c)	<i>Aplicación práctica del uso combinado de VNTC con sistemas MRLS</i>	28
2.	VNTC con capacidad ISR y realización de ataques directos	29
a)	<i>El éxito de los drones de categoría militar en la guerra de Nagorno-Karabaj</i>	29
b)	<i>Drones con capacidad de ataque directo en la guerra de Rusia contra Ucrania</i>	33
3.	Factores externos para determinar la contribución real a la victoria	36
a)	<i>Inversión militar y capacidades de respuesta</i>	36
b)	<i>Importancia de la logística</i>	40
c)	<i>Límites técnicos, tropas y equipamiento tradicional</i>	42
B.	CAPITULO 2: Acciones ofensivas en el ciberespacio	45
1.	Conceptualización y dimensiones clave	45
2.	Acciones llevadas a cabo en función de las dimensiones del ciberespacio	46
a)	<i>Acciones en las dimensiones ciber-físicas y ciber-lógicas</i>	46
b)	<i>Acciones en el ciber espacio en la dimensión ciber-cognitiva</i>	50
VII.	Conclusiones	55
VIII.	Anexos	57

A.	Anexo 1: Tabla comparativa de drones implementados en los conflictos, clasificados en función de su uso primordial.....	57
1.	Vehículos autónomos de combate aéreo con capacidades ISR	57
2.	Vehículos autónomos de combate aéreo con capacidades ISR y ataque.....	60
3.	Vehículos autónomos de combate aéreo con capacidad merodeadora y/o autodestructiva	63
IX.	Fuentes y referencias bibliográficas.....	64

Acrónimos:

ISR: Inteligencia, vigilancia, reconocimiento

RAM: Revolución de los asuntos militares

VNTC: Vehículos no tripulados de combate aéreo

I. Introducción

A. La relevancia de las innovaciones tecnológicas en el ámbito militar: Las Revoluciones de los Asuntos Militares (RAM)

En el contexto postmoderno actual, las guerras y su naturaleza están experimentando cambios profundos y significativos tanto a nivel táctico como al nivel operacional. Como explicó Hables Gray: "La guerra es un sistema de discurso, pero cada tipo de guerra tiene diferentes reglas de discurso. En la guerra posmoderna, el papel central de los humanos está siendo eclipsado por la creciente importancia de las máquinas" (Chin, 2019, p. 772). Este cambio podría evidenciar un alejamiento de las guerras en los términos de Clausewitz, es decir, grandes números de tropas luchando en frentes extendidos, hacia estrategias que pueden ser llevadas a cabo por un número más reducido de individuos, a menudo con la ayuda de tecnología sofisticada (Singer, 2002, p. 195).

Desde el inicio de la Guerra Fría, la creciente inversión en nuevas tecnologías por parte de los estados dio lugar a avances significativos como las comunicaciones inalámbricas o la vigilancia por satélite (Chin, 2019, p. 770). Sin embargo, con el final de la Guerra Fría se produjo una disminución en la inversión estatal en defensa, en la investigación y en el desarrollo tecnológico. Esto último dio lugar a un proceso de privatización que fomentó la aparición de compañías militares privadas y, de esta manera, se siguieron desarrollando importantes tecnologías que posteriormente fueron implementadas a nivel militar por parte de los estados (Singer, 2002, p. 186)

Hoy, la voluntad de mejorar tecnológicamente los arsenales militares se sigue poniendo de manifiesto en los diversos planes internacionales de desarrollo en el ámbito militar como la estrategia *Third Offset* de Estados Unidos diseñada para preservar la superioridad militar-tecnológica del país (Chin, 2019, p. 773) o, de la misma manera, a través de los distintos planes de modernización militar implementados por la República Popular de China (Chen y Feffer, 2009). En referencia al último estado mencionado, a pesar de la dificultad para caracterizar sus capacidades militares debido a la escasez de documentos públicos (Cordesman et al., 2019, p.477), varias fuentes, como el Índice Elcano de Presencia Global (2022), indican un aumento en dichas capacidades. Por

ejemplo, este índice señala un incremento en su puntuación en la dimensión de presencia militar, pasando de 245 puntos en 2021 a 365 puntos en 2022 (Olivié y Gracia, 2022).

No obstante, estos avances tecnológicos no se limitan únicamente a los últimos tiempos. En efecto, a lo largo de la historia se produjeron numerosas revoluciones de los asuntos militares (RAM) y, concretamente, en los años 70 comenzó la más reciente de ellas debido, principalmente, a la introducción de armas guiadas, drones de combate y otros sistemas de ataque que fueron cambiando significativamente la naturaleza operativa de las guerras (Kosal, 2019, p.8; Miller, 2022). Como lo destacan algunos expertos, el impacto de esta RAM pudo observarse por primera vez de manera notable en la Guerra del Golfo de 1991, en la que Estados Unidos puso de manifiesto sus capacidades tecnológicas en un nuevo concepto operativo de combate.

Tal y como lo reconoce Chin (2019, p.771), la Guerra del Golfo fue un marcador que reveló “el poder de la tecnología” en la guerra convencional. Aun así, no se ha alcanzado consenso a nivel doctrinal sobre cuántas RAM tuvieron lugar a lo largo de la historia, ni si conflictos concretos como la Guerra del Golfo fueron realmente eventos en los que se pudieron poner de manifiesto estos cambios tecnológicos de forma completa. Este desacuerdo doctrinal se evidencia, por ejemplo, en el análisis de Krepinevich (2008, p.17): "*Cavalry to Computer: The Pattern of Military Revolutions*", en el que destaca diez revoluciones tecnológicas que pudieron haber tenido lugar, desde el descubrimiento de la pólvora hasta la revolución nuclear, mientras que otros autores como Alvin y Heidi Toffler, únicamente consideraron la existencia de tres RAM.

A pesar de estas divergencias doctrinales, parece innegable que en las últimas décadas el desarrollo sin precedentes de nuevas tecnologías a nivel militar y, recientemente, los avances en inteligencia artificial (IA) y demás sistemas tecnológicos complejos, permitieron producir nuevas armas como los vehículos no tripulados de combate aéreo (VNTC) y llevar a cabo acciones ofensivas en el ciberespacio cada vez más sofisticadas capaces de alterar el funcionamiento o destruir infraestructuras críticas durante conflictos armados. Los VNTC mencionados anteriormente, son máquinas autónomas o controladas de manera remota por personal militar o civil (Kosal, 2019, p.25) que permiten una presencia en el campo de batalla para llevar a cabo maniobras militares sin la necesidad de presencia física humana. Su relevancia ha sido muy alta

sobre todo en conflictos recientes, como la guerra de Rusia contra Ucrania o la guerra de Nagorno-Karabaj, pero al mismo tiempo generan dudas sobre si realmente su implementación generalizada en los arsenales militares permite alcanzar la victoria por las partes implicadas.

B. Relevancia de estas nuevas tecnologías en conflictos recientes: El caso de la guerra de Rusia contra Ucrania y la guerra de Nagorno-Karabaj

Si nos referimos de manera más concreta a las guerras de Rusia contra Ucrania desde el 2014 y la guerra de Nagorno-Karabaj del 2020, se puede observar que en ambos conflictos se produjeron importantes evoluciones en las estrategias militares y en los tipos de equipamiento utilizados por las partes implicadas. En el caso de Rusia, tal y como lo asegura Noorman (2023, p.1), ya desde hace varias décadas el país vio profundos cambios en sus “formas y métodos de guerra” así como en sus estructuras de fuerza y conceptos operativos. Muchos de estos cambios se dieron a partir de los años 90, sobre todo debido al aumento de la disponibilidad de armas avanzadas a nivel tecnológico, capaces de realizar ataques de alta precisión y a distancias cada vez mayores de manera más precisa. Debido al surgimiento de estos nuevos métodos de ataque utilizados por tropas extranjeras, Rusia tuvo dificultades para seguir implementando su estrategia de principios y mediados del siglo XX basada en la batalla profunda y en las operaciones profundas, en otras palabras, romper la línea de frente enemiga atacando de manera simultánea, llevando a cabo ataques aéreos y uso de artillería de largo alcance. Todo ello, seguido con un “segundo escalón mecanizado que explotara el avance inicial” (Noorman, 2023, p.1).

Como señaló el coronel general ruso Andrey Valeryevich Kartapolov, estos cambios en la estrategia de guerra llevaron a los soviéticos a cambiar de manera progresiva estos ataques masivos con grandes efectivos en plena Guerra Fría, por grupos de ataque tácticos más pequeños que no fuesen tan vulnerables a ataques enemigos dirigidos hacia grupos de soldados. Esta vulnerabilidad a ataques cada vez más precisos, también se debió a la proliferación de los VNTC que permiten el desarrollo de misiones de inteligencia, vigilancia y reconocimiento (ISR) para un subsecuente ataque o para realizar acciones ofensivas de manera directa. En este caso se estaría hablando de

capacidades para realizar ataques mediante un “sistema uniforme” que combinaría en algunos casos distintos elementos de reconocimiento y ataque (Gerasimov, 2019, p.132).

Ya en 1984, el Mariscal Nikolai Ogarkov, jefe del Estado Mayor soviético en ese momento, reconoció la importancia de las “máquinas voladoras no tripuladas” (Noorman, 2023, p.1) y años más tarde fueron ampliamente utilizados tanto en la guerra de Rusia contra Ucrania como en la guerra de Nagorno-Karabaj. Estas mejoras tecnológicas fueron impulsadas por una inversión de más de 640 mil millones de dólares entre 2003 y 2017, incluyeron avances en capacidades cibernéticas, electrónicas y de drones, según Fox (2017, p.3). Este autor también enfatiza cómo, desde 2014, las operaciones en el Dombás demostraron la relevancia de las nuevas tecnologías y tácticas ofensivas en el ciberespacio para la guerra moderna (Fox, 2017, p. 26).

La segunda guerra de Nagorno-Karabaj fue considerada también como un punto de inflexión (Popescu, 2021, p.37). Esto fue debido sobre todo al uso, por parte de Azerbaiyán, de drones de categoría militar altamente sofisticados, como puede ser el turco Bayraktar TB-2 o los drones de merodeo, también denominados de manera común: “drones suicidas” o “drones kamikaze”. En resumen, los drones y las operaciones ofensivas en el ciberespacio se emplearon ampliamente en ambos conflictos debido a diversos factores, incluyendo:

- 1) Su versatilidad, que los hace útiles para una amplia gama de aplicaciones como misiones ISR, ataques directos o ataques electrónicos.
- 2) Su alcance y autonomía, ideales para misiones que requieren largas horas de vigilancia continua.
- 3) El menor riesgo para los pilotos al no estar presentes dentro de la nave.
- 4) La percepción de que pueden implicar una estrategia menos propensa a ser interpretada como una escalada en el conflicto (Jones, 2022, p.7).

Según Jones (2022, p.9) la intensidad del uso de VNTC durante conflictos bélicos se ha multiplicado por siete y se ha observado un aumento de aproximadamente 23 veces del número horas de vuelo anuales.

No obstante, aquí se plantea una cuestión altamente interesante, las capacidades

tecnológico-militares modernas como los drones y acciones en el ciberespacio fueron ampliamente utilizadas por todas las partes, pero, sin embargo, ambos conflictos se desarrollaron de manera diferente y tuvieron resultados notablemente diferenciados. Por una parte, la segunda guerra de Nagorno-Karabaj culminó en menos de 2 meses (seis semanas) desde el inicio de las hostilidades (Modebadze, 2021, p. 104) y acabó con una victoria abrumadora, por parte de las tropas azeríes, mientras que la guerra de Rusia contra Ucrania cumple, a fecha de redacción de este trabajo de fin de grado, aproximadamente dos años desde la invasión rusa a Ucrania, de febrero de 2022 o 10 años si se habla del conflicto desde las protestas del Euromaidan de 2013-2014 (Diuk, 2014, p.10), todo ello, sin una clara victoria por las partes y convirtiéndose así en un conflicto enrocado en el tiempo.

Estos nuevos sistemas fueron, por tanto, utilizados de manera bastante generalizada en ambos conflictos, pero parece que su implementación dio lugar a resultados distintos, desafiando la tesis de que los avances tecnológicos en el ámbito militar deberían otorgar ventajas innegables a quienes los adoptan. Estas diferencias percibidas hacen relevante realizar una comparativa para intentar determinar cómo fueron implementados, cuál fue el papel jugado por estas nuevas tecnologías y si realmente contribuyeron de forma significativa para alcanzar la victoria por las partes.

El presente trabajo plantea la hipótesis general de que el uso de VNTC y acciones en el ciberespacio no fue similar en ambos conflictos, y que sus resultados divergieron debido a la forma en que fueron implementados y a la influencia de factores externos, lo que no garantizó siempre el éxito y no sustituyó completamente al equipamiento militar convencional.

De la misma manera, se proponen tres hipótesis específicas que serán evaluadas a lo largo del desarrollo:

- 1) Los drones utilizados en ambos conflictos no fueron similares en cuanto a características y modos de implementación, pero sí crearon cambios en la estrategia de la guerra.
- 2) La eficacia de los VNTC para alcanzar la victoria en conflictos depende del contexto (factores externos) y, si bien cambian la guerra, no eliminan el combate

directo ni el armamento tradicional, ni aseguran la victoria.

- 3) Las acciones en el ciberespacio simplemente complementaron la guerra y tuvieron un alcance limitado en ambos conflictos.

II. Objetivos de estudio

El presente trabajo tiene como objetivo general de investigación, identificar las similitudes y diferencias de la implementación de drones y operaciones en el ciberespacio en la guerra de Rusia contra Ucrania desde el 2014 y en la segunda guerra de Nagorno-Karabaj (Artsaj), evaluando si contribuyeron a alcanzar la victoria, y si complementaron o reemplazaron el equipamiento militar tradicional. Todo ello, naturalmente investigando la naturaleza híbrida de estos conflictos. Como se ha comentado, se parte de la hipótesis de que, el recurso a tecnologías modernas como los VNTC o las acciones en el ciberespacio no fue completamente similar en ambos conflictos, y que los resultados divergieron debido a la forma en la que fueron implementados y a la influencia de factores externos, lo que no garantizó siempre el éxito y no sustituyó completamente el equipamiento militar convencional. Para realizar una investigación rigurosa y ordenada del objetivo general, se propone una estructura en dos capítulos cada uno contando con un objetivo específico. Aquí se enumeran los objetivos generales del estudio y los objetivos específicos:

Objetivo general: Identificar similitudes y diferencias de la implementación de VNTC y operaciones en el ciberespacio en la guerra de Rusia contra Ucrania y en la guerra de Nagorno Karabaj del 2020, evaluando si contribuyeron a alcanzar la victoria.

Objetivo específico 1: Identificar y comparar (1) el uso de VNTC en las guerras de Nagorno-Karabaj (2020) y Rusia contra Ucrania (desde 2014), (2) centrándose en su contribución a la victoria y su papel en alcanzar la supremacía táctica.

Objetivo específico 2: Identificar y comparar (1) las acciones en el ciberespacio que fueron utilizadas en la guerra de Nagorno Karabaj del 2020 y en la Guerra de Rusia contra Ucrania desde el 2014, (2) evaluando si realmente contribuyeron a alcanzar la victoria por las partes.

III. Estado de la cuestión

A. La percepción de la evolución lineal de la implementación de tecnología: entre el estado embrionario y la madurez

La incorporación de tecnologías avanzadas como los drones y las ciberoperaciones por los estados ha ido progresivamente revolucionando la concepción, ejecución y comprensión de la guerra en el siglo XXI. Todo ello generando también debates sobre su impacto global y su efectividad para asegurar victorias.

En primer lugar, parece interesante destacar que, según parte de la doctrina, la implementación de nuevas tecnologías en los arsenales militares parece entenderse como una progresión lineal marcada por distintas etapas de desarrollo y maduración. Por ejemplo, cuando Katsuya (2021, p.42) se refiere a las etapas de desarrollo de las RAM, distingue tres fases sucesivas:

- 1) La fase embrionaria.
- 2) La fase inmadura.
- 3) La fase madura.

En realidad, complementando esta clasificación propuesta, Kosal (2019, p.17) y Krepinevich (1994) sostienen que una RAM no basta con la simple implementación técnica de una determinada innovación tecnológica, y su simple funcionamiento adecuado en el campo de batalla, sino que requiere de cuatro cambios más profundos más allá de la implementación, concretamente: (1) la innovación tecnológica en sí misma, (2) sistemas de desarrollo e implementación avanzados, (3) innovación en el ámbito operacional y (4) adaptación organizativa y de planificación.

Teniendo en cuenta las visiones propuestas por estos dos autores, se podría interpretar que, a medida que la tecnología evoluciona y alcanza niveles de madurez más avanzados, los conflictos contemporáneos tenderían a replicar el uso de tecnologías implementadas en enfrentamientos previos de manera unívoca, o bien, a incorporar variaciones de estos hasta alcanzar un nivel completo de madurez. Sin embargo, la aplicación práctica de estas tecnologías no sigue una trayectoria lineal en todos los casos. Al menos en los dos conflictos estudiados, parece evidente que ni la "adaptación

organizativa y de planificación" para incorporar estas tecnologías, ni la integración de "sistemas de implementación avanzados" han sido criterios completamente cumplidos. En realidad, las fuentes consultadas parecen mostrar que los estados recurren a distintos métodos de implementación dependiendo de los conflictos específicos y de una serie de factores adicionales. Todo ello parece indicar que las nuevas tecnologías, a pesar de suponer cambios, no siguen una implementación con una tendencia clara ni parece que se haya alcanzado el punto más álgido de la RAM comenzada a mediados de los años 70.

En efecto, las diferencias observadas dan lugar a discrepancias en la doctrina, argumentando por una parte que, efectivamente la tecnología juega un papel crucial en la modernización de las fuerzas armadas, en la transformación de las estrategias de combate y en alcanzar la victoria, mientras que otros argumentos parecen matizar esta afirmación argumentando que la efectividad no puede ser entendida ni evaluada en completo aislamiento de otros factores, ni estas tecnologías presentan un cambio radical en los resultados bélicos.

B. La revolución percibida por la implementación de drones

En primer lugar, al observar la segunda guerra de Nagorno-Karabaj y la guerra de Rusia contra Ucrania desde el 2014, una parte de la doctrina parece afirmar que la incorporación de tecnologías avanzadas, como los VNTC, ha marcado un punto de inflexión en la manera en la que los estados conciben y ejecutan la guerra en el siglo XXI. Por ejemplo, tal y como afirma Popescu (2021, p.40) refiriéndose a la guerra de Azerbaiyán contra Armenia: fue el "primer conflicto posmoderno en el que los drones abrumaron una fuerza terrestre convencional", es decir, dando a entender que no solo complementaron, sino que dominaron las operaciones militares llevadas a cabo por Azerbaiyán. Además, Chirac (2023, p.28) señala como la incorporación de drones ha redefinido los campos de batalla tradicionales, alejándolos de las dinámicas de las confrontaciones terrestres masivas que implican acciones cinéticas contra armamento convencional o combate cuerpo a cuerpo, y dejando de esta manera paso a una guerra moderna, caracterizada por la precisión, la movilidad y la eficiencia de costos.

En esta línea de razonamiento, Popescu (2021) de nuevo afirma que en dicha guerra se produjo un acercamiento a la "guerra de quinta generación" caracterizada por

un uso híbrido de tácticas convencionales y no convencionales, que incorporaría además otros elementos frecuentemente relacionados con las nuevas tecnologías como: los ciberataques, la inteligencia artificial, sistemas de ataque completamente autónomos, o la desinformación (p.37). Pero además de este cambio considerable en la forma de realizar la guerra, el percibido éxito bélico impulsado por el uso intensivo de drones de categoría militar ha reconfigurado, según Ilić & Tomašević (2021, p.15), las percepciones internacionales sobre la viabilidad y efectividad del uso de estas nuevas tecnologías, incluso para actores estatales con recursos limitados. Efectivamente, este cambio motivó a una diversidad de países incluidos, Ucrania, Estonia, Bielorrusia, o Kazajistán, entre muchos otros a integrar drones de ataque en sus arsenales militares con el objetivo de replicar las ventajas tácticas conseguidas por Azerbaiyán. En el caso de Ucrania, por ejemplo, el país realizó en una ocasión la compra a Turquía (Setien, 2020) de seis drones de categoría militar Bayraktar TB-2 por 69 millones de dólares.

Como lo destacan algunos expertos, estos países también desarrollaron progresivamente sus capacidades de producción de este tipo de aparatos, tanto de categoría militar como de categorías inferiores, invirtiendo en la creación de industria propia para su producción nacional, lo que mostraría el interés en este tipo de equipamiento. En el contexto ucraniano, por ejemplo, cuando el país obtuvo la independencia de la Unión Soviética, heredó una infraestructura notablemente anticuada que representaba aproximadamente el 30 % de la industria militar soviética (Lowther & Siddiki, 2022, p. 4-5). No fue hasta la anexión de Crimea por Rusia en el 2014 que aceleró su modernización militar permitiéndole obtener *software* y *hardware* moderno en materia militar, entre lo que se incluyeron tecnologías como VNTC.

Es importante recalcar que, tras la invasión rusa de Ucrania, el país no disponía de un tejido industrial lo suficientemente desarrollado para permitir la producción nacional de VNTC pero, al cabo de los meses, este tejido industrial se fue desarrollando hasta alcanzar un nivel de producción considerable. La doctrina también argumenta que el desarrollo de centros de producción y formación de pilotos de drones en Ucrania, como reporta Dronarium (2024), subraya la creciente importancia de estas tecnologías no solo en términos operativos sino también en la construcción de una base industrial y tecnológica autónoma. Según esta última fuente, desde el principio de la invasión rusa de Ucrania, ya se han formado en el país más de 4500 pilotos de drones para utilizarlos tanto

en el campo de batalla como en otros escenarios. De esta manera, como afirma Kowrach (2018, p.35), la guerra de Rusia contra Ucrania se convirtió en la primera guerra a nivel mundial en la que, ambas partes enfrentadas, recurrieron a VNTC de manera generalizada, para llevar a cabo sus operaciones. Reutilizando la expresión de DeVore (2023), esta podría ser considerada la primera: “guerra simétrica de drones”.

La doctrina también ha ido destacando de manera consistente el apoyo a la adquisición de estas nuevas tecnologías, por parte de distintos líderes a nivel mundial, lo que evidenciaría que son consideradas como activos relevantes. Por ejemplo, volviendo al caso de la guerra de Armenia contra Azerbaiyán, muchos expertos destacan como el presidente azerí apoyó en numerosas ocasiones la adquisición de VNTC turcos Bayraktar TB-2, al igual que sucedió en Ucrania, alabando continuamente su papel transformador en conflictos anteriores, como durante la guerra de Siria (Chiriac, 2023, p.32).

Es cierto que muchos expertos recuerdan constantemente algunas debilidades que se pueden atribuir a los drones de guerra, como:

- 1) La poca capacidad para operar en condiciones climáticas adversas.
- 2) Su menor capacidad para operar con grandes cargas de munición.
- 3) La lentitud con la que son capaces de volar.
- 4) El ruido que emiten (Ilić & Tomašević, 2021, p.15).

Pero, a pesar de ello, una gran parte de la doctrina sigue destacando las grandes ventajas que ofrecen durante las guerras y los logros que pueden conseguir a nivel táctico y operacional. En este sentido, autores como Oprean (2023, p.10) o Ivanchenko et al. (2023, p.23), señalan la incorporación de drones de combate como una parte indispensable de las operaciones militares ucranianas, destacando también su valor en la desmoralización del adversario y en la consecución de objetivos militares a gran escala. Todas ellas, características que también destaca la doctrina en la guerra de Nagorno-Karabaj del 2020.

Sin embargo, a pesar de estas visiones sobre la eficacia transformadora de los drones en los conflictos armados contemporáneos, existen matices considerables en la percepción sobre su impacto definitivo en la consecución de la victoria. En efecto, un

análisis de la doctrina también revela que la adopción y eficacia de estas tecnologías no están exentas de limitaciones, desafíos significativos y variaciones según el contexto de cada conflicto en particular. Como ilustra Chiriac (2023, p. 38) en el caso de la guerra en Ucrania, Rusia no mostró inicialmente gran interés en desarrollar su capacidad de producción de drones militares, lo que sugiere que, efectivamente, la implementación de estas tecnologías puede ser más compleja en la práctica. Según este autor, al comienzo de la invasión rusa del 2022 “Rusia no aprendió nada de los errores de Armenia” mostrando una reticencia a recurrir al uso de vehículos aéreos autónomos para imponerse a su oponente. Este apunte introduce una perspectiva crítica esencial para la siguiente sección de la revisión literaria, donde se exploran las voces dentro de la doctrina que cuestionan la narrativa de una revolución en la guerra impulsada por la implementación de estas tecnologías.

C. Reevaluación y cuestionamiento de la eficacia de los VNTC

Como se ha comentado, una revisión más detenida de la doctrina revela una postura más cautelosa hacia el impacto del uso de VNTC en la consecución de la victoria, manteniendo un tono mucho menos elogiador de estos sistemas sobre todo en momentos o en conflictos determinados. En este sentido, DeVore (2023, p. 264) destaca que, aunque los drones de categoría militar como los Bayraktar, Forpost u Orion fueron inicialmente considerados como armas transformadoras, su ciclo de vida en el frente demostró una vulnerabilidad aguda que llevó a su retiro del servicio activo.

En efecto, a pesar de su costo mucho inferior, en comparación con las aeronaves tripuladas utilizadas convencionalmente, estos dispositivos son altamente susceptibles a sufrir daños considerables cuando son alcanzados por contramedidas eficaces contra sus componentes y estructura, como pueden ser las piezas mecánicas o los circuitos electrónicos, que son vulnerables, entre otros, a ataques electrónicos direccionados o a sistemas antiaéreos convencionales. Por ello esta parte de la doctrina sostiene que la efectividad atribuida a los VNTC se enfrenta a un desafío fundamental: su capacidad para alterar decisivamente los resultados de los conflictos puede verse limitada por la facilidad con la que pueden ser neutralizados. Este análisis sugiere que la revolución de los drones en la guerra, aunque significativa, no es omnipotente ni definitiva.

De la misma manera, es importante mencionar que algunos expertos afirman que ninguno de los dos conflictos estudiados supuso una transición completa hacia la guerra “futurista”, dominada por sistemas hiperconectados y autónomos, sino que se observó la persistencia de enfrentamientos convencionales. Efectivamente, tanto la guerra de Nagorno-Karabaj del 2020 como la guerra entre Rusia y Ucrania desde 2014 se han caracterizado por la importancia crítica de las operaciones convencionales. Por ejemplo, Kartomo et al. (2022, p. 111) y Fabbrini (2023, p. 2) coinciden en describir el conflicto en Ucrania como una guerra convencional, donde el poder aéreo y los misiles de alta precisión desempeñan roles clave, pero el despliegue de grandes números de tanques y la persistencia de las fuerzas de combate convencionales subrayan la continuidad de las tácticas tradicionales en la guerra.

D. La importancia del contexto para la eficacia militar

Más allá de esta visión negativa de la eficacia de los drones en la guerra, una parte sustancial de la doctrina insiste en la necesidad de una perspectiva más matizada para comprender cómo se alcanza la victoria. En efecto, Chiriac (2023, p. 32) subraya que determinar como un Estado gana una guerra es un problema complejo que combina aspectos tangibles, como las fuerzas o las técnicas disponibles, con aquellos intangibles, como las decisiones estratégicas. Esta combinación de elementos hace que la respuesta no sea sencilla, y no se puedan hacer afirmaciones de manera taxativa, subrayando la importancia de considerar una amplia gama de factores más allá de la mera implementación tecnológica.

En esta misma línea de razonamiento, Ilić & Tomašević (2021, p. 15) argumentan que, a pesar de la eficacia percibida de los drones y los ataques cibernéticos, es esencial una combinación efectiva de estas nuevas tecnologías con sistemas más tradicionales, como las unidades mecanizadas blindadas y el combate cuerpo a cuerpo. Esta visión se apoya en la idea de que la guerra moderna debe ser entendida como una orquesta en la que todos los elementos deben funcionar conjuntamente para alcanzar objetivos significativos, y donde la implementación de la tecnología debe ser contextualizada cuidadosamente en función de cada caso particular.

La importancia de una perspectiva matizada es crucial para entender el impacto

de la tecnología en conflictos recientes. Esto se evidenció con la invasión rusa de Georgia en el 2008, un claro ejemplo de guerra híbrida (Seskuria, 2022). Aunque la “gran revolución” tecnológica en el campo de batalla fue innegable según parte de la doctrina, investigaciones sugieren que la cantidad de tropas también jugó un papel crucial (Beehner et al., 2018, p. 4). Por lo tanto, es esencial analizar con cuidado la contribución tecnológica frente a otros factores determinantes.

Esta sección subraya la idea de que, aunque las innovaciones tecnológicas como los drones y los ataques cibernéticos han redefinido aspectos de la guerra moderna, su efectividad y relevancia deben evaluarse en el contexto de una estrategia militar combinada que integre tanto elementos nuevos como tradicionales. La victoria en la guerra, por lo tanto, no se reduce a la superioridad tecnológica, sino que emerge de la capacidad de integrar y adaptar un espectro completo de capacidades militares en respuesta a las dinámicas particulares de cada campo de batalla.

E. La percepción de las acciones en el ciberespacio como limitadas

En lo que se refiere a las acciones ofensivas en el ciberespacio, la percepción sobre su contribución a la victoria es considerablemente más pesimista. Diversas voces dentro de la doctrina sugieren que, en conflictos como la guerra de Ucrania, los ataques cibernéticos han tenido poco o ningún impacto en el desarrollo de las hostilidades. Según Kostyuk y Zhukov (2017, p. 12), estos ataques no lograron alcanzar objetivos críticos de manera efectiva durante periodos prolongados. No obstante, aun así, Stone (2013) plantea que estas acciones pueden considerarse actos de guerra dada su fuerza, violencia y letalidad, lo que indica una visión generalmente pesimista, aunque matizada, sobre la importancia de estas acciones.

Realmente los ciberataques en sentido estricto, es decir acciones concretas en el ámbito ciber-lógico parecen haber sido limitadas y generalmente llevadas a cabo por grupos no identificados o no aliados de manera directa a las fuerzas armadas de las partes. Esto ya se pudo observar en conflictos bélicos como la guerra de Estonia del 2007, la primera en incorporar ataques cibernéticos de grandes magnitudes, como ataques de denegación de servicio (DDoS) que inhabilitaron importantes páginas gubernamentales y afectaron infraestructuras críticas (Herzog, 2011, p. 51) haciendo que sitios web que

normalmente recibían 1.000 visitas al día colapsaran después de recibir hasta 2.000 accesos por segundo (Herzog, 2011, p. 51). Dicho esto, parte de la doctrina sí reconoce la efectividad de este tipo de acciones para desestabilizar, además gracias a acciones con muy bajo coste mediante el uso de *bots* distribuidos globalmente.

Según la doctrina, estos ataques no siempre son atribuibles directamente, y no se han percibido históricamente como medios eficaces para alcanzar la victoria de manera independiente, pero su combinación con tácticas terrestres u otros sistemas de ataque puede servir para desestabilizar y aumentar las probabilidades de lograr victorias significativas en el terreno. Russell (2014, p. 103) observa que, en conflictos anteriores, los ciberataques a menudo coincidieron estratégicamente con los días de mayor ofensiva, sugiriendo una planificación anticipada. Esto indica que, aunque la doctrina no descarta completamente la ineficacia de las acciones cibernéticas, se reconocen patrones similares en distintos conflictos a escala global como en la guerra de Rusia contra Ucrania o de Nagorno-Karabaj. No obstante, la eficacia y contribución de estos ataques a la victoria a menudo queda condicionada a su integración con otros sistemas y capacidades militares.

Además, la doctrina coincide en que las acciones ofensivas en el ciberespacio frecuentemente trascienden las operaciones contra infraestructura o servidores gubernamentales, desarrollándose también a través de las redes sociales y configurándose casi como batallas de información. Willett (2022) destaca: “Los ataques cibernéticos durante la guerra entre Rusia y Ucrania han involucrado una masiva “batalla de información en línea”

Como se ha comentado a través de los últimos apartados, existe una división significativa dentro de la doctrina militar sobre el impacto de las innovaciones tecnológicas en la guerra moderna. Por un lado, una corriente de pensamiento sostiene que las mejoras tecnológicas, como la implementación de VNTC en los arsenales militares, ha marcado un cambio radical en cómo se libran los conflictos, presentando los avances como claramente determinantes y clave en los resultados bélicos. Por otro lado, hay otra perspectiva que sostiene que muchos aspectos de estos conflictos se han desarrollado de forma convencional, lo que, en cierto modo, ofrece una visión menos alentadora sobre la superioridad técnica ofrecida por estas nuevas tecnologías.

El presente trabajo fin de grado parece enfocarse más en la comprensión matizada del éxito de estas tecnologías en la guerra de Rusia contra Ucrania y en la guerra de Azerbaiyán contra Armenia del 2020, intentando considerar la implementación de estas tecnologías en sí mismas y contrastarla con factores externos como sus formas o momentos de implementación. La revisión de literatura parece apuntar a que el éxito de los drones en la segunda guerra de Nagorno-Karabaj puede no observarse de la misma manera en conflictos posteriores, como el de Rusia contra Ucrania, mostrando así situaciones en las que estos sistemas podrían no haber determinado de manera tan contundente el éxito bélico de las partes. Además, como se ha señalado, la expectativa de que la adopción de tácticas utilizadas con éxito en conflictos anteriores se replique linealmente en enfrentamientos subsecuentes a veces puede no cumplirse en su totalidad.

IV. Marco teórico

A. La relevancia del realismo

Antes de adentrarse en el concepto de la guerra híbrida, que es el concepto que parece recoger mejor las características de las guerras contemporáneas, especialmente si se toman en cuenta aspectos como la implementación de nuevas tecnologías en los arsenales militares, parece relevante enmarcar dicha teoría en un paraguas teórico mayor. Basándose en una visión puramente teórico-internacionalista, la teoría que podría ofrecer mejor ese contexto, podría ser la teoría realista de las relaciones internacionales. En efecto, esa parece ser la más adecuada para investigar, comprender y analizar el uso y la implementación de nuevas tecnologías en el contexto de una guerra a gran escala entre estados, y más concretamente, la teoría del realismo ofensivo. Esto se debe a que estas teorías se basan en cinco supuestos: (1) el contexto internacional anárquico; (2) la racionalidad de los estados; (3) la falta de claridad sobre las intenciones de los demás estados; (4) la supervivencia y la seguridad como objetivo principal para ellos y; (5) la posesión de considerables capacidades militares y la intención de seguir aumentándolas (Karagiannis, 2012, p.75). Este enfoque, basado en la relevancia del Estado como principal actor en las relaciones internacionales (Mammadov, 2022, p.6) y arraigado en la percepción de un sistema internacional anárquico, donde la seguridad es un bien escaso, proporciona una base sólida para analizar la evolución de la guerra en la era moderna.

Dentro de la teoría realista, el marco propuesto por los realistas ofensivos es especialmente pertinente ya que consideran que los estados buscan alcanzar sus objetivos políticos maximizando su poder relativo frente al resto de estados del sistema internacional basándose en su percepción de seguridad. Esta búsqueda muchas veces implica políticas exteriores expansionistas, aprovechando oportunidades para ganar más poder y debilitar a potenciales adversarios (Lobell, 2002, p.165-166). Tal y como lo asegura Karagiannis (2012, p.75), citando a Mear-Sheimer, los estados: “no dudarían en lanzar guerras contra adversarios cuando ello sirva a sus intereses”. Sin embargo, cabe matizar, que, a pesar de esta ser la visión clásica de las teorías realistas, Lobell (2002, p.165-166), sostiene que no siempre la hegemonía o la primacía internacional es el fin último que todo estado anhela alcanzar. En realidad, estos objetivos de expansión variarán de estado a estado, debido a factores como la geografía, sus tradiciones, etc. Es decir, que la estrategia de seguridad de cada Estado dependerá de sus situaciones concretas (Kunertova, 2023a).

Es importante decir que tanto la segunda guerra de Nagorno-Karabaj como la guerra de Rusia contra Ucrania se han estudiado en numerosas ocasiones desde la perspectiva realista o desde la del realismo ofensivo. Umarach y Muhammad (2023) argumentan, por ejemplo, que Azerbaiyán, en su disputa con Armenia, buscó asegurar su territorio incrementando su capacidad militar para tomar control del enclave de Nagorno-Karabaj, una región que históricamente consideró propia y todo ello esforzándose para aumentar su presupuesto y capacidades militares como lo describe Mammadov (2022, p.6). De la misma manera estudios como el de Kumar (2023, p.927), observan la guerra de Rusia contra Ucrania como una guerra que tendió hacia un modo de operaciones característico del realismo ofensivo.

Este marco conceptual realista es crucial no solo para entender la adquisición de nuevas tecnologías militares por parte de los estados, sino que también sirve como una base sólida para introducir y contextualizar el concepto de guerra híbrida. Este último, es fundamental para comprender las dinámicas de las guerras contemporáneas ya que encapsula la fusión de tácticas convencionales y no convencionales observadas en complejos conflictos como los que se plantean en este estudio.

B. Definición y evolución del concepto de guerra híbrida

1. Surgimiento del término

Tras la anexión de Crimea por Rusia en 2014 (Magen, 2014), el concepto de guerra híbrida adquirió relevancia en los círculos de la defensa transformándose en un término relevante en teoría militar y de uso relativamente común para describir diversos desafíos de seguridad y defensa. Reichborn-Kjennerud y Cullen (2016, p.2) destacan que la guerra híbrida pasó de la “oscuridad relativa de los círculos teóricos militares” a convertirse en un término más convencional utilizado para describir un conjunto extenso de desafíos de seguridad y defensa.

La guerra híbrida, según Danyk et al. (2017), no es un concepto particularmente nuevo, sino que simplemente se refiere a una “combinación de tácticas de guerra convencionales y no convencionales o irregulares”. Esta combinación se extiende más allá del campo de batalla para abarcar áreas como la economía, las relaciones diplomáticas o el campo de la información (incluyendo la guerra psicológica, la cibernética y hasta la desinformación), entre muchas otras (p. 5-6). En efecto, la guerra híbrida implica un enfoque asimétrico, cuyo objetivo es lograr efectos significativos a gran escala a través de recursos no convencionales en el ámbito militar, alejándose del recurso exclusivo a equipamiento armamentístico.

Por lo que destacan diversos autores, el propósito principal de estos conflictos y tácticas híbridas, es principalmente desestabilizar tanto los procesos internos como externos de un Estado en guerra. Entre muchas otras estrategias, algunas de estas acciones incluyen: la desestabilización económica, la promoción del descontento de la población o generar condiciones que propicien la emigración de algunas regiones. Pero además de esto, los esfuerzos suelen verse reforzados por la aplicación y el recurso a otras capacidades como labores de inteligencia, operaciones de fuerzas especiales, uso de fuerzas militares convencionales y la participación de combatientes irregulares (Danyk et al., 2017, p. 5-6), todo ello, naturalmente, sin olvidar el recurso a nuevas tecnologías, que consiguen alejar los conflictos actuales del concepto de una guerra convencional. En este trabajo de fin de grado, se investigará el papel de los VNTC y las acciones ofensivas en el ciberespacio dentro del marco de la guerra híbrida a través del análisis comparativo de las dos guerras mencionadas a lo largo de las secciones anteriores.

2. Críticas y debates sobre el concepto

Sin embargo, este concepto de guerra híbrida ha sido objeto de numerosas críticas en los últimos años. Algunos argumentan que se ha convertido en un término paraguas para cualquier tipo de intervención militar y que carece de un valor analítico por no contener nada “distintivamente nuevo” (Reichborn-Kjennerud y Cullen, 2016). Además, el concepto también se criticó por distorsionar supuestamente las distinciones tradicionales entre momentos de paz, de conflicto y de guerra; convirtiéndose según parte de la doctrina en un sinónimo de la “estrategia global” ya que podría adaptarse o moldearse a cualquier situación (Reichborn-Kjennerud y Cullen, 2016, p.2). De la misma manera se menciona que el término se ha ido adaptando según el análisis de distintas situaciones y contextos, lo que ha llevado a una falta de claridad conceptual. Esto en parte se debe a que el concepto se dedujo al “observar al enemigo”, lo que fue cambiando progresivamente su definición y significado según el “sujeto de análisis” (Reichborn-Kjennerud & Cullen, 2016, p.2).

A pesar de las críticas recibidas por la supuesta falta de rigor conceptual, el concepto de guerra híbrida ha proporcionado una base sólida para comprender la naturaleza de los conflictos actuales y específicamente los dos seleccionados para el presente estudio. Como señalan Reichborn-Kjennerud y Cullen (2016, p. 2): “La literatura sobre las guerras híbridas, y sus críticas, ofrecen terrenos fértiles para discutir el futuro de la guerra y la forma de combatir”. En efecto, esta perspectiva ayuda a alejarse de una visión de la guerra puramente instrumental y técnica reconociendo que el concepto de guerra está en constante cambio.

Inicialmente, la guerra híbrida se utilizó para describir la creciente sofisticación y complejidad de los conflictos en los que estaban involucrados actores estatales en el campo de batalla, como Hezbollah en el Líbano, entre otros. Estos actores combinaban tácticas convencionales, con otros modos de operación no militares y novedosos, como sistemas de armas modernos y tecnologías como ataques cibernéticos, VNTC, o comunicación cifrada, desafiando así el concepto tradicional occidental de la guerra convencional para alcanzar objetivos políticos o estratégicos (Reichborn-Kjennerud y Cullen, 2016, p.2-3). No obstante, el concepto evolucionó hacia la discusión de una forma de guerra, llevada a cabo también por estados, notablemente por Rusia contra Ucrania.

Como se ha mencionado anteriormente, esto implicaría “la integración total de los medios militares y no militares del poder estatal para conseguir alcanzar objetivos políticos” (Reichborn-Kjennerud y Cullen, 2016, p.3). Se entiende que los estados son capaces de coordinar y sincronizar sus capacidades para crear efectos sinérgicos que superan el éxito de los conflictos tradicionales.

La guerra híbrida, especialmente en su ejecución por estados, se caracteriza por un “nublamiento” de lo que se entiende por guerra (Ehrhart, 2017, p.4) y, en definitiva, se caracteriza por un uso estratégico de la ambigüedad con la que se pretende complicar o socavar los procesos de toma de decisiones del oponente y también dificultar la interpretación de lo sucedido en el campo de batalla (Reichborn-Kjennerud y Cullen, 2016, p.4). Como señala Chin (2019, p. 779), las tecnologías emergentes están desafiando el monopolio tradicional del estado sobre el uso de la violencia, introduciendo progresivamente nuevas oportunidades y métodos de ataque. Los avances en biotecnología, nanotecnología y la revolución de la información no solo están cambiando el campo de batalla, sino que también permiten tácticas que pueden ser consideradas “no militares”, ofreciendo así ventajas significativas en conflictos.

Un ejemplo destacado de estas tácticas no convencionales es Rusia, que ha sido acusada de emplear métodos no tradicionales como la manipulación de redes sociales y el *hackeo* de elecciones para influir más allá de sus fronteras. Estas tácticas, facilitadas por el desarrollo tecnológico, representan una característica persistente del espectro de conflictos y son empleadas por una variedad de estados, subrayando la evolución y la complejidad creciente de la guerra híbrida en el contexto moderno (Chin, 2019, p. 779).

V. Metodología

La metodología de esta investigación se fundamenta en un enfoque cualitativo y comparativo de la información recopilada mediante fuentes secundarias para explorar el impacto de la tecnología militar moderna y las estrategias de guerra híbrida en los conflictos de Nagorno-Karabaj y de Rusia contra Ucrania, evaluando específicamente si fueron implementaciones que contribuyeron a alcanzar la victoria.

En esta línea, la recopilación de datos se realizó a través de una cuidadosa selección de informes académicos, documentos políticos y análisis de expertos o think-tanks. Todo ello se complementó con fuentes de datos abiertas para corroborar y complementar los datos ofrecidos en los informes de combate. En lo relativo a este último punto, se recurrió por ejemplo a la base de datos Oryx, reconocida por su rigurosa documentación sobre equipamiento militar derribado en conflictos contemporáneos. De este recurso se extrajeron datos detallados sobre la cantidad y tipo de armamento destruido en ciertos puntos críticos de los conflictos analizados, buscando evaluar las posibles causas y orígenes de la destrucción de algunos equipos militares.

Este proceso implicó una meticulosa recopilación de fuentes abiertas a través de su plataforma web, seguido de una cuidadosa filtración y clasificación de los datos según categorías específicas, como tipo de armamento, y contexto del conflicto. Con estos datos clasificados, se procedió a elaborar estadísticas relevantes que permitieron una interpretación precisa de los patrones de daño y pérdida de material bélico, proporcionando así estadísticas empíricas para su posterior interpretación. A lo largo de la investigación se empleó un enfoque comparativo por temas para identificar las tendencias y divergencias en el uso de las nuevas tecnologías seleccionadas.

La selección de la bibliografía pertinente se realizó mediante la exploración de bases de datos académicas como Google Scholar y JSTOR, empleando palabras clave específicas como "Guerra Híbrida Nagorno-Karabaj", "Tecnología Armamentística Nagorno-Karabaj", "Drones en Guerra de Ucrania" o "Ciberoperaciones Guerra de Ucrania". Se procuró dar prioridad a las fuentes que poseen una conexión directa con los objetivos de la investigación, prestando especial atención a los materiales publicados en los últimos años. Este criterio temporal garantizó la contemporaneidad y aplicabilidad de la información recogida, aumentando así el rigor del estudio.

La investigación se llevó a cabo reconociendo las limitaciones impuestas por el acceso restringido a información confidencial, especialmente la militar, todo ello buscando la máxima objetividad al corroborar la información a través de diversas fuentes reconocidas por su integridad y fiabilidad.

Para el desarrollo del planteamiento de esta investigación, el TFG se desarrollará de la siguiente manera. En el primer capítulo, dedicado específicamente a los VNTC, se

pretende identificar y comparar qué drones fueron usados en ambas guerras, centrándose en su contribución a la victoria y en su papel en la supremacía táctica. Para facilitar el desarrollo, se clasificarán según su uso principal. Dicho objetivo está dividido en dos hipótesis específicas. En primer lugar, se plantea que los drones utilizados en ambos conflictos no fueron del todo similares en cuanto a características y modos implementación, pero sí crearon cambios en la estrategia tradicional de la guerra (anexo 1). En segundo lugar, su segunda hipótesis específica presupone que la eficacia de los drones para alcanzar la victoria en los conflictos depende del contexto (factores externos) y, si bien cambian la guerra, no eliminan el combate directo ni el armamento convencional, ni aseguran la victoria.

El segundo capítulo, está dedicado a las acciones ofensivas en el ciberespacio, el objetivo específico de dicho capítulo es identificar y comparar cuáles fueron utilizadas en ambas guerras, evaluando si realmente contribuyeron alcanzar la victoria de las partes. Se propone una hipótesis específica que sugiere que las acciones en el ciberespacio simplemente complementaron la guerra y tienen alcances limitados en ambos conflictos (anexo 1).

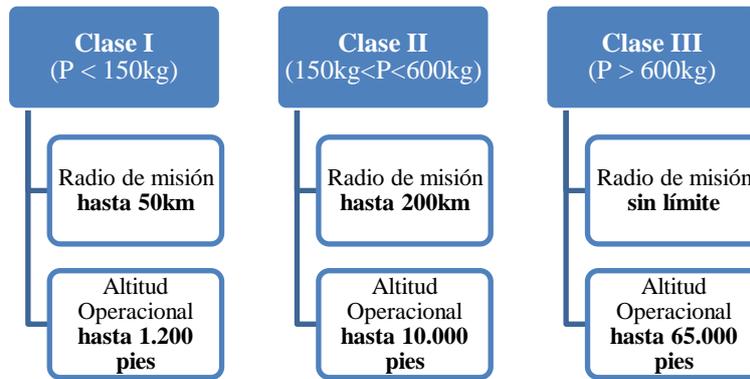
VI. Desarrollo y Discusión

A. CAPÍTULO 1: Vehículos no tripulados de combate aéreo (VNTC)

Como fue comentado, el primer capítulo del trabajo está dedicado específicamente a los VNTC. En él se pretende identificar y comparar específicamente cuáles de ellos fueron usados en ambas guerras, centrándose en su contribución a la victoria y en su papel en la supremacía táctica de las partes. En primer lugar, se plantea que los drones utilizados en ambos conflictos no fueron del todo similares en cuanto a características y modos implementación, pero sí crearon cambios en la estrategia tradicional de la guerra. Efectivamente, se presupone que, si bien los VNTC prevalecieron en misiones de reconocimiento y vigilancia, su impacto en operaciones ofensivas directas fue limitado. No obstante, se presupone también que transformaron significativamente la dinámica de los conflictos, permitiendo una mayor precisión y una clara identificación de objetivos, lo que a su vez impulsó cambios tácticos en las maniobras de tropas. En segundo lugar, la segunda hipótesis específica presupone que la eficacia de los VNTC para alcanzar la victoria en los conflictos depende del contexto (factores externos) y, si bien cambian la guerra, no eliminan el combate directo ni el armamento convencional, ni aseguran la victoria. Específicamente, se presupone que la eficacia de los drones dependió en gran medida de su integración con otras formas de capacidad de ataque y de factores externos, tales como la coordinación y planificación, así como las capacidades de respuesta enemigas. Además, a pesar de que proporcionaron una ventaja táctica en algunas situaciones, como en el caso de Azerbaiyán en Nagorno-Karabaj, estos VNTC complementaron, más que reemplazaron al equipamiento militar tradicional, mejorando la efectividad de ciertos ataques, sin garantizar por sí mismos la victoria.

Antes de dar comienzo a esta sección, parafraseando a Hassanalian y Abdelkefi (2017, p.100), parece importante precisar que cuando se habla de drones o de VNTC usados en conflictos bélicos las clasificaciones pueden ser muy numerosas debido a la gran cantidad de modelos existentes y a sus características variadas. Algunas de esas clasificaciones tienen en cuenta, por ejemplo, las características de las alas, de los motores o del peso del aparato. Pero a pesar de las innumerables clasificaciones, es necesario utilizar algún tipo de método de clasificación para poder realizar un análisis estructurado y comprensible. Para realizar las comparativas oportunas, a lo largo de análisis, se

recurrirá frecuentemente a la clasificación en tres categorías realizada por la OTAN: Clase I, hasta 150 kg; clase II, desde 150 kg hasta 600 kg; y, clase III, más de 600 kg (Onetto, 2021, p.90). Esta clasificación incluye algunos parámetros adicionales pero el criterio del peso prevalece ante las discrepancias que pueden darse entre otros criterios:



Elemento gráfico 1: Jerarquía de elaboración propia con datos de Pérez Arrieu y Allende (2021, p.30). P = Peso máximo de despegue

Este primer capítulo seguirá una estructura concreta para simplificar las comparativas y llevar a cabo un análisis más claro. Se estructurará según las funciones principales de los VNTC. Un primer apartado se referirá específicamente a (1) los VNTC únicamente con capacidad ISR (por sus siglas en inglés: inteligencia, vigilancia y reconocimiento), es decir, drones cuya única función es realizar operaciones no cinéticas y un segundo apartado se referirá a (2) los drones con capacidad ISR y capacidad de ataque propia.

1. VNTC con capacidad ISR (Inteligencia, Vigilancia, Reconocimiento)

a) Diferencias de clases utilizadas

Como se ha mencionado, la guerra de Ucrania fue la primera guerra en la que ambas partes enfrentadas utilizaron VNTC de manera considerable para llevar a cabo sus operaciones, sobre todo desde la crisis de Crimea (Kowrach, 2018, p.31), mientras que en la guerra de Azerbaiyán contra Armenia, a pesar de que fueron altamente importantes y utilizados, no se alcanzó el uso generalizado de manera simétrica por las partes.

Entre toda la amalgama de drones que fueron utilizados cabe destacar, en primer

lugar, el papel jugado por los drones que tienen únicamente capacidad ISR. Estos drones generalmente no tienen capacidad de ataque y se dedican exclusivamente a la recopilación de inteligencia y realizar acciones de vigilancia y de reconocimiento, a menos que sean modificados para otros propósitos. Como lo asegura Frąckiewicz (2023), estos dispositivos transformaron rápidamente la manera en la que se recopilan datos en la guerra, y ayudaron de manera considerable a alcanzar los objetivos de las partes en el campo de batalla. Esto se debe a que pueden ser utilizados entre muchas otras funciones, para recopilar inteligencia mediante imágenes o vídeo, detectar movimientos en el frente, realizar mediciones de señales u otras métricas a través de sensores específicos o actuar como centros de comunicaciones para operaciones integradas. Esto es más evidente en el caso de los drones diseñados específicamente para un uso militar, especialmente los de categorías más elevadas según la clasificación de la OTAN. Una de las funciones clave de estos aparatos es la habilidad para monitorear grandes áreas durante periodos de tiempo muy extensos, y así informar a las partes de la realidad del entorno para poder tomar decisiones razonadas y adaptadas al terreno (Frąckiewicz, 2023).

En numerosas fuentes consultadas, se puede observar que en ambos conflictos se recurrió de forma frecuente a los VNTC para realizar numerosos tipos de operaciones ISR. En el caso de la guerra de Rusia contra Ucrania, Karber (2015, p. 13) destaca que desde el principio de la guerra del Dombás, es decir, desde mediados del 2014, los separatistas rusos y Ucrania comenzaron a utilizar al menos 14 tipos de VNTC, muchos de ellos únicamente con capacidades ISR. A pesar de que no se mencionan los modelos implicados, se destaca por ejemplo el uso de “UAVs de vigilancia estratégica de muy largo alcance y gran altitud volando a lo largo de la frontera y la costa meridional ucraniana”, “aviones no tripulados de ala fija de largo alcance y gran altitud que sobrevuelan las posiciones ucranianas” o “cuadricópteros tácticos de muy corto alcance utilizados para explorar posiciones de defensa y evaluación de daños de batalla” (Karber, 2015, p. 13). Esto demuestra el uso dado a estos sistemas desde el comienzo de la guerra e introduce un aspecto relevante único para este conflicto: el uso de drones comerciales. Por otro lado, si se observan los informes que cubren la guerra de Nagorno-Karabaj se encuentran interesantes diferencias con el uso de estos dispositivos en comparación con la guerra de Rusia contra Ucrania.

Por una parte, en el conflicto de Nagorno-Karabaj, Azerbaiyán hizo un uso

intensivo de drones con capacidades ISR, que abarcaron varias clases militares definidas por la OTAN (anexo 1). Se desplegaron drones de Clase III como los Hermes 900, Heron y Searcher, además de los de Clase II, como los Hermes 450, Aerostar y Hermes 180, o los de Clase I, incluyendo los Thunder B, Orbiter 3 y Skylark, igualmente de procedencia israelí. En contraste, en el enfrentamiento entre Rusia y Ucrania, hubo una tendencia mucho más pronunciada hacia el uso casi exclusivo de drones de clase militar I, lo que refleja una estrategia de vigilancia y reconocimiento significativamente diferente entre los dos conflictos, recurriendo en uno de ellos a aparatos de mayor envergadura mientras que en el otro parece haber una tendencia hacia aparatos menores.

Pero además de estos aparatos de categoría militar, como apuntan Plokšto y Demeško (2017, p.70), en Ucrania las operaciones militares incorporaron también modelos de uso “civil”, es decir, drones comerciales, o aparatos creados *ad hoc* empleando componentes inicialmente no destinados a uso militar. Esto claramente marca una diferencia notable con la guerra de Artsaj, en la que, según los datos disponibles, las partes recurrieron casi exclusivamente a drones de categoría militar. Esto podría apuntar, sin duda a una implementación diferenciada de ambos conflictos desafiando la idea de una implementación lineal de las innovaciones militares.

En el caso de Ucrania dichos aparatos comerciales que incluyeron, según la comparativa realizada, cuadricópteros como los Evo II o los drones Mavic desarrollados por la compañía asiática DJI, cambian en muchos sentidos la manera en la que se abordan los combates en el suelo, ya que permitieron a los soldados de unidades tácticas más reducidas llevar consigo sus propios drones para llevar a cabo sus operaciones ISR o de ataque. La mayoría de estos dispositivos civiles son muy ligeros (< 2kg), pueden ser portados por una única persona y generalmente no necesitan infraestructura compleja para poder ser operados (Kunertova, 2023b, p.578). Además de esto, es muy importante destacar que se trata de productos más baratos y más fácilmente reemplazables, lo que puede resultar provechoso en conflictos en los que las probabilidades de perder equipamiento aéreo son más elevadas. Esto último es un aspecto que se tratará en detalle en puntos posteriores, pero esto demuestra un cambio considerable a la hora de recurrir a drones en ambos conflictos, cambiando así las tácticas de guerra.

b) Uso combinado de drones y coordinación con sistemas lanzacohetes múltiple

Si se habla exclusivamente de los drones con capacidad ISR, muchas veces se hace considerable énfasis en su capacidad de recopilación de información ya que no disponen de capacidad de ataque, pero se suele destacar menos frecuentemente su relevancia a la hora de realizar operaciones en combinación con otros drones y con otras capacidades de ataque, situaciones que claramente muestran su relevancia. Según las fuentes consultadas, esta práctica fue recurrente en ambos conflictos estudiados, lo que puede mostrar como el uso de estos dispositivos pudo aportar ventajas a las partes que lo usan para alcanzar sus objetivos bélicos, sobre todo, en términos de precisión e identificación de objetivos.

En el caso de Ucrania, según Kunertova (2023b, p.581), el número de drones desplegados de clase I, fue notablemente superior al de cualquier guerra pasada. Lo más interesante es que muchos de ellos fueron drones únicamente con capacidades ISR y se usaron de forma conjunta con otros aparatos similares llegando a alcanzar grandes enjambres. Por ejemplo, durante un sobrevuelo de la ciudad de Bakhmut se llegaron a usar hasta 50 de ellos conjuntamente para la realización de misiones ISR. Según los datos de este autor, la recopilación de información por estos aparatos permitió detectar alrededor del 86 % de los objetivos. Aunque esta cifra sea un tanto difícil de comprobar, denota claramente la importancia del papel de los drones y su uso combinado con otros tipos durante la guerra. En el caso de Rusia, de la misma manera, la estrategia militar muchas veces no solo incorporó un único dron para realizar operaciones de vigilancia, sino varios de ellos localizados a distintas alturas sobre el mismo objetivo. Esto se realizó para poder recopilar datos e imágenes complementarias del objetivo para realizar operaciones más precisas posteriormente (Karber, 2015, p.13).

Por otro lado, en el caso de la guerra de Nagorno-Karabaj, es interesante destacar que Azerbaiyán recurrió al antiguo AN-2, un avión de combate prácticamente obsoleto que fue modificado para ser usado como señuelo para descubrir las defensas antiaéreas armenias. Dichos sistemas de defensa eran consecutivamente reconocidos por otros drones con capacidades ISR para poder ser detectados y posteriormente neutralizados (Díaz Rosaenz, 2021, p.22). Eso también prueba este uso combinado de drones para

conseguir objetivos militares. Además de ese uso, otros drones de clase III únicamente con capacidad ISR según la clasificación de la OTAN, como los Hermes 900 o los Heron, también fueron utilizados para realizar vuelos de alta altura para adquirir información sobre los blancos, reconocer los elementos terrestres desplegados e incrementar la efectividad de los ataques. Este uso combinado de drones y su gran utilidad para la identificación de objetivos parece no haber sido del todo utilizado por parte de Armenia, en parte, debido a su escasez de VNTC, lo que pudo disminuir claramente su capacidad para realizar ataques de las mismas características. Dicho esto, el uso combinado de drones efectivamente puede aportar una ventaja táctica a las partes que los implementan de manera efectiva en el campo de batalla.

Es cierto que los drones ISR pueden tener algunas desventajas, como, por ejemplo, (1) la necesidad de planificación previa contra objetivos fijos, (2) la falta de reprogramación rápida de las rutas o (3) las dificultades para rastrear objetivos móviles (Karber, 2015, p.13) pero aun así su relevancia parece alta cuando se utilizan en conjunto con otros métodos de ataque, como es el caso de la coordinación con sistemas de lanzacohetes múltiples. En el contexto de la guerra en Ucrania, se ha observado desde el principio el uso extensivo de numerosos drones para la identificación de objetivos, lo que ha facilitado la ejecución de ataques altamente letales y precisos, como los realizados por sistemas de lanzamiento de cohetes BM-21 MLRS (Karber, 2015, p.13). Este patrón de utilización de drones seguido de ataques mediante otros medios se observa en todos los conflictos estudiados y por todas las partes. A pesar de que estos sistemas difieren en su origen y fabricación, el principio es similar. Después de identificar los objetivos mediante drones, estos se retiran, y aproximadamente 15 minutos después se inicia un ataque con misiles lanzados desde sistemas de lanzacohetes múltiples. Posteriormente, una vez transcurrido un breve lapso desde el lanzamiento de los misiles, los drones regresan a la zona atacada para evaluar los daños causados (Karber, 2015, p.13). Estas operaciones se inscriben en el denominado “reconnaissance strike complex” (Jones, 2022, p.17) diseñado para coordinar armas de largo alcance y alta precisión junto con la recopilación de inteligencia en tiempo real, en aras de lograr una velocidad de reacción más rápida (Frías Sánchez, 2021, p.1061).

*c) Aplicación práctica del uso combinado de VNTC con sistemas
MRLS*

En primer lugar, en la guerra entre Rusia y Ucrania desde 2014, se han destacado varios casos de implementación de sistemas MRLS por parte de Rusia, siendo uno de los más notorios la batalla de Zelenopillya del 11 de julio de ese año. Se trata de un caso emblemático de la efectividad de los drones ISR en la detección y ataque preciso de objetivos. En efecto, según Kowrach (2018, p.30), durante esta confrontación se evidenció cómo Rusia, mediante el uso de VNTC, logró averiguar la ubicación de un grupo de tropas ucranianas que se habían concentrado hacia el norte en la autopista que conduce a la ciudad de Luhansk y lanzar un devastador ataque con el sistema de lanzacohetes múltiples BM-21 Grad. En cuestión de minutos, las fuerzas rusas lograron aniquilar prácticamente dos batallones y diezmar la 79ª Brigada Aerotransportada. Es importante decir que este evento no solo mostró la capacidad de los drones para mejorar significativamente la precisión de los ataques, sino también las consecuencias que puede tener eso en el campo de batalla, obligando a crear grupos de tropas que sean más dinámicos y pequeños para poder evitar este tipo de ataques. Pero, además de esto, se puso de evidencia las consecuencias de la falta de capacidades de detección por parte de las fuerzas ucranianas, lo que indica claramente que la efectividad de estos drones y sistemas de ataque está supeditada en muchas situaciones a la falta de presencia de contramedidas por parte de los adversarios. Pero más allá del caso concreto de esta batalla, la utilización de estos sistemas no se limitó a ataques aislados. Como señala el mismo autor, la integración de estas estrategias facilitó una serie de ataques en los meses subsiguientes, resultando en acciones ofensivas decisivas, concretamente 53 ataques dirigidos a 40 localizaciones distintas, que permitieron a las fuerzas pro-rusas presentes en el Dombás a avanzar significativamente en la región.

En el caso de Ucrania, también se pudieron ver aplicaciones concretas de drones ISR en combinación con sistemas de ataque de artillería como MLRS o los sistemas de artillería de alta movilidad HIMARS proporcionados por Estados Unidos. Según algunos informes, se pone de evidencia que estos sistemas utilizaron para atacar de manera recurrente puntos estratégicos de la logística rusa, consiguiendo en algunos momentos de la guerra “poner en llamas” importantes depósitos de armas (Szóke y Kusica, 2023, p.7). Sin la recopilación de información mediante la colaboración internacional, pero también

mediante el uso de drones de categoría militar y de rango civil. El uso de estos dispositivos de artillería no habría sido posible y, sin duda, no habría permitido a Ucrania avanzar o conseguir alcanzar objetivos concretos en momentos determinados. Todo ello, no obstante, debe matizarse con referencia a otros factores que serán discutidos en los siguientes apartados.

Por último, en el caso de la guerra de Nagorno-Karabaj, es importante destacar que el conflicto estuvo dividido en dos fases. La primera de ellas se libró durante las tres primeras semanas en las zonas más planas circundantes del enclave que habían sido controladas por parte de Armenia desde el alto al fuego de 1994. Esa fase de la guerra se concentró en las regiones de Fuzuli y Jabrail en la frontera con Irán, y según numerosos informes, se destaca que fue en ese momento en el que se identificó la mayor superioridad técnica y militar de Azerbaiyán, sobre todo a nivel aéreo, mediante el uso de VNTC para misiones ISR que permitieron identificar objetivos armenios de manera efectiva. Azerbaiyán recurrió a drones militares de categoría militar como el Bayraktar TB-2 de clase III según la clasificación de la OTAN (anexo 1.2) que, a pesar de tener capacidad de ataque propio, también fue utilizado de manera bastante notable para misiones ISR (Jones, 2022, p.17-20), recopilando datos que también permitieron orientar los sistemas de disparo de artillería MRLS por parte de Azerbaiyán contra objetivos específicos armenios. Esto supuso una ventaja frente a la parte opuesta, pero también muestra que la efectividad de estos aparatos depende en gran medida de la capacidad de otros sistemas para llevar a cabo sus ataques de forma precisa.

2. VNTC con capacidad ISR y realización de ataques directos

a) El éxito de los drones de categoría militar en la guerra de Nagorno-Karabaj

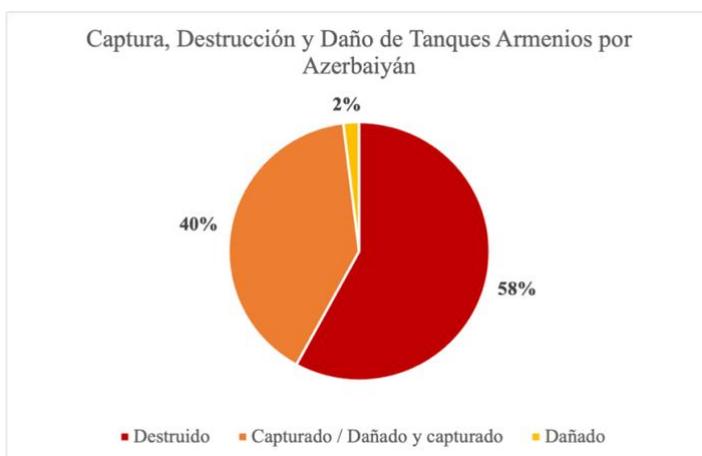
Si se habla de VNTC con capacidad ISR y de ataque directo, parece relevante comenzar analizando el caso de su implementación en la guerra de Nagorno-Karabaj. En los primeros días tras el comienzo de los ataques, comenzó, como se dijo anteriormente, la primera fase de la guerra en la que Azerbaiyán consiguió alcanzar rápidamente una superioridad frente a su oponente. La ofensiva se realizó por varios frentes, atacando “todo el frente del dispositivo defensivo” (Díaz Rosaenz, 2021, p.7) armenio sobre todo en las regiones norte y sur del enclave disputado. Las tropas se introdujeron así en una

breve guerra de desgaste, pero rápidamente se pusieron de manifiesto las pocas ganancias significativas de las fuerzas terrestres. En ese momento fue cuando la importancia de los VNTC implementados por Azerbaiyán comenzó a hacerse evidente. El país utilizó numerosos drones de rango militar, sobre todo de clase III como los turcos Bayraktar TB-2 que gracias a sus capacidades ISR y de ataque directo, permitieron destruir las defensas aéreas armenias y alcanzar una gran cantidad de objetivos de manera efectiva (Frías Sánchez, 2021, p.1061). Se trata de sistemas altamente sofisticados que tienen un rango de control de hasta 300 km, una autonomía de hasta 27 horas de vuelo (anexo 1.2) y están equipados con pequeñas municiones MAM-C de 20 libras y MAM-L de 50 libras que permiten realizar ataques directos, precisos y de gran impacto. Así, gracias a la superioridad aérea presentada por Azerbaiyán sobre todo gracias a los Bayraktar TB-2, a los pocos días el sistema defensivo armenio colapsó (Díaz Rosaenz, 2021, p.8).

También es importante destacar el papel de las municiones merodeadoras en este éxito en el campo de batalla, que introdujeron una dimensión adicional en la estrategia de combate. Se trata de armas capaces de permanecer en el área de operaciones a la espera de identificar un objetivo y posteriormente dirigirse a gran velocidad hacia él para autodestruirse causando daños. Aquí es importante destacar la coordinación de estas municiones, con drones únicamente con capacidad ISR y otros con capacidad de ataque directa. Como indica Onetto (2021, p.90), es el empleo coordinado de drones merodeadores como los Harop o la línea Orbiter de origen israelí con otro tipo de dispositivos de clases elevadas, como el Bayraktar-TB2 lo que subraya la importancia estratégica de estas tácticas en el conflicto. La efectividad de estas tácticas se vio reflejada en la destrucción de importantes activos antiaéreos. Gazpio (2021) destaca cómo los sistemas de misiles antiaéreos TOR-M2KM de fabricación rusa fueron neutralizados por ataques de municiones merodeadoras Harop y por los drones Bayraktar TB-2, reduciendo significativamente las capacidades de defensa aérea de Armenia. Este impacto fue amplificado por la destrucción de numerosas unidades de defensas aéreas armenias, incluidos sistemas 9K33 OSA y 9K35 Strela, durante las primeras dos semanas de enfrentamientos, un hecho resaltado por Pérez Arrieu y Allende (2021), quienes documentan la pérdida de alrededor 60 unidades de estas defensas.

No obstante, entre todos los VNTC y municiones merodeadoras que fueron importantes para el éxito bélico de Azerbaiyán, el papel de los Bayraktar TB-2 fue de los

más relevantes. Efectivamente, fue uno de los aparatos que realmente causó una diferencia notoria, ayudando a Azerbaiyán a alcanzar sus objetivos militares. A pesar de que la obtención de información sobre el equipamiento perdido durante una guerra puede ser una tarea desafiante, es importante intentar acercarse lo máximo posible a la realidad para poder realizar observaciones verídicas. Para evaluar cómo fue eliminado cierta parte del equipamiento Armenia se recurrió a los datos disponibles en la web Oryx, que como se ha explicado en la sección de metodología, es una plataforma que proporciona datos detallados sobre las pérdidas de material bélico en diversos conflictos, combinando fuentes abiertas y fotografías geolocalizadas.

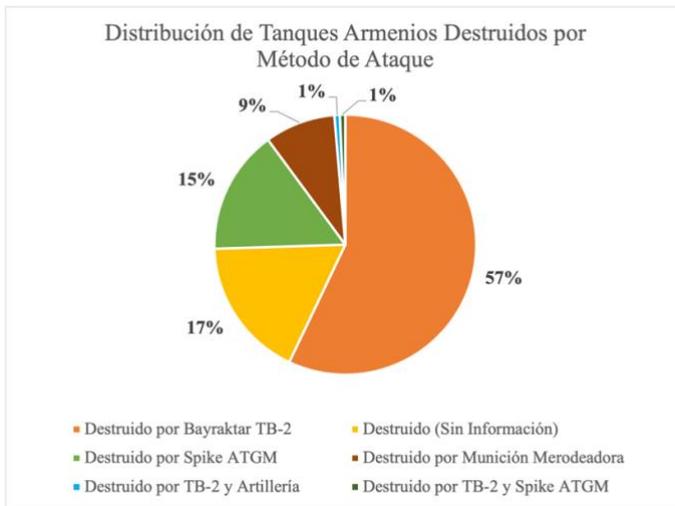


Elemento gráfico 2: Gráfico de elaboración propia en Microsoft Excel © con datos de Oryx (2023)

El gráfico anterior muestra una representación de los datos obtenidos de la web de Oryx sobre los tanques armenios alcanzados por la ofensiva de Azerbaiyán a lo largo del conflicto. Es preciso recordar que el presente análisis está sujeto a las limitaciones inherentes al seguimiento de conflictos armados con fuentes abiertas, y se reconoce la posibilidad de que existan ciertos eventos no documentados. Sin embargo, la información presentada ofrece una estimación sustancial del equipamiento afectado. En la elaboración de este gráfico se recopilaban y categorizaron datos específicos de los tanques armenios afectados, incluyendo los modelos T-72 Ural, T-72A, T-72AK, T-72AV, T-72B, y otras variantes T-72 no especificadas. Los resultados se clasificaron según el estado en que cada tanque fue afectado: destruido, capturado/dañado y posteriormente capturado, o solo dañado.

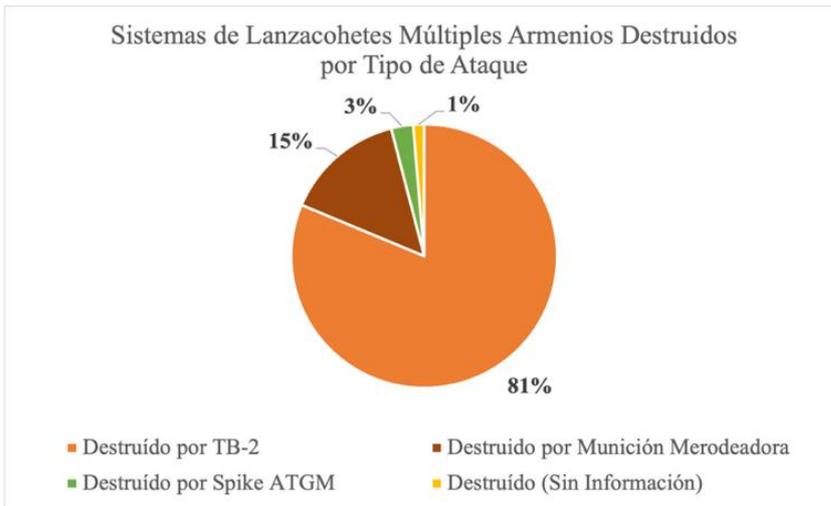
De acuerdo con los datos resultantes (elemento gráfico 2), se puede decir que la mayor parte de los tanques alcanzados por Azerbaiyán (el 58%) fueron destruidos,

mientras que un 40% fueron capturados o dañados y luego capturados. Estos valores muestran que la destrucción representa más de la mitad de los incidentes documentados, lo cual destaca la severidad del impacto sufrido por los tanques armenios en manos azeríes. Por otro lado, un marginal 2% corresponde a tanques que únicamente sufrieron daños, pero no fueron totalmente neutralizados.



Elemento gráfico 3: Gráfico de elaboración propia en Microsoft Excel © con datos de Oryx (2023)

Estos datos son relevantes para observar la eficacia de los ataques azeríes, pero si se desglosa el 58 % anterior, que corresponde a los tanques destruidos por las fuerzas de Azerbaiyán, se puede observar que la mayor parte de los daños fueron causados por el Bayraktar TB-2. En efecto, por sí solo, representa el 57 % de las causas de destrucción de tanques armenios (elemento gráfico 3) lo que resalta de manera significativa la eficiencia e importancia de los VNTC en la estrategia militar de Azerbaiyán, sobre todo estos de una clase militar elevada. Frente a estos datos imponentes, el gráfico también revela que el 15 % de los tanques restantes fueron destruidos por misiles antitanque guiados (ATGM) tipo Spike, 9 % fue destruido por munición merodeadora y otros fueron destruidos por la combinación de drones como el Bayraktar TB-2 y fuego de artillería. Este último caso fue el menos recurrente, pero aun así los datos revelan la integración de capacidades aéreas y terrestres en operaciones combinadas para alcanzar objetivos bélicos. El 17 % restante representa aquellos tanques sobre los que no se dispone información específica sobre la causa de su destrucción.



Elemento gráfico 4: Gráfico de elaboración propia en Microsoft Excel © con datos de Oryx (2023)

Por último, el mismo procedimiento fue realizado para identificar la causa de destrucción de sistemas de lanzacohetes armenios por tipo de ataque (elemento gráfico 4). Los datos son todavía más sorprendentes. Los datos apuntan a que en torno al 81 % de estos sistemas fueron destruidos por el Bayraktar TB-2, mientras que únicamente el 19 % restante fue destruido por munición merodeadora, artillería u otras causas no identificadas. Estos datos revelan claramente la importancia de los drones con capacidades ISR y ataque directo para alcanzar objetivos, lo que ayudó a Azerbaiyán a superar las dificultades experimentadas durante la primera fase. Esto también demuestra que los VNTC no fueron únicamente utilizados para misiones ISR.

b) Drones con capacidad de ataque directo en la guerra de Rusia contra Ucrania

En el caso de la guerra de Rusia contra Ucrania desde el 2014, según los datos sobre drones con capacidad de ataque directo (anexo 1.2), las partes recurrieron a drones de ataque de clase III y a otros de clases inferiores. Ucrania recurrió a los Tupolev T-141, Tupolev-143, y a los Bayraktar TB-2 al igual que en Nagorno-Karabaj, mientras que, en el caso de Rusia, únicamente se podría destacar el uso del Orion. Todos ellos son VNTC con capacidad para llevar a cabo ataques directos de forma nativa o si son modificados para ello. Sin embargo, se puede observar una diferencia clara en comparación con la guerra del Cáucaso: el uso de drones de clases inferiores. Similar a lo que se pudo observar en la sección relativa a los drones únicamente con capacidad ISR. Efectivamente, tanto Rusia como Ucrania, recurrieron de manera más pronunciada al uso

de este tipo de dispositivos, muchos de ellos, naturalmente, de rango militar como los Switchblade 300, ST-35 o los R-18 utilizados por Ucrania, o los Lancet-3, Kalashnikov KUV o Zastava utilizados por Rusia. Todo ello, sin olvidar la implementación sin precedentes de drones comerciales.

Los drones de clase III como los Bayraktar TB-2, al igual que en Nagorno-Karabaj, permitieron alcanzar objetivos bélicos de manera más precisa. Por ejemplo, estos drones ayudaron a Ucrania a contrarrestar eficazmente las ofensivas rusas en las primeras etapas después de la invasión del 2022 (Kreps & Lushenko, 2023, p.272). No obstante, los ataques realizados por estos VNTC muchas veces se recogen de manera puntual y anecdótica, y parecen disminuir a medida que se avanza en el conflicto. En ningún caso se encuentran datos tan flagrantes como en Nagorno-Karabaj. Algunos informes como los de Konaev (2023, p.9), Eslami (2022, p.509) o Antal (2022, p. 213), efectivamente, destacan que el Bayraktar TB-2 fue útil para la destrucción de tanques de combustible, sistemas de defensa, antimisiles o convoyes militares y se destacan algunos hitos de guerra en los que contribuyeron como durante el hundimiento del navío de guerra ruso Mosková en 2022. Pero, de nuevo, la importancia de estos drones en este conflicto parece no ser tan evidente.

Las municiones merodeadoras también fueron relevantes sobre todo para el bando ruso. A partir de mediados del 2022, Rusia comenzó a adquirir sistemas de drones merodeadores suicida a Irán, llamados drones kamikaze Shahed-136 (Kunertova, 2023, p.96). Estos drones fueron utilizados desde octubre del 2022, para alcanzar infraestructura civil y otros objetivos. Uno de los momentos en los que su uso fue más importante fue por ejemplo en mayo del 2023 cuando Rusia desplegó cerca de 60 drones Shahed sobre Kiev (Konaev, 2023, p.9). Según datos de Al Jazeera (2023), tras el ataque 200 edificios de la capital, incluyendo 77 residenciales, sufrieron cortes de electricidad. No obstante, al igual que los drones con capacidad de ataque directa como los Bayraktar TB-2, el énfasis sobre la eficacia de estos sistemas no es tan constante ni unívoco. Se comenta que Ucrania gracias a sus sistemas de defensa fue capaz de interceptar cerca del 80 % de estos drones y aunque el restante 20 % consiguió causar estragos, muchas veces no se trató de eventos que se pudiesen considerar como un avance o ventaja significativa en la guerra.

Como destaca Kunertova (2023b, p.583), en la guerra de Ucrania los drones se

han convertido en elementos consumibles como “balas o artillería” muchas veces debido a su precio inferior, esto marca una innovación y diferencia en comparación con conflictos previos (Lowther & Siddiki, 2022, p.4-5). El ejemplo más claro de esta tendencia es la implementación de drones comerciales a gran escala en el frente para misiones de ISR y/o ataque directo. Desde el principio de la guerra, más de 200 empresas en el territorio nacional ucraniano están manufacturando este tipo de drones y compañías internacionales también pusieron a disposición de las tropas sus dispositivos. Cuando llevaron consigo algún tipo de carga explosiva, actuaron prácticamente como dispositivos explosivos improvisados (Fogel, 2022) ayudando a las tropas que los usaban a alcanzar objetivos puntuales desplegando pequeñas granadas o cargas explosivas sin poner en riesgo equipamiento militar de alto valor. Pero, además de estos pequeños logros tácticos, algunas empresas también han desarrollado en base a estos modelos comerciales dispositivos más sofisticados capaces de llevar consigo cargas explosivas mayores. Este es el caso, por ejemplo, de la compañía ucraniana Aerorozvidka fundada por jóvenes ucranianos independientes durante las revueltas del Euromaidan del 2014 (Borger, 2022).

Entre todos los drones que fueron desarrollados por este grupo de técnicos, se llegaron a crear aparatos de ocho rotores, de aproximadamente 1,5 m de envergadura y capaces de lanzar bombas y granadas antitanque propulsadas. Uno de los mayores éxitos de estos drones, fue durante la invasión de Ucrania del 2022, cuando el grupo colaboró en las ofensivas contra la columna mecanizada de tanques de aproximadamente 40 millas de longitud que se dirigía hacia Kiev por el frente del norte. Esta colaboración con las tropas desplegadas por parte de Ucrania permitió, según diversas fuentes, destruir varios de los vehículos que encabezaban el convoy, causando así importantes dificultades para el avance de las tropas (Borger, 2022) y dificultando claramente la consecución de los objetivos de Moscú. Es preciso volver a destacar que el uso de estos dispositivos de combate aéreo se menciona de una manera más esporádica y puntual en este conflicto y su contribución a alcanzar la victoria es mucho más cuestionable que en el caso de la guerra del Cáucaso.

3. Factores externos para determinar la contribución real a la victoria

En las secciones anteriores se detalló cómo los drones implementados mejoraron la capacidad de recopilación de información para llevar a cabo ataques más precisos contra objetivos enemigos, ya sea de manera directa o mediante la combinación con otros tipos de armas, contribuyendo así a la consecución de los objetivos militares de las partes involucradas. No obstante, al observar estos momentos de éxito de una manera detallada, se infiere que la eficacia de los drones es relativa al contexto y a los factores externos del campo de batalla. Como propone Díaz Rosaenz (2021), la eficacia de los sistemas debe ser “entendida como parte de un sistema más amplio integrado por aeronaves tripuladas, sistemas de comando y control y artillería terrestre combinando la capacidad de adquirir, guiar, atacar y engañar al enemigo” (p.16).

a) Inversión militar y capacidades de respuesta

Uno de los elementos importantes a considerar son las diferencias de inversión militar entre las partes involucradas. En primer lugar, si se habla de los gastos militares en función del PIB de los países se observa que en el caso de Ucrania y Rusia ambas mantuvieron niveles de inversión relativamente estables entre el 2003 y el 2021, situados, aproximadamente en 2,6 % en el caso de Ucrania y 4,03 % en el de Rusia (World Bank Open Data, 2024a). En segundo lugar, en el caso de Azerbaijón y Armenia, se observa que la inversión de estos dos países sigue una tendencia similar al alza desde el 2003 y sufriendo aumentos y disminuciones similares a lo largo del tiempo (World Bank Open Data, 2024b). No obstante, si se recurre al gasto nominal de estos estados se puede observar que la situación cambia considerablemente. Mientras el gasto de Rusia, en la misma temporada, se sitúa de media en los 70.000 millones de dólares americanos, la inversión ucraniana se situó constante en torno a los 3000 millones de dólares americanos. De forma similar, en el caso de Azerbaijón, la inversión fue del 2003 al 2021 superior a la de Armenia, alcanzando de media 1800 millones de dólares americanos anuales y en el caso de Armenia una media de 429 millones de dólares.



Elemento gráfico 5: Gráfico de elaboración propia en Microsoft Excel © con datos de World Bank Open Data (2024b)



Elemento gráfico 6: Gráfico de elaboración propia en Microsoft Excel © con datos de World Bank Open Data (2024a)

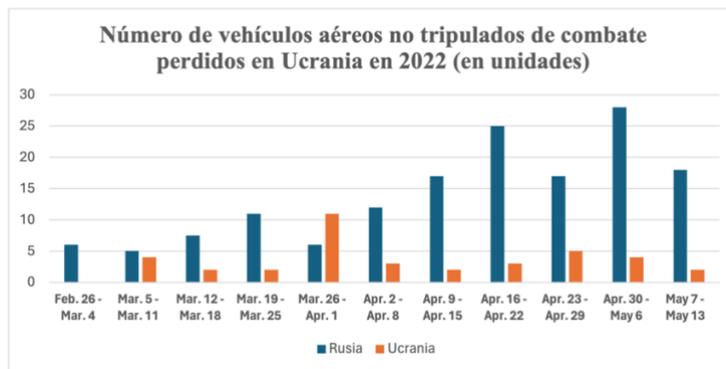
Estas diferencias presupuestarias permitieron a Azerbaiyán adquirir una gran cantidad de armas, no solamente de Rusia, pero también de otros países como Israel y Turquía (Ilić & Tomašević, 2021, p.11). Efectivamente, entre el 2000 y el 2019, Azerbaiyán obtuvo el equivalente a 825 millones de dólares en armas de Israel y aproximadamente 123 millones de Turquía, en el caso de este último país, esa inversión le permitió adquirir varias unidades del Bayraktar TB-2, sistemas MLRS y otros tipos de munición, lo que le permitió crear un arsenal militar notablemente superior al de su oponente (Ilić & Tomašević, 2021, p.11). Además, considerando que Azerbaiyán recurrió a lo largo de la guerra a importantes ataques aéreos para llevar a cabo su ofensiva, la capacidad de respuesta adversaria a este tipo de ataques es fundamental para poder comprender la eficacia de los drones (Popescu, 2021, p.40).

Aquí es donde las diferencias de capacidades armamentísticas se ponen de manifiesto. Al igual que existieron diferencias en la cantidad de dispositivos MLRS disponibles para las partes, por ejemplo, de 30 a 40 unidades del BM-30 Smerch para el bando azerí frente a únicamente 6 unidades para Armenia (Ilić & Tomašević, 2021, p.11), también se observaron diferencias en las características de los sistemas antiaéreos

implementados. Efectivamente, Armenia disponía de sistemas antiaéreos que, además de haber sido destruidos en las dos primeras semanas de conflicto como se detalla anteriormente, no eran del todo eficaces contra los VNTC azeríes (Jones, 2022, p.1). Muchos de estos sistemas como los OSA, Krug y Stela-10 eran sistemas de la época de la Guerra Fría y los más nuevos que fueron adquiridos como los S-300 y los TOR-M2KM no estaban preparados para derribar aparatos con baja velocidad de vuelo y capaces de realizar vuelos de baja altura como los Bayraktar TB-2. Para poner un ejemplo, el sistema de defensa antiaéreo SA-8 utilizado por Armenia únicamente era capaz de derribar con éxito objetivos que volasen a una velocidad de al menos 365 km/h y los drones turcos empleados por Azerbaiyán realizaban vuelos a aproximadamente 200 km/h (Pérez Arrieu & Allende, 2021, p.36). Lo mismo sucedió con antiguos cañones antiaéreos ZSU-23-4 y el 9k33 Osa, “quienes eran víctimas de los drones sin que estos estuvieran dentro de su alcance” (Díaz Rosaenz, 2021). Frente a esta deficiencia en la capacidad de respuesta por parte de Armenia, las fuerzas azeríes “se nuclearon sobre sistemas de largo alcance rusos S-300PMU-2 [...]” todos ellos sistemas modernizados de alcance medio que consiguieron hacer frente a la gran mayoría de los vehículos aéreos implementados por Armenia (Díaz Rosaenz, 2021, p.19).

Todo lo anterior, hizo que, naturalmente, las tropas azeríes pudiesen llevar a cabo sus operaciones sin ser frenadas por la capacidad de respuesta de Armenia, por tanto, efectivamente los drones permitieron a una de las partes alcanzar la victoria, pero esto se debió en gran parte a las grandes diferencias existentes en cuanto a equipamiento. En el caso de la guerra de Rusia contra Ucrania, la situación fue considerablemente distinta. A pesar de las diferencias en cuanto a inversión militar destacadas anteriormente, muchas de las dificultades en cuanto a equipamiento militar, encontradas por Ucrania fueron superadas gracias a la forma de implementar sus tácticas de combate, la manera en la que realizaron sus maniobras y gracias al equipamiento recibido por colaboradores internacionales (Congressional Research Service, 2023). Algunos de estos sistemas proporcionados sobre todo por países occidentales incluyeron, por ejemplo, el conocido sistema de cohetes de artillería HIMARS proporcionado por Estados Unidos, sistemas de defensa antiaérea o equipamiento de artillería (Hsiao-Huang, 2020). Todo ello, sin mencionar la colaboración ucraniana con “empresas de defensa occidentales tras la invasión de Crimea en 2014” lo que equipó al ejército ucraniano con sistemas de guerra electrónica y radares antiaéreos (Lowther y Siddiki, 2022, p.11-12).

Considerando la adquisición de estos dispositivos de defensa por ambas partes, se puede afirmar que ambos estados demostraron una alta capacidad de respuesta ante ataques con drones, lo que comprometió la efectividad de su extenso arsenal de estos equipos (Chávez, 2023) y puso en duda su contribución a alcanzar la victoria en el campo de batalla. En efecto, al principio de la invasión rusa de Ucrania del 2022, muchos de los drones desplegados por Rusia, como los Orlan-10 de clase I y con capacidad ISR y ataque directo, fueron rápidamente abatidos por las tropas ucranianas y no fueron del todo efectivos (Eslami, 2022, p.510). Teniendo esto en cuenta, Rusia pareció desplegar con mayor cautela sus vehículos aéreos no tripulados de grado militar “para maniobras de alto riesgo y objetivos de alto valor” (Chávez, 2023, p.1) por miedo a perderlos.



Elemento gráfico 7: Gráfico de elaboración propia en Microsoft Excel © con datos de Jones (2022)

Esta observación se ve respaldada por los datos presentados por Jones (2022, p.23), con base en las fuentes públicas Oryx (2022) y ACLED. Al inicio de la invasión rusa de 2022, marcada por una significativa retirada de la ofensiva del norte poco después de su comienzo, se evidencia que la pérdida de drones rusos fue menor en comparación con etapas posteriores. Esto sucedió a pesar de la firme respuesta de Ucrania en dicha área, especialmente entre el 26 de febrero y el 6 de abril de 2022, periodo durante el cual se detuvo la ofensiva del norte para enfocar todos los esfuerzos en la región del Dombás (Jones, 2022, p.18). Cabe matizar que posteriormente en el conflicto, Rusia logró desplegar de manera efectiva sistemas de guerra electrónica, alterando significativamente la dinámica del enfrentamiento. Estos sistemas permitieron a Rusia ejecutar ataques contra drones ucranianos y otros dispositivos operando en variadas bandas del espectro electromagnético, contrarrestando así la ventaja inicial de Ucrania en el uso de drones al comienzo de la guerra. Entre los sistemas desplegados se destacan el Krasukha-2/4, el R-330Zh Zhitel y el RB301B Borisoglebsk-2 (Lowther & Siddiki, 2022, p.12) que

consiguieron derribar hasta 41 drones ucranianos entre los cuales se encontraban 11 unidades de Bayraktar TB-2 (Jones, 2022, p.23).

Dicho esto, se puede concluir que la colaboración de los drones a alcanzar la victoria por las partes depende en gran medida de las capacidades de respuesta del oponente. Mientras que en la guerra del Cáucaso Azerbaiyán pudo hacer uso más efectivo de estos aparatos debido a la debilidad armenia, en el caso de la guerra de Rusia contra Ucrania, esto no fue del todo cierto debido a las capacidades de ambas partes de responder de manera efectiva a este tipo de ataques. Esta capacidad simétrica de respuesta probablemente fue uno de los factores que contribuyeron al surgimiento y al uso incrementado de drones comerciales en la guerra por ambas partes.

b) Importancia de la logística

Es preciso apuntar que el éxito de los drones para alcanzar la victoria por las partes depende de forma considerable de los aspectos logísticos y organizativos subyacentes a su implementación en el campo de batalla. Más allá de la mera capacidad militar y la sofisticación tecnológica, la eficacia en la gestión y despliegue de estas tecnologías resulta crítica. Pero además de eso, no solo la logística propia sino también la logística del adversario. En el contexto de la invasión rusa de Ucrania en 2022, la estrategia inicial rusa contemplaba ataques simultáneos a través de múltiples frentes: norte, noreste, este y sur, buscando una rápida captura de Kiev y otros centros urbanos importantes desde Bielorrusia, según numerosos informes, para forzar la capitulación del gobierno ucraniano (Jones, 2022). Sin embargo, este plan ambicioso se vio comprometido por problemas logísticos significativos.

Las operaciones, aunque coordinadas en su inicio, revelaron una falta de previsión estratégico-logística por poner un foco demasiado importante a nivel táctico, lo que impactó negativamente en la provisión de material necesario para el ejército y redujo la capacidad operacional de manera significativa (Skoglund et al., 2022). El intento de tomar el aeropuerto de Antonov y la ausencia de un plan de contingencia efectivo subrayan las deficiencias en la planificación y ejecución logística. Esto llevó a la adaptación forzosa de la estrategia rusa, reorientando sus esfuerzos hacia el sur y el este, especialmente en la región del Dombás, ante la imposibilidad de avanzar hacia Kiev debido a la combinación

de una férrea resistencia ucraniana y las propias falencias logísticas (Jones, 2022; Skoglund et al., 2022). Por tanto, la implementación de drones de combate en una situación en la que la logística de las partes no es adecuada, puede colaborar a la falta de eficiencia para alcanzar la victoria. Mostrando así, una relación sumamente importante entre la implementación de estas nuevas tecnologías y la realidad conjunta de los demás medios de combate.

De la misma manera, es interesante destacar que, en momentos de considerable avance de una de las partes, incluso con la combinación de drones y sistemas de lanzamiento de cohetes, se observa que estos logros frecuentemente se deben a deficiencias logísticas o debilidades evidenciadas por el oponente. Como destacan Gady y Kofman (2023, p.8), gran parte de la estrategia ofensiva de Ucrania en su conflicto con Rusia se centró en tácticas de desgaste y el empleo de "bombardeos intensivos" para alcanzar objetivos militares. A pesar de la utilización de sistemas MRLS como los HIMARS en combinación con la información obtenida mediante drones con capacidad ISR, estos autores destacan que la guerra de maniobras dio resultados mixtos, y no pudo ser completamente implementada por Ucrania. Indican que muchos de estos ataques de precisión hacia las redes de mando y control o las vías de comunicación terrestre del adversario fueron eficaces cuando las condiciones de la guerra de desgaste eran propicias. Todo ello, por supuesto, independientemente de la tecnología empleada.

Un ejemplo que proporcionan estos autores es el avance logrado por las fuerzas ucranianas en la región de Kharkiv, considerada una de las victorias tácticas más importantes de Ucrania desde el comienzo de la invasión. En menos de 10 días, las fuerzas armadas ucranianas consiguieron recuperar aproximadamente 6000 km² de territorio ocupado por Rusia. Durante esta ofensiva, se emplearon diversos métodos de ataque, incluyendo numerosos sistemas MRLS, que sin duda contribuyeron al logro de los objetivos militares. No obstante, también es crucial destacar la situación del adversario en el momento de esta victoria táctica. En ese momento, Rusia estaba llevando a cabo una "reubicación de unidades regulares del ejército y un equipamiento sustancial a los óblasts de Kherson y Zaporizhia en julio y agosto de 2022" (Gady y Kofman, 2023, p.8) anticipando ataques ucranianos en esas regiones. Esta estrategia resultó crucial para el

éxito de Ucrania en la ofensiva de Kharkiv porque la falta de refuerzos rusos llevó al colapso de su posición.

Todo lo anterior demuestra que la incorporación de drones, junto con las innovaciones que presentan, no puede estar dissociada de cómo se implementan tanto las estrategias logísticas propias como las del adversario. El simple despliegue de estos sistemas al margen de una ofensiva bien preparada y coordinada revela que, por sí mismos, estos sistemas no garantizan el éxito.

c) Límites técnicos, tropas y equipamiento tradicional

La implementación coordinada de los vehículos aéreos autónomos de combate mencionada en la última sección revela claramente que la contribución a la victoria por estos aparatos no es absoluta, y que el papel de otros factores es altamente relevante. En este contexto es muy importante resaltar el papel jugado por el equipamiento militar tradicional y los efectivos terrestres en los conflictos analizados. Esto entra en contraposición con una de las principales tesis sobre estos aparatos que afirma que a medida que estas nuevas tecnologías se van incorporando al campo de batalla, el papel de las tropas pasa a un segundo plano. Sin embargo, la evidencia encontrada en los conflictos de Azerbaiyán y de Rusia contra Ucrania subrayan la persistencia del combate convencional y la relevancia crítica de las fuerzas terrestres.

En este sentido, Fox (2017, p.31) destaca cómo desde el comienzo del conflicto ruso-ucraniano, hubo un despliegue considerable de unidades provenientes tanto de los ejércitos nacionales, por ejemplo, tropas del ejército ucraniano para realizar una de las contraofensivas más importantes en el continente europeo desde el fin de la segunda guerra mundial (Karber, 2015, p.36), como de *proxies*, notablemente grupos separatistas ucranianos. Pero lo más importante de esta movilización es que incluyó combates intensos y directos por parte de las tropas en oposición al uso de armamento a gran escala. La batalla de Sloviansk en julio de 2014 es un ejemplo destacado de estas tácticas, demostrando el impacto decisivo de las fuerzas especiales ucranianas y la brigada número 95 al recuperar el control de la tercera ciudad más importante del Dombás realizando acciones cuerpo a cuerpo y hasta a veces combate puerta por puerta con el objetivo de minimizar las bajas humanas (Karber, 2015, p.36).

Además de las operaciones en Ucrania, la relevancia de los combatientes terrestres también fue relevante en la guerra de Nagorno-Karabaj. Efectivamente, a pesar de la creciente importancia de los drones y la tecnología de vigilancia, el combate terrestre y las capacidades militares convencionales mantuvieron un papel fundamental (Díaz Rosaenz, 2021, p.25). Después de la primera fase de la guerra, en la que los drones jugaron un papel central, en la segunda fase se requirió una gran cantidad de ataques cuerpo a cuerpo, la tecnología amplificó el poder humano en lugar de reemplazarlo, pasó en cierta medida a segundo plano y se hizo evidente la importancia de la presencia humana en el campo de batalla (Díaz Rosaenz, 2021, p.25). Esto último se debió principalmente a que las tropas azeríes se adentraron progresivamente en las regiones montañosas de Nagorno-Karabaj, donde la eficacia de los vehículos de combate aéreo fue menor debido a la complejidad del terreno y a las limitaciones técnicas de estos dispositivos en dicho entorno (Díaz Rosaenz, 2021, p.17). Kunertova (2023, p.98) refuerza este argumento, señalando que la cantidad de bajas entre las tropas rusas y ucranianas y, por extensión, armenias y azeríes destaca la centralidad de los humanos en combate, a pesar de la utilización extensiva de drones.

Finalmente, aunque los VNTC y otras tecnologías avanzadas han transformado ciertos aspectos de la guerra moderna, no han eliminado la necesidad de operaciones terrestres ni la eficacia del combate cercano como se ha visto en ambos conflictos. Esto se ve claramente en la operación para la conquista de la ciudad de Shusha, en la que el éxito militar se debió en gran parte a la capacidad de las tropas para realizar operaciones cuerpo a cuerpo, donde la destreza y el valor individual siguen siendo decisivos (Díaz Rosaenz, 2021, p.25). La persistencia de estas tácticas, incluso en una era de guerra híbrida y automatizada, recalca la importancia inalterable de los soldados y el equipamiento militar tradicional en el logro de objetivos estratégicos.

A modo de conclusión de este capítulo, cuyo objetivo era identificar y comparar los drones, que fueron utilizados en ambos conflictos centrándose en su contribución a la victoria, se puede decir que en lo relativo a la primera hipótesis específica, contrariamente a lo que se había previsto, a pesar de que la inclusión de los VNTC creó cambios en la estrategia tradicional de la guerra, su implementación en ambos conflictos no fue

completamente similar. A pesar de que se recurrió a VNTC de clase III en ambos conflictos, la guerra en Ucrania destacó por la implementación pionera de drones comerciales en sus operaciones, desafiando la premisa de que predominaría el uso de drones de categoría militar. Este hallazgo contradice la premisa sobre la prevalencia del uso de VNTC de categoría militar en ambos conflictos. Además de esto, se había anticipado que el uso de estos aparatos habría sido principalmente para misiones ISR, mejorando así la precisión en la identificación de objetivos. De nuevo, esto únicamente fue demostrado parcialmente, ya que a pesar que los drones con capacidades ISR fue relevante y permitió obtener alta precisión para llevar a cabo ataques mediante sistemas MRLS, los VNTC con capacidad para realizar acciones ofensivas directas también fue muy importante, sobre todo en la guerra de Azerbaiyán contra Armenia, en la que estos sistemas no solo mejoraron la capacidad de los ataques, sino que en ocasiones, fueron responsables de más de la mitad del daño infligido al equipamiento adversario.

Con respecto a la segunda hipótesis específica, que anticipaba que la efectividad de los drones en alcanzar la victoria depende del contexto, y aunque transforman el panorama de la guerra, no eliminan la necesidad de combate directo ni de armamento tradicional, ni garantizan por sí solos la victoria, se concluye que esta hipótesis se valida plenamente a la luz de los hallazgos. Efectivamente, se corroboró que la eficacia de los drones se ve significativamente influenciada por su integración con otras formas de ataque, sobre todo para los drones únicamente con capacidad ISR que requirieron la combinación con artillería y sistemas de lanzamiento de misiles para ser efectivos contra las fuerzas enemigas. Además, se confirmó la suposición de que factores externos a la mera implementación de estos dispositivos juegan un rol crucial en determinar su éxito en el campo de batalla. Entre estos factores, las disparidades en inversiones militares, el apoyo internacional, la habilidad para neutralizar los drones enemigos, así como la organización y logística tanto propia como del adversario, se identificaron como elementos decisivos. Estos factores externos mostraron que efectivamente, tal y como se había previsto, la eficacia de los VNTC fue mayor en un conflicto que en otro, por ejemplo, en la guerra de Nagorno-Karabaj debido a la falta de capacidades de defensa armenias. Todo esto lleva a concluir que los drones complementaron más que reemplazaron el equipamiento militar tradicional, mejorando la eficacia de ciertos ataques en ambos conflictos, pero no se reemplazó el papel central de las tropas o del armamento convencional.

B. CAPITULO 2: Acciones ofensivas en el ciberespacio

1. Conceptualización y dimensiones clave

Siguiendo la estructura marcada, el segundo capítulo del trabajo está dedicado específicamente a las acciones ofensivas en el ciberespacio. En él se pretende identificar y comparar qué acciones en el ciberespacio fueron utilizadas en ambos conflictos y evaluar si contribuyeron a alcanzar la victoria por las partes. Dicho objetivo específico tiene una hipótesis específica que plantea que las acciones en el ciberespacio simplemente complementaron la guerra y tienen alcances limitados en ambos conflictos. Efectivamente, se presupone que, si bien las acciones en el ciberespacio lograron interrumpir temporalmente las comunicaciones y la logística del adversario, o desmoralizarlo, no tuvieron un impacto duradero en la capacidad operativa global de las fuerzas enemigas. De la misma manera, se presupone que dichas acciones estuvieron coordinadas con ataques terrestres, que las redes sociales se convirtieron en un campo de batalla psicológico, que el alcance de las acciones en el ciberespacio fue más importante en la guerra de Rusia contra Ucrania que en la de Nagorno-Karabaj y, por último, que dichas acciones fueron llevadas a cabo principalmente por grupos no militares.

Antes de comenzar esta sección, parece relevante especificar de lo que se está hablando, y tal y como lo explican Mladenovic y Radunovic (2018), cuando se hace referencia a las acciones ofensivas en el ciberespacio, nos referimos a las operaciones cibernético-ofensivas que se llevan a cabo en el dominio y “teatro de operaciones” que es el ciberespacio (p.102). En la cumbre de la OTAN de Varsovia en 2016, el ciberespacio pasó a ser reconocido como un dominio operacional en sí mismo, al igual que otros dominios, como el terrestre, el marítimo, el aéreo o el espacial (Fuente Cobo, 2022, p.88). Esto quiere decir que se trata de un área en la que se pueden realizar operaciones militares, utilizando capacidades específicas para influir, afectar o controlar la información digital y las infraestructuras civiles o militares.

Pero este nuevo dominio operacional no puede ser entendido si no se especifica mejor cuáles son sus componentes. En este sentido, se suelen reconocer tres dimensiones que ilustran las distintas acciones ofensivas que se realizan en este teatro de operaciones: (1) la dimensión ciber-lógica; (2) la dimensión ciber-física y; (3) la dimensión ciber-

informativa/cognitiva (Mladenovic & Radunovic, 2018). La primera de ellas es considerada como la más tradicional y se refiere a las operaciones que tienen lugar dentro de las redes y sistemas informáticos, como el *hackeo* o la inserción de *malware*. La segunda reconoce que el ciberespacio está conectado con el mundo físico a través de sistemas que pueden ser controlados digitalmente, por ejemplo, numerosas infraestructuras críticas civiles (red eléctrica...) y, por tanto, las acciones ofensivas en esta dimensión buscan afectar el mundo físico mediante acciones concretas. Por último, la tercera se centra en la influencia sobre la percepción, decisiones y comportamientos de las personas a través de operaciones en el ciberespacio. Esto incluye, por ejemplo, la guerra de información en redes sociales.

2. Acciones llevadas a cabo en función de las dimensiones del ciberespacio

a) Acciones en las dimensiones ciber-físicas y ciber-lógicas

Según la literatura consultada, se puede decir que entre los dos conflictos hubo diferencias considerables en lo que se refiere a las acciones ofensivas en las dimensiones ciber-físicas y ciber-lógicas. En primer lugar, a pesar de que es difícil identificar el origen de un ataque cibernético, en la guerra de Nagorno-Karabaj ninguno de los países implicados parece haber contado con unidades militares especializadas en realizar ciberoperaciones ofensivas, pero, aun así, se pudo observar una activa participación de grupos independientes denominados grupos de *hacktivistas*, un vocablo inglés, que surge de la combinación de las palabras *hackers* y *activistas*. En otras palabras, se trata de grupos independientes no vinculados formalmente a ningún Estado, pero que realizan este tipo de acciones de apoyo en un contexto bélico o conflicto determinado.

En lo que respecta al ambiente ciber-lógico, Onetto (2021) señala que los grupos de *hacktivistas* por ambas partes lanzaron operaciones contra medios de comunicación adversarios, demostrando la naturaleza descentralizada y no oficial de las acciones en el ciberespacio en este contexto (p. 90). Estas actividades tienen mucho que ver con el concepto de guerra híbrida propuesto en el marco teórico para comprender la naturaleza de las guerras estudiadas, ya que pone de manifiesto cómo individuos y colectivos pueden influir significativamente en el desarrollo de un conflicto sin estar directamente

vinculados a las estructuras gubernamentales o militares de un estado, trascendiendo así el concepto tradicional de la guerra en términos de Clausewitz.

El Centro Criptológico Nacional (CCN, 2021) documenta varias instancias de ciberataques que tuvieron lugar durante el conflicto, incluyendo ataques de denegación de servicio (DDoS) por parte de “*Anonymous Greece*” contra 77 sitios web gubernamentales azerbaiyanos con el dominio *gov.az*, o la alteración de contenido en sitios armenios y de Nagorno-Karabaj por el “*Karabak Hacking Team*”. Este último grupo confirmado, alteró el contenido de 46 principales sitios web gubernamentales a las pocas semanas del comienzo de la guerra. Estos ataques, aunque limitados debido a su carácter revocable y a su impacto poco duradero, demostraron la capacidad de los grupos independientes para interrumpir temporalmente el acceso a recursos informativos y manipular la información en línea (p. 61). La mayoría de los servicios informáticos afectados volvieron a la normalidad al cabo de horas, o en el peor de los casos, días. Antes del estallido del conflicto, ya se habían registrado ataques similares, como el llevado a cabo por “*Sakhavat & Ferid*” que desfiguró el portal gubernamental y la web del primer ministro de Armenia, inyectando contenido político.

En segundo lugar, en lo relativo a las acciones ofensivas en el ciberespacio durante el conflicto entre Rusia y Ucrania, es crucial distinguir la naturaleza y la escala de estas operaciones en comparación con lo observado en la guerra de Nagorno-Karabaj. Las acciones cibernéticas emprendidas por Rusia han jugado un papel significativamente más crítico y extenso, apuntando a una amplia gama de objetivos dentro de Ucrania con el propósito de debilitar su capacidad militar, gubernamental y económica. En este sentido, Konaev (2023) destaca la intensidad y el enfoque de las actividades de amenaza cibernética de Rusia en este contexto, señalando que estas acciones han buscado degradar, interrumpir y destruir las funciones militares, gubernamentales y económicas de Ucrania. Además, también fue atacada infraestructura civil crítica, cadenas de suministro y centros logísticos, intentando limitar el acceso del público ucraniano a la información (p. 13). Aunque existen similitudes entre la implementación en ambos contextos, parece que también hubo cambios considerables.

Numerosos estudios proporcionan una perspectiva cronológica que ilustra como, desde el inicio de las tensiones en el Dombás en el 2014 hasta febrero del 2022, Rusia, o

grupos de *hacktivistas*, fueron ejecutando varias series de ataques cibernéticos contra Ucrania en las dimensiones ciber-lógicas y físicas. El análisis de Przetacznik y Tarpova (2022, p.4), destaca que estos ataques han variado desde operaciones de denegación de servicio distribuido (DDoS), que fueron destinadas a desestabilizar redes y comunicaciones ucranianas a principios de marzo del 2014, hasta esfuerzos por manipular los resultados de las elecciones presidenciales ucranianas a través de grupos *hacktivistas* pro-rusos ese mismo año.

Sin embargo, un aspecto muy interesante en este sentido es que las acciones ofensivas no tuvieron únicamente la intención de causar alteraciones en páginas web o desestabilizar, como en el caso de la guerra de Azerbaiyán contra Armenia, sino que los ataques se realizaron también en el ámbito ciber-físico con consecuencias tangibles y, en ocasiones, causando alteraciones considerables. Esta diferencia con la guerra de Nagorno-Karabaj también muestra que las guerras contemporáneas, pueden ser notablemente distintas, y de nuevo, no seguir una progresión lineal o unívoca en lo que se refiere a la aplicación de estas nuevas tecnologías en los enfrentamientos.

Przetacznik y Tarpova (2022) detallan cómo, por ejemplo, ataques de denegación de servicio distribuido (DDoS) en diciembre de 2015 y enero de 2016 resultaron en cortes de energía y apagones en Kiev, afectando a más de 230.000 consumidores y mostrando la capacidad de las operaciones cibernéticas para impactar directamente en la infraestructura crítica de un país (p. 4). Más tarde, En la víspera de la invasión a gran escala de Ucrania en febrero de 2022, grupos pro-rusos intensificaron también sus esfuerzos realizando numerosos ataques contra Ucrania, por ejemplo, desplegando *malware* destructivo como HermeticWiper, dirigido a agencias gubernamentales y bancos ucranianos. El mismo día de la invasión, un ciberataque también logró interrumpir los módems Viasat KA-SAT en Ucrania, afectando no solo a Ucrania sino también causando interrupciones en Alemania, el Reino Unido y otras ubicaciones (Grossman et al., 2023, p. 11). Posteriormente, se desplegaron varios *wipers* en las redes ucranianas, como Industroyer2, un *wiper* que ya había sido utilizado en el 2016 específicamente contra la infraestructura eléctrica de Ucrania. Estos ataques, que continuaron de febrero a abril, se centraron en perturbar las operaciones normales del gobierno y afectar infraestructura crítica, reflejando un uso estratégico de las capacidades cibernéticas para complementar operaciones militares convencionales (Grossman et al., 2023, p. 11). Por último, además

de estos ataques dirigidos a infraestructuras e instituciones estatales, grupos pro-rusos no identificados también lanzaron *malware* y ataques de *phishing* contra servicios gubernamentales y ciudadanos ucranianos, ampliando así el espectro de su campaña cibernética contra Ucrania (Przetacznik & Tarpova, 2022, p. 4).

En respuesta a los ataques rusos, Ucrania, junto con *hackers* independientes de todo el mundo, lanzó contraataques cibernéticos dirigidos a sistemas gubernamentales, medios de comunicación, instituciones financieras, y otras infraestructuras críticas en Rusia. Estos esfuerzos no solo buscaban interrumpir las operaciones rusas sino también exponer y difundir datos sensibles del gobierno y financieros rusos. De la misma manera posteriormente, grupos no identificados, también llevaron a cabo más acciones ofensivas en el ciberespacio contra Rusia (Przetacznik & Tarpova, 2022, p. 5) que, aunque también fueron limitados, consiguieron alterar páginas oficiales y canales informativos.

La coordinación entre operaciones cibernéticas y acciones militares cinéticas es una pregunta recurrente y difícil de contestar con el contexto de una guerra híbrida como las que se estudian en este documento, pero al mismo tiempo es una de las respuestas más interesantes para la evaluación del impacto estratégico de los ataques cibernéticos en conflictos modernos. En el presente caso, tanto Przetacznik & Tarpova (2022) como Grossman et al. (2023) sugieren que, en el caso de la guerra en Ucrania, es altamente probable que los ataques cibernéticos hayan sido cuidadosamente coordinados con la invasión cinética del país. Esta coordinación se podría ilustrar con el despliegue del *malware* HermeticWiper el 23 de febrero, coincidiendo justamente con la invasión cinética y subrayando así una sincronización deliberada entre los esfuerzos cibernéticos y militares (Grossman et al., 2023). En el caso de Azerbaiyán y Armenia, aunque los ataques no hayan tenido tanto impacto y no se hayan producido exactamente el día del comienzo de la ofensiva, sí que se vieron periodos en los que se realizaron este tipo de operaciones al mismo tiempo que se llevaban a cabo las acciones militares.

La utilización estratégica de operaciones cibernéticas en conjunción con acciones militares directas amplifica significativamente su efectividad. Aunque muchos ataques pueden no tener un impacto duradero, su capacidad para generar inseguridad, tensión, e ineficiencia dentro de las instituciones afectadas es indudable. En efecto, cuando se coordinan adecuadamente con operaciones cinéticas, pueden ayudar a alcanzar los

objetivos de las partes, pero por si solos difícilmente pueden asegurar la victoria como se ha visto a través de estos dos casos.

Para concluir esta sección, la comparación entre los conflictos en Ucrania y Nagorno-Karabaj revela diferencias significativas en la naturaleza y alcance de los ataques cibernéticos. En el contexto de Nagorno-Karabaj, aunque los ataques cibernéticos se llevaron a cabo durante el conflicto, la evidencia de operaciones cibernéticas coordinadas directamente con acciones militares es menos clara, y no hay documentación sustancial de ataques contra infraestructura crítica armenia o azerí por parte de los estados respectivos. A diferencia de Ucrania, donde los ataques se dirigieron no solo a sistemas de información sino también a infraestructura crítica como redes eléctricas y servicios de emergencia, en Nagorno-Karabaj, los ataques se centraron más en objetivos gubernamentales y de información, sin incursiones significativas en el dominio físico como sistemas eléctricos o de suministro de agua.

b) Acciones en el ciber espacio en la dimensión ciber-cognitiva

En lo que se refiere a la dimensión ciber-cognitiva, la guerra de Nagorno-Karabaj proporciona un estudio de caso revelador sobre cómo la guerra de la información y las campañas en redes sociales pueden influir profundamente en la percepción pública y la moral de un conflicto. La combinación de tecnología militar avanzada, como los drones de combate, con estrategias de comunicación en el ciberespacio, subrayó la naturaleza multifacética de la guerra moderna, donde el campo de batalla se extendió al ámbito cognitivo de las poblaciones involucradas. En este sentido, Onetto (2021) señala que en el conflicto de Nagorno-Karabaj, tanto gobiernos como actores no estatales recurrieron a medios no violentos y a la guerra de la información, destacando el papel crucial de las redes sociales en la difusión de información (p. 90). Efectivamente, la dimensión informativa se convirtió en una herramienta muy eficaz para ayudar a alcanzar la victoria de las partes, no únicamente en el campo de batalla, sino también en las mentes.

Díaz Rosaenz (2021) profundiza esta idea, explicando cómo el uso de tecnología en la guerra como el uso de VNTC, permitió la grabación constante y la difusión de imágenes de los combates, inundando así las redes sociales con contenido que tenía como objetivo influir en la percepción pública y desmoralizar al enemigo. Algunas de esas

imágenes fueron reproducidas por *youtubers* o simplemente compartidas a través de las redes sociales. Rostomyan (2023) confirma esta dinámica, indicando que la publicación en redes sociales de imágenes de ataques y las consecuencias de la guerra ayudó a “visualizar el impacto de la guerra” (p.12), motivando a la población y creando un terreno fértil para la difusión de narrativas específicas. En este proceso de adquisición de imágenes jugó también un papel relevante la diferencia en cuanto a capacidad tecnológica de las partes. Antal (2022) proporciona un análisis específico sobre cómo la superioridad tecnológica de Azerbaiyán en el uso de drones afectó la dimensión ciber-cognitiva del conflicto. Los videos de alta calidad mostrando la destrucción de defensas aéreas y objetivos armenios por drones turcos Bayraktar TB-2 y misiles merodeadores israelíes Harop tuvieron un impacto significativo en la moral armenia (p. 213).

En el caso de la guerra de Ucrania, igual que en Nagorno-Karabaj, la guerra psicológica incluyó propaganda, grabación de vídeos de emboscadas o grabación de destrucción de objetivos para colgar en las redes sociales. Geers (2015) proporciona un análisis un tanto temprano de la guerra de la información en Ucrania, señalando que, desde el comienzo del conflicto en 2014, Rusia mostró una ventaja considerable en el control de la información en las redes sociales, utilizando la desinformación y ejerciendo control sobre plataformas como VKontakte que dispone, según datos del 2021, de más de 1000 millones de cuentas creadas y aproximadamente 63 millones de usuarios activos mensualmente. Konaev (2023) amplió este punto, indicando que Rusia también ha utilizado las redes sociales principalmente para difundir mensajes de apoyo a su "operación especial", movilizar a los ciudadanos rusos, desacreditar a los líderes ucranianos y difundir datos sobre la “cultura occidental”. Esta estrategia de operaciones de influencia se dirige a múltiples audiencias, incluyendo tanto a la población interna de Rusia como a audiencias internacionales, buscando socavar el apoyo a Ucrania y a las instituciones occidentales (p. 14).

Del mismo modo, el uso de cuentas falsas y sistemas automatizados de publicación (*bots*) como parte de las estrategias en la guerra de información marca un desarrollo en el aspecto ciber-cognitivo de las guerras contemporáneas. Este fenómeno se observó en ambos conflictos. En primer lugar, en el contexto de Nagorno-Karabaj, Onetto (2021) destaca cómo Azerbaiyán orquestó una intensa guerra de información en paralelo a las hostilidades físicas (DFRLab, 2021), utilizando plataformas como Twitter y

Facebook para difundir información favorable. Facebook informó sobre la eliminación de una vasta red azerbaiyana que incluía 589 cuentas de Facebook y 7.906 páginas de Instagram, señalando el papel de estos "*bots*" en la promoción de publicaciones pro-azeríes y la diseminación de información beneficiosa para Azerbaiyán (p. 100). Por el lado armenio, Thomas y Zhang (2020) observaron la emergencia de numerosas cuentas sospechosas dedicadas a retuitear contenido pro-armenio en X (anteriormente Twitter), muchas de las cuales presentaban los mismos errores tipográficos, indicando una alta probabilidad de que fueran cuentas falsas diseñadas para amplificar contenido (p. 9). En segundo lugar, En el caso de Ucrania también se identificaron acciones muy similares. Konaev (2023) reportó que, durante los primeros días de la guerra, Facebook desmanteló una red operada desde Rusia y Ucrania por violar las políticas de comportamiento inauténtico coordinado. En este sentido, Shen et al. (2023) proporcionan una perspectiva cuantitativa, identificando que aproximadamente el 13.4% de las cuentas en X durante la guerra de Rusia y Ucrania fueron *bots*, responsables de alrededor del 16.7% de los *tweets* publicados.

A pesar de las diferencias en las tácticas específicas de guerra de la información y el uso de plataformas digitales entre los conflictos en Nagorno-Karabaj y Ucrania, una constante se mantiene clara: tanto antes del inicio de las hostilidades como durante ellas, la cantidad de interacciones a través de medios digitales, incluyendo mensajes de apoyo a los países enfrentados, experimentó un incremento significativo. Esta tendencia se evidencia a través del uso de *hashtags* en redes sociales a lo largo de ambos conflictos, destacando la importancia de estas plataformas como campos de batalla para la conciencia y el apoyo internacional.

En el caso de Nagorno-Karabaj, antes del comienzo de la guerra en septiembre de 2020, varios análisis revelaron una predominancia de *hashtags* pro-azerbaiyán sobre aquellos pro-armenia, con una significativa diferencia en el volumen de menciones. Esto sugiere una mayor movilización o eficacia en la utilización de redes sociales por parte de Azerbaiyán para difundir su narrativa y conseguir apoyo (Onetto, 2021, p. 94). Este es un dato que contrasta con los datos obtenidos justo después del comienzo de la guerra, cuando se identificaron de manera generalizada un mayor número de *hashtags* pro-armenia que pro-azerbaiyán. Estas diferencias muestran que, dependiendo de la situación hubo un mayor apoyo en las redes sociales a un bando o a otro, pero todo sirve para

mostrar la misma idea de que las redes sociales se convirtieron efectivamente en una dimensión clave para ganar ventajas por parte de los estados a nivel cognitivo y así animar o desanimar a las distintas partes. A medida que avanzaba el conflicto, surgieron nuevos hashtags que se extendieron rápidamente a través de las redes, como *#WeWillWin* y *#StopAzerbaijanAggression*, reflejando una estrategia de comunicación multilingüe y transnacional para capturar la atención y solidaridad internacional (Onetto, 2021, p. 90).

De manera similar, durante la guerra de Rusia contra Ucrania, los hashtags pro-ucranianos predominaron en los primeros momentos de la invasión, aunque se observaron variaciones en el uso de *hashtags* pro-rusos en momentos determinantes del conflicto, como después de votaciones en la Asamblea General de la ONU. Este dinamismo en el uso de *hashtags* refleja los cambios en la percepción pública y la movilización de apoyo a nivel global, adaptándose a los desarrollos en el terreno (Zia et al., 2023, p. 4).



Elemento gráfico 8: Captura de X mostrando el “hilo” publicado por Kardashian (2020). Traducción automática del inglés por X.

Durante los conflictos, la participación de celebridades y la movilización de las diásporas armenia y ucraniana, junto con las cuentas especializadas conocidas como "milblogs", también demostraron el considerable poder de estas figuras y colectivos para influenciar la narrativa y movilizar apoyo global. Un ejemplo de este tipo de cuentas puede ser por ejemplo la cuenta de la *influencer* americana Kim Kardashian que, debido a su ascendencia armenia, generó una amplia resonancia en redes sociales, con

publicaciones que lograron más de 24.000 comentarios, 22.000 *retweets* y 45.000 “me gusta”, evidenciando cómo individuos de alto perfil pueden dirigir la atención hacia causas específicas (Kardashian, 2020). Paralelamente, la diáspora armenia, descrita por Chernobrov (2022, p. 643) como un ejército de "ciber-combatientes", utilizó tácticas coordinadas para aumentar la visibilidad de contenido pro-Armenia, mientras que, en Ucrania, la intensificación de contenidos pro-rusos por parte de milbloggers durante momentos críticos del conflicto refleja una estrategia similar para influir en la percepción pública y apoyar operaciones de influencia (Katalinić, 2023, p. 1111).

A pesar de existir similitudes entre la manera en la que se utilizaron las redes sociales para llevar a cabo estrategias en el ámbito cibernético, en Ucrania, la estrategia de Rusia ha sido más sofisticada y multifacética, aprovechando su control sobre los canales de información para lanzar campañas a gran escala en busca de desestabilizar e impactar la opinión pública a nivel global. Sin embargo, es crucial destacar que las redes sociales se convirtieron en un campo de batalla adicional que complementó al resto de ataques terrestres y no terrestres. Como señala Chernobrov (2022, p. 643), estas acciones, a pesar de su importancia, funcionaron en conjunto con las operaciones militares, intentando influir en políticas, apoyar a los propios y desmoralizar a los oponentes, aunque los resultados de estas campañas en el ciberespacio sobre el resultado final de la guerra puedan ser discutibles.

Para concluir este capítulo, se puede decir que la hipótesis que preveía que las acciones en el ciberespacio sirvieron principalmente como complemento a las operaciones de guerra física, y tuvieron alcances limitados, ha sido corroborada por los hallazgos de este estudio. Las acciones en el ciberespacio lograron interrumpir las comunicaciones y la logística del adversario, o desmoralizarlo, en ambos conflictos, aunque de manera temporal y con variaciones significativas en su alcance y efectividad. Por ejemplo, el alcance de estos ataques fue notablemente mayor en la guerra de Rusia contra Ucrania, ya que incorporó, además de las dimensiones ciber-lógicas, ataques en el resto de las dimensiones del ciberespacio. En particular, se destaca que, en el conflicto ruso-ucraniano, el espectro de los ataques se extendió a infraestructuras críticas civiles y militares, demostrando un uso más sofisticado y amplio del ciberespacio como herramienta de guerra. Los resultados también indican que las acciones ofensivas en el ciberespacio fueron generalmente llevadas a cabo por grupos no directamente vinculados

a gobiernos ni a estados y estuvieron coordinadas con operaciones terrestres, tal y como se había previsto. Esto claramente refuerza la idea de una guerra híbrida, donde el ciberespacio se integra de manera efectiva en la estrategia militar general para desestabilizar y debilitar a los adversarios, preparando el terreno para ofensivas físicas y generando ventajas tácticas considerables. Finalmente, en el ámbito de las redes sociales se observó que se convirtieron en un frente psicológico e informativo crucial. Aunque estas acciones no produjeron cambios físicos directos en el campo de batalla, desempeñan un papel significativo en la guerra híbrida, influenciando la percepción y el ánimo de los involucrados a través de la difusión de propaganda, desinformación, y sobre todo contenido gráfico obtenido a lo largo de las ofensivas.

VII. Conclusiones

El presente trabajo fin de grado ha abordado un estudio comparativo de dos escenarios de conflicto contemporáneos, la guerra de Nagorno-Karabaj en 2020 y la guerra de Rusia contra Ucrania iniciada en 2014, con el objetivo de identificar similitudes y diferencias de la implementación de VNTC y acciones ofensivas en el ciberespacio, evaluando si contribuyeron a alcanzar la victoria.

La hipótesis general planteada suponía una utilización diferenciada de VNTC y de acciones en el ciberespacio en ambos conflictos, con resultados divergentes debido a factores externos y de implementación. Esta hipótesis ha sido validada. Se ha constatado que, si bien hay una adopción generalizada de los VNTC y de las acciones en el ciberespacio en ambos conflictos, las metodologías y efectos divergieron significativamente. En Ucrania, el uso innovador de drones comerciales y la extensión de ciberataques a infraestructuras críticas destacaron, mostrando un panorama más amplio y sofisticado de guerra híbrida. Mientras tanto, en Nagorno-Karabaj, los drones jugaron un papel directamente ofensivo y crítico, a menudo causando más de la mitad del daño enemigo. Este éxito flagrante del conflicto en el Cáucaso, no fue replicado de la misma manera en Ucrania sobre todo, debido a factores externos, más allá de la propia implementación de estas nuevas tecnologías en el campo de batalla.

Efectivamente, las conclusiones de los capítulos específicos apoyan la afirmación

de que, a pesar del papel transformador de estas tecnologías en la estrategia militar, no suplantaron a los métodos convencionales en ninguno de los conflictos estudiados. El éxito militar sigue siendo el resultado de la concurrencia de varios factores, donde la tecnología moderna actúa como un complemento que potencia y amplía las capacidades ofensivas, pero en ningún caso las reemplaza. Los drones y las operaciones cibernéticas, aunque cruciales, no garantizan la victoria por sí solos, ya que su eficacia está intrínsecamente ligada a la sinergia con operaciones terrestres convencionales, el apoyo internacional, las inversiones militares y la capacidad de cada parte para contrarrestar las tácticas implementadas por el adversario. La naturaleza híbrida de la guerra contemporánea, caracterizada por la intersección de lo físico y lo digital, se refleja claramente en la integración efectiva del ciberespacio y de los VNTC en la estrategia militar general. Las acciones cibernéticas, aunque indirectas, y generalmente menos evidentes, han probado ser eficaces en desmoralizar y desestabilizar, además de servir como complemento para sus ofensivas físicas para potenciar y alcanzar los resultados bélicos.

En última instancia, este trabajo confirma que la naturaleza de la guerra ha evolucionado con la progresiva implementación de tecnologías como los VNTC. Sin embargo, subraya igualmente que la esencia del conflicto armado y la búsqueda de la victoria siguen siendo un dominio en el que el ingenio humano, la estrategia, las capacidades de respuesta y las realidades político-económicas tienen un impacto decisivo. En consecuencia, aunque cambian las tácticas y la estrategia de la guerra, esta última sigue estando profundamente supeditada al éxito de los principios fundacionales de las confrontaciones militares.

VIII. Anexos

A. Anexo 1: Tabla comparativa de drones implementados en los conflictos, clasificados en función de su uso primordial

1. Vehículos autónomos de combate aéreo con capacidades ISR

Leyenda:

	Clase I OTAN
	Clase II OTAN
	Clase III OTAN
	Dispositivo Comercial

Azerbaiyán	Ucrania	Rusia
<p>Hermes 900 (Israel)</p> <p>Rango de control (alcance): 2500km Autonomía: 36h Altura máxima: Alta</p> <p>Usos: ISR</p>	<p>PD-2 (Ucrania)</p> <p>Rango de control (alcance): 200km Autonomía: 10h Altura máxima: Media</p> <p>Usos: ISR + Dirección/Corrección de Trayectorias de Fuego de Artillería</p>	<p>Eleron-3 (Rusia)</p> <p>Rango de control (alcance): 250km Autonomía: 1h45 Altura máxima: Baja-Media</p> <p>Usos: ISR</p>
<p>Heron (Israel)</p> <p>Rango de control (alcance): >1000km Autonomía: >30h Altura máxima: Media</p> <p>Usos: ISR</p>	<p>Spectator-M1 (Ucrania)</p> <p>Rango de control (alcance): 200km Autonomía: 3h Altura máxima: Baja</p> <p>Usos: ISR a nivel táctico (portátil por personal militar)</p>	<p>Granat (Rusia)</p> <p>Rango de control (alcance): 180km Autonomía: 6h Altura máxima: Baja-Media</p> <p>Usos: ISR + Intercepción de Comunicaciones (a través de SIGINT)</p>
<p>Searcher (Israel)</p> <p>Rango de control (alcance): 350km Autonomía: 17h Altura máxima: Media</p> <p>Usos: ISR</p>	<p>FlyEye (Polonia)</p> <p>Rango de control (alcance): 180km Autonomía: 2,5h Altura máxima: Baja</p> <p>Usos: ISR + Dirección de trayectorias de fuego de artillería</p>	<p>Supercam S450 (Russia)</p> <p>Rango de control (alcance): 100km Autonomía: 7h Altura máxima: Baja-Media</p> <p>Usos: ISR</p>
<p>Hermes 450 (Israel)</p> <p>Rango de control (alcance): 200km Autonomía: 17h Altura máxima: Media</p> <p>Usos: ISR</p>	<p>Magylas (Estonia)</p> <p>Rango de control (alcance): 120km Autonomía: 2h Altura máxima: Baja (no confirmado)</p> <p>Usos: ISR + Dirección de trayectorias de fuego de artillería</p>	<p>Takhion (Russia)</p> <p>Rango de control (alcance): 40km Autonomía: 6h Altura máxima: Baja</p> <p>Usos: ISR</p>

<p>Aerostar (Israel)</p> <p>Rango de control (alcance): 200 km Autonomía: 12h Altura Máxima: Media</p> <p>Usos: ISR a nivel táctico</p>	<p>PD-1 (Ucrania)</p> <p>Rango de control (alcance): 100km Autonomía: 7h Altura máxima: Baja</p> <p>Usos: ISR + “Foto mapeo”</p>	<p>421-16E2 (Rusia)</p> <p>Rango de control (alcance): 35km Autonomía: 4h Altura máxima: Baja</p> <p>Usos: ISR</p>
<p>Hermes-180/200 (Israel)</p> <p>Rango de control (alcance): 150km Autonomía: 10h Altura máxima: Baja</p> <p>Usos: ISR a nivel táctico</p>	<p>Sparrow (España)</p> <p>Rango de control (alcance): 70km Autonomía: 1h30 Altura máxima: Baja</p> <p>Usos: ISR & Ajustar/direccionar artillería</p>	<p>421-08M (Rusia)</p> <p>Rango de control (alcance): 30km Autonomía: 1h30</p> <p>Usos: ISR táctico</p>
<p>Thunder B (Israel)</p> <p>Rango de control (alcance): 150km Autonomía: 24h Altura máxima: Baja</p> <p>Usos: ISR a nivel táctico</p>	<p>A1-SM Furia (Ucrania)</p> <p>Rango de control (alcance): 50km Autonomía: 3h Altura máxima: Baja</p> <p>Usos: ISR</p>	<p>Merlin-VR (Rusia)</p> <p>Rango de control (alcance): Desconocido. Autonomía: 10h Altura máxima: Baja-Media</p> <p>Usos: ISR</p>
<p>Orbiter 3 (Israel)</p> <p>Rango de control (alcance): 150km Autonomía: 6h Altura máxima: Baja-Media</p> <p>Usos: ISR a nivel táctico</p>	<p>Leleka-100 (Ucrania)</p> <p>Rango de control (alcance): 45km Autonomía: 2h30 Altura máxima: Baja</p> <p>Usos: ISR</p>	<p>EVO II (China) → Compra libre.</p> <p>Rango de control (alcance): 13km Autonomía: 40 min Altura máxima: Baja-Media</p> <p>Usos: Cuadricóptero ISR a nivel táctico (portátil por personal militar)</p>
<p>Orbiter 2 (Israel)</p> <p>Rango de control (alcance): 50km Autonomía: 3h Altura máxima: Baja-Media</p> <p>Usos: ISR a nivel táctico (portátil por personal militar)</p>	<p>RQ-20 Puma (USA)</p> <p>Rango de control (alcance): 20km Autonomía: 3h Altura máxima: Baja</p> <p>Usos: ISR</p>	<p>Mavic Series (DJI – China) → Compra libre.</p> <p>Rango de control (alcance): 1-8km Autonomía: 40 min Altura máxima: Baja</p> <p>Usos: Cuadricóptero ISR a nivel táctico (portátil por personal militar)</p>
<p>Skylark (Israel)</p> <p>Rango de control (alcance): 50-60km Autonomía: 2h Altura máxima: Baja-Media</p> <p>Usos: ISR a nivel táctico (portátil por personal militar)</p>	<p>Vector (Alemania)</p> <p>Rango de control (alcance): 15km Autonomía: 2h Altura máxima: Baja</p> <p>Usos: ISR</p>	

	<p>Quantix</p> <p>Rango de control (alcance): 2km Autonomía: 45m Altura máxima: Baja</p> <p>Usos: ISR (vigila 1.6 km2 de manera autónoma)</p>		
	<p>Mini UAS (Türkiye, Bayraktar)</p> <p>Rango de control (alcance): 15km Autonomía: 1h30 Altura máxima: Baja</p>		
	<p>EVO II (China) → Dispositivo comercial.</p> <p>Rango de control (alcance): 13km Autonomía: 40 min Altura máxima: Baja-Media</p> <p>Usos: Cuadricóptero ISR a nivel táctico (portátil por personal militar)</p>		
	<p>Skydio X2 (USA) → Dispositivo comercial.</p> <p>Rango de control (alcance): 10km Autonomía: 35 min Altura máxima: Baja</p> <p>Usos: Cuadricóptero ISR a nivel táctico (portátil por personal militar)</p>		
	<p>Mavic Series (DJI – China) → Dispositivo comercial.</p> <p>Rango de control (alcance): 1-8km Autonomía: 40 min Altura máxima: Baja</p> <p>Usos: Cuadricóptero ISR a nivel táctico (portátil por personal militar)</p>		
	<p>Golden Eagle (USA) → Dispositivo comercial.</p> <p>Rango de control (alcance): 3km Autonomía: 30 min Altura máxima: Baja</p> <p>Usos: Cuadricóptero ISR a nivel táctico (portátil por personal militar)</p>		

	Rotor Riot FPV (USA) → Dispositivo comercial. Rango de control (alcance): Corto Autonomía: Baja Altura máxima: Baja Usos: ISR	
	Spartacus Hurricane Rango de control (alcance): Corto Autonomía: Baja Altura máxima: Baja Usos: ISR + Provisión de alimentos, medicamentos...	

Elaboración propia

Fuente: Jones (2022), (Vadim, 2022), (Autel Robotics, 2024), (DJI, 2024), (Skydio, 2024)

2. Vehículos autónomos de combate aéreo con capacidades ISR y ataque

Leyenda:

	Clase I OTAN
	Clase II OTAN
	Clase III OTAN
	Dispositivo Comercial

Azerbaiyán		Ucrania		Rusia	
Bayraktar TB2 (Türkiye) Rango de control (alcance): 300km Autonomía: 27h Altura máxima: Media-Alta Usos: <ul style="list-style-type: none"> - ISR. - Capacidad para llevar y lanzar munición precisa contra objetivos, incluyendo bombas guiadas, sin necesidad de autodestrucción de la nave. 		Tupolev TU-141 (URSS) Rango de control (alcance): 1000km Altura máxima: Media-Alta Usos: <ul style="list-style-type: none"> - Principalmente ISR de largo alcance. - Posibilidad de ser modificado para llevar y lanzar munición precisa contra objetivos, sin necesidad de autodestrucción de la nave. 		Orion (Rusia) Rango de control (alcance): 250km Autonomía: 24h Altura máxima: Media-Alta Usos: ISR + máximo 4 bombas guiadas para ataque directo	
Kargu (Türkiye) Rango de control (alcance): 10km Autonomía: 30min Altura máxima: Baja		Bayraktar TB2 (Türkiye) Rango de control (alcance): 300km Autonomía: 27h		Forpost-R (Rusia-Israel) Rango de control (alcance): 450km Autonomía: 20h Altura máxima: Media	

<p>Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR. - Capacidad autodestructiva de precisión en caso de ataque. 	<p>Usos:</p> <ul style="list-style-type: none"> - ISR - Capacidad para llevar y lanzar munición precisa contra objetivos, incluyendo bombas guiadas, sin necesidad de autodestrucción de la nave. 	<p>Usos: ISR + Misiles antitanque + bombas guiadas por misiles</p>
	<p>Tupolev TU-143 (URSS)</p> <p>Rango de control (alcance): 200km Altura máxima: Baja-Media</p> <p>Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR de largo alcance. - Posibilidad de ser modificado para llevar y lanzar munición precisa contra objetivos, sin necesidad de autodestrucción de la nave. 	<p>Orlan 10 (Rusia)</p> <p>Rango de control (alcance): 600km Autonomía: 18h Altura máxima: Media</p> <p>Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR de largo alcance. - Posibilidad de ser modificado para llevar y lanzar munición precisa contra objetivos, sin necesidad de autodestrucción de la nave.
	<p>UJ-22 (Ucrania)</p> <p>Rango de control (alcance): 800km Autonomía: 7h Carga de explosivos: Hasta 20kg Altura máxima: Baja</p> <p>Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR. - Capacidad para llevar y lanzar munición precisa contra objetivos, sin necesidad de autodestrucción de la nave. 	<p>Orlan 30 (Rusia)</p> <p>Rango de control (alcance): 600km Autonomía: 16h Altura máxima: Baja</p> <p>Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR. - Posibilidad de ser modificado para llevar y lanzar munición precisa contra objetivos, sin necesidad de autodestrucción de la nave.
	<p>ST-35 Silent Thunder (Ucrania)</p> <p>Rango de control (alcance): 30km Autonomía: 1h Altura máxima: Baja</p> <p>Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR. - Capacidad autodestructiva de precisión en caso de ataque. 	<p>Lastochka-M (Rusia)</p> <p>Rango de control (alcance): 45km Autonomía: 2h Altura máxima: Baja</p> <p>Usos:</p> <ul style="list-style-type: none"> - ISR - Capacidad para llevar y lanzar munición precisa contra objetivos sin necesidad de autodestrucción de la nave.

	<p>Switchblade 300</p> <p>Rango de control (alcance): 10km Autonomía: 15min Usos:</p> <ul style="list-style-type: none"> - Principalmente ISR. - Capacidad autodestructiva de precisión en caso de ataque. 		<p>Kalashnikov KYB Kub (Rusia)</p> <p>Rango de control (alcance): 40km Autonomía: 30min Carga de explosivos: Hasta 3kg</p>	
	<p>R-18 (Ucrania: Aerorozvidka)</p> <p>Rango de control (alcance): 4km Autonomía: 40min Usos:</p> <ul style="list-style-type: none"> - ISR - Capacidad para llevar y lanzar munición precisa contra objetivos (incluyendo blindados), sin necesidad de autodestrucción de la nave. 		<p>Lancet-3 (Rusia)</p> <p>Rango de control (alcance): 40km Autonomía: 40min Carga de explosivos: Hasta 3kg Altura máxima: Baja-Media</p>	
	<p>Drones comerciales con capacidad ISR modificados → Dispositivo comercial.</p> <p>Rango de control (alcance): Corto Autonomía: Baja Altura MAX: Baja Usos: ISR + modificaciones para ataques directos</p>		<p>Zastava (Rusia-Israel)</p> <p>Rango de control (alcance): 15km Autonomía: 1h20 Altura máxima: Baja Usos:</p> <ul style="list-style-type: none"> - ISR - Capacidad para llevar y lanzar munición precisa contra objetivos, sin necesidad de autodestrucción de la nave. 	
	<p>Drones comerciales con capacidad ISR modificados → Dispositivo comercial.</p> <p>Rango de control (alcance): Corto Autonomía: Baja Altura máxima: Baja Usos: ISR + modificaciones para ataques directos</p>			

Elaboración propia

Fuente: Jones (2022), (Vadim, 2022), (Autel Robotics, 2024), (DJI, 2024), (Skydio, 2024)

3. Vehículos autónomos de combate aéreo con capacidad merodeadora y/o autodestructiva

Azerbaiyán	Ucrania	Rusia
<p>Harop (Israel)</p> <p>Rango de control (alcance): 1000km Autonomía: 6h Carga explosiva: 26Kg</p> <p>Usos:</p> <ul style="list-style-type: none"> - Diseñado para ataques de precisión contra defensas antiaéreas y demás objetivos 	<p>Punisher (Ucrania)</p> <p>Rango de control (alcance): 45km Autonomía: 3h Carga de explosivos: Hasta 2kg</p> <p>Usos:</p> <ul style="list-style-type: none"> - Reutilizable. - Uso conjunto con dron que realiza la identificación y seguimiento de objetivos. - Difícil detección. 	<p>Shahed-136 (Irán)</p> <p>Rango de control (alcance): 1800km Autonomía: Desconocido.</p> <p>Usos:</p> <ul style="list-style-type: none"> - Capacidad autodestructiva. - Diseñado para buscar, seguir y atacar objetivos humanos específicos.
<p>Orbiter- 3 (Israel)</p> <p>Rango de control (alcance): 150km Autonomía: 7h</p> <p>Usos:</p> <p>Diseñado para ataques de precisión contra infraestructuras ligeras (blindaje ligero) y objetivos humanos.</p>	<p>Warmate (Polonia)</p> <p>Rango de control (alcance): 30km Autonomía: 50min</p> <p>Usos:</p> <ul style="list-style-type: none"> - Capacidad autodestructiva. - Diseñado para buscar, seguir y atacar objetivos humanos específicos. - Difícil detección. <p>Precio estimado: 12.000\$</p>	<p>Shahed-131 (Irán)</p> <p>Rango de control (alcance): 900km Autonomía: Desconocido.</p> <p>Usos:</p> <ul style="list-style-type: none"> - Capacidad autodestructiva. - Diseñado para buscar, seguir y atacar objetivos humanos específicos.
<p>Orbiter-1K (Israel)</p> <p>Rango de control (alcance): 100km Autonomía: 2h30</p> <p>Usos:</p> <ul style="list-style-type: none"> - Diseñado para ataques de precisión contra infraestructuras ligeras (blindaje ligero) y objetivos humanos. 	<p>Phoenix Ghost (EE. UU.)</p> <p>Autonomía: 6h</p> <p>Usos:</p> <ul style="list-style-type: none"> - Capacidad autodestructiva. - Diseñado para buscar, seguir y atacar objetivos humanos específicos. 	
<p>Skystriker (Israel)</p> <p>Rango de control (alcance): 100km Autonomía: 2h Carga de explosivos: 5-10kg</p> <p>Usos:</p> <ul style="list-style-type: none"> - Diseñado para ataques de precisión contra infraestructuras ligeras (blindaje ligero) y objetivos humanos. 		

Elaboración propia

Fuente: Jones (2022), (Vadim, 2022)

IX. Fuentes y referencias bibliográficas

- Al Jazeera. (2023, 25 noviembre). More than 70 Russian drones hit Kyiv, wounding five: Ukrainian officials. *Al Jazeera*.
<https://www.aljazeera.com/news/2023/11/25/more-than-70-russian-drones-hit-kyiv-wounding-five-ukrainian-officials>
- Antal, J. F. (2022). *7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting*. Casemate.
- Autel Robotics. (2024). *EVO II specification*. <https://shop.autelrobotics.com/pages/evo-ii-specification>
- Beehner, L., Collins, L., Ferenzi, S., Person, R., & Brantly, A. F. (2018). Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia. *Modern War Institute*. <https://vtechworks.lib.vt.edu/handle/10919/82532>
- Borger, J. (2022, 10 abril). The drone operators who halted Russian convoy headed for Kyiv. *The Guardian*. <https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv>
- CCN. (2021). Informe Anual 2020: Hacktivismo y Ciberyihadismo. *Centro Criptológico Nacional (CCN)*. <https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/5933-ccn-cert-ia-17-21-informe-anual-2020-hacktivismo-y-ciberyihadismo-1/file?format=html>
- Chapter Five: Russia and Eurasia. (2022). *The Military Balance*, 122(1), 164-217.
<https://doi.org/10.1080/04597222.2022.2022930>
- Chávez, K. (2023, enero). *Learning on the Fly: Drones in the Russian-Ukrainian War* / *Arms Control Association*. Arms Control Association.
<https://www.armscontrol.org/act/2023-01/features/learning-fly-drones-russian-ukrainian-war>

- Chen, S., & Feffer, J. (2009). CHINA'S MILITARY SPENDING: SOFT RISE OR HARD THREAT? *Asian Perspective*, 33(4).
<https://www.jstor.org/stable/42704692>
- Chernobrov, D. (2022). Diasporas as cyberwarriors: infopolitics, participatory warfare and the 2020 Karabakh war. *International Affairs*, 98(2), 631-651.
<https://doi.org/10.1093/ia/iia015>
- Chin, W. (2019). Technology, War and the State: Past, present and future. *International Affairs*, 95(4), 765-783. <https://doi.org/10.1093/ia/iiz106>
- Chiriac, C. (2023). *The Nagorno-Karabakh conflict – zero point of future conflicts?* Questa Soft. <https://www.cceol.com/search/article-detail?id=1213508>
- Congressional Research Service. (2023). Ukrainian Military Performance and Outlook. *Congressional Research Service*.
<https://crsreports.congress.gov/product/pdf/IF/IF12150>
- Cordesman, A. H., Burke, A. A., & Molot, M. (2019). Chinese Military Modernization. *Center For Strategic And International Studies (CSIS)*.
<http://www.jstor.com/stable/resrep22586.42>
- Danyk, Y., Малярчук, Т., & Briggs, C. M. (2017). Hybrid War: high-tech, information and cyber conflicts. *Connections: The Quarterly Journal*, 16(2), 5-24.
<https://doi.org/10.11610/connections.16.2.01>
- DeVore, M. R. (2023). “No end of a lesson:” observations from the first high-intensity drone war. *Defense & Security Analysis*, 39(2), 263-266.
<https://doi.org/10.1080/14751798.2023.2178571>
- DFRLab. (2021, 15 diciembre). Patriotic astroturfing in the Azerbaijan-Armenia Twitter war. *Medium*. <https://medium.com/dfrlab/patriotic-astroturfing-in-the-azerbaijan-armenia-twitter-war-9d234206cdd7>

- Díaz Rosaenz, I. D. R. (2021). *Operaciones militares desarrolladas en el nivel operacional durante el conflicto por Nagorno Karabaj entre septiembre y noviembre del 2020* [Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina]. <http://www.cefadigital.edu.ar/handle/1847939/2111>
- Diuk, N. (2014). EUROMAIDAN: Ukraine's Self-Organizing Revolution. *World Affairs*, 176(6), 9-16. <https://www.jstor.org/stable/43555086>
- DJI. (2024). *DJI Mavic Serie Store*. https://store.dji.com/de/shop/mavic-series?gad_source=1&gclid=CjwKCAiA29auBhBxEiwAnKcSqsMJf4YsZ-gf3ywm0IgxDPmkDEfEM68PM8POXIOiC_VKmqL-y8IjthoCigIQAvD_BwE
- Dronarium. (2024). *Dronarium Академия*. <https://dronarium.academy/en/>
- Ehrhart, H. (2017). Postmodern warfare and the blurred boundaries between war and peace. *Defense & Security Analysis*, 33(3), 263-275. <https://doi.org/10.1080/14751798.2017.1351156>
- Eslami, M. (2022). Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War. *Journal For Peace And Nuclear Disarmament*, 5(2), 507-518. <https://doi.org/10.1080/25751654.2022.2149077>
- Fabbrini, F. (2023). The War in Ukraine and the Future of the EU. *Social Science Research Network*. <https://doi.org/10.2139/ssrn.4135493>
- Fogel, B. (2022, 22 agosto). *Will the Drone War Come Home? Ukraine and the Weaponization of Commercial Drones - Modern War Institute*. Modern War Institute. <https://mwi.westpoint.edu/will-the-drone-war-come-home-ukraine-and-the-weaponization-of-commercial-drones/>
- Fox, A. C. (2017). *Hybrid Warfare: The 21st Century Russian Way of Warfare*. <https://apps.dtic.mil/sti/pdfs/AD1038987.pdf>

- Frąckiewicz, M. (2023, 19 diciembre). *The Role of Military Drones in Intelligence, Surveillance, and Reconnaissance (ISR)*. TechnoSpace2.
<https://ts2.com.pl/en/the-role-of-military-drones-in-intelligence-surveillance-and-reconnaissance-isr/>
- Frías Sánchez, C. J. F. S. (2021). El campo de batalla futuro. . . que quizá es presente. *Instituto Español de Estudios Estratégicos (IEEE)*, 1057-1078.
https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM07_2021_CARFRI_Batalla.pdf
- Fuente Cobo, I. F. C. (2022). La OTAN y el ciberespacio. *Instituto Español de Estudios Estratégicos (IEEE): Revista Ejército*, 972.
https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf
- Gazpio, A. M. (2021). *Sistemas GNSS y sensores remotos usados en el último conflicto del cáucaso sur Nagorno Karabaj*.
<http://www.cefadigital.edu.ar/handle/1847939/2274>
- Geers, K. (2015). *Cyber War in Perspective: Russian Aggression Against Ukraine* (CDDCOE).
https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf
- Gerasimov, V. (2019). Russian General Staff Chief Valery Gerasimov's 2018 presentation to the General Staff Academy (H. Orenstein, Trad.). *MILITARY REVIEW*. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-19/Gerasimov-III-print-2.pdf>
- Grossman, T. G., Kaminska, M. K., Shires, J. S., & Smeets, M. S. (2023). The Cyber Dimensions of the Russia-Ukraine War. *European Cyber Conflict Research Initiative (ECCRI)*. <https://eccri.eu/wp->

content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf

- Herzog, S. (2011). Revisiting the Estonian Cyber attacks: digital threats and multinational responses. *Journal Of Strategic Security*, 4(2), 49-60.
<https://doi.org/10.5038/1944-0472.4.2.3>
- Ilić, D., & Tomašević, V. (2021). The impact of the Nagorno-Karabakh conflict in 2020 on the perception of combat drones. *Serbian Journal Of Engineering Management*, 6(1), 9-21. <https://doi.org/10.5937/sjem2101009i>
- Ivanchenko, O., Kurdiuk, S., Khatuntsev, Y., & Rudnichenko, S. (2023). ANALYSIS OF APPLICATION POSSIBILITIES AND CLASSIFICATION OF UNMANNED AERIAL VEHICLES FOR THE SUPPORT OF COMBAT OPERATIONS OF THE NAVY OF THE ARMED FORCES OF UKRAINE. *Zbìrnik Naukovih Prac' Deržavnogo Naukovo-doslidnogo Ìnstitutu Viprobuvan' Ì Sertifikacìi Ozbroènnâ Ta Vìjs'kovoì Tehniki*, 18(4), 23-34.
<https://doi.org/10.37701/dndivsovt.18.2023.04>
- Jones, S. G. (2022). *COMBINED ARMS WARFARE AND UNMANNED AIRCRAFT SYSTEMS: a NEW ERA OF STRATEGIC COMPETITION*. Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221110_Jones_CombinedArms_UASs.pdf?VersionId=2xC7tI7AtaEEaNOG0AEKAOdjDsvYwHMn
- Karagiannis, E. (2012). The 2008 Russian–Georgian war via the lens of Offensive Realism. *European Security*, 22(1), 74-93.
<https://doi.org/10.1080/09662839.2012.698265>

- Karber, P. A. (2015). Lessons learned” from the Russo-Ukrainian War. *The Potomac Foundation*. <https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf>
- Kardashian, K. N. K. (2020, 27 septiembre). *Kim Kardashian en X*: «Call upon Baku to cease all offensive uses of force, cut off all US military aid to #Azerbaijan being used against Armenians & warn #Turkey to stop sending arms & fighters to Baku 🙏AM👉» / X. X (Previamente Twitter).
<https://twitter.com/KimKardashian/status/1310278059266904069>
- Kartomo, A., Legionosuko, T., & Risman, H. (2022). *Analysis of The Russia-Ukraine War Based on Giulio Douhet’s Airpower Theory and as The Best Practice For Indonesia’s Air Force*. <https://www.semanticscholar.org/paper/Analysis-of-The-Russia-Ukraine-War-Based-on-Giulio-Kartomo-Legionosuko/cffa804e98b2d0e1b2f88b22caadcea645c616f4>
- Katalinić, J. (2023). Analysis of Pro-Russian Tweets during Russian Invasion of Ukraine. *University Of Zagreb (Croatia)*.
<https://doi.org/10.23919/mipro57284.2023.10159929>
- Katsuya, T. (2021). The Gulf War as a Harbinger of a Revolution in Military Affairs (RMA). *National Institute For Defense Studies (NIDS)*, 41-49.
https://www.nids.mod.go.jp/event/proceedings/forum/pdf/2021/EN_06_tsukamoto.pdf
- Konaev, M. (2023, 4 octubre). *U) Tomorrow’s Technology in Today’s War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability*. Policy Commons.
<https://policycommons.net/artifacts/4867028/u-tomorrows-technology-in-todays-war/5704260/>

- Kosal, M. E. (2019). *Disruptive and game changing technologies in modern warfare: Development, Use, and Proliferation*. Springer Nature.
- Kostyuk, N., & Zhukov, Y. M. (2017). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal Of Conflict Resolution*, 63(2), 317-347.
<https://doi.org/10.1177/0022002717737138>
- Kowrach, J. M. (2018). US Army Counter-Unmanned Aerial Systems: More Doctrine Needed. *School Of Advanced Military Studies US Army Command And General Staff College Fort Leavenworth, KS*.
<https://apps.dtic.mil/sti/pdfs/AD1071111.pdf>
- Krepinevich, A. F. (1994). Cavalry to Computer: The Pattern of Military Revolutions. *The National Interest*, 37. <https://www.jstor.org/stable/42896863>
- Krepinevich, A. F. (2008). Cavalry to computer: The pattern of Military Revolutions. *En Routledge eBooks* (pp. 374-386). <https://doi.org/10.4324/9780203928462-30>
- Kreps, S. E., & Lushenko, P. (2023). Drones in modern war: evolutionary, revolutionary, or both? *Defense & Security Analysis*, 39(2), 271-274.
<https://doi.org/10.1080/14751798.2023.2178599>
- Kumar, A. (2023). An analytical study of Russia-Ukraine war in reference to the offensive realist approach in international relations. *World Journal Of Advanced Research And Reviews*, 18(3), 926-933.
<https://doi.org/10.30574/wjarr.2023.18.3.0906>
- Kunertova, D. (2023a). The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin Of The Atomic Scientists*, 79(2), 95-102.
<https://doi.org/10.1080/00963402.2023.2178180>

- Kunertova, D. (2023b). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, 44(4), 576-591.
<https://doi.org/10.1080/13523260.2023.2262792>
- Lobell, S. E. (2002). War is politics: Offensive realism, domestic politics, and security strategies. *Security Studies*, 12(2), 165-195.
<https://doi.org/10.1080/09636410212120012>
- Lowther, A., & Siddiki, M. K. (2022). Combat drones in Ukraine. *Air & Space Operations Review (ASOR)*, 1(4).
https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-4/Lowther.pdf
- Magen, Z., Baruch, P. S., & Bagno-Moldavsky, O. (2014). *The Annexation of Crimea: International Ramifications*. <https://www.jstor.org/stable/resrep08214>
- Mammadov, A. (2022). Azerbaijan's foreign policy analysis in the perspective of Neorealist Theory: In the example of the Karabakh problem. *Journal Of Eastern European And Central Asian Research*, 9(3), 513-520.
<https://doi.org/10.15549/jeecar.v9i3.864>
- Miller, C. (2022). *Chip war: The Fight for the World's Most Critical Technology*. Simon and Schuster.
- Mladenovic, D., & Radunovic, V. (2018). Defining offensive cyber capabilities. *ResearchGate*. <https://www.researchgate.net/publication/326265622>
- Modebadze, V. (2021). THE ESCALATION OF CONFLICT BETWEEN ARMENIANS AND AZERBAIJANIS AND THE PROBLEMS OF PEACEFUL RESOLUTION OF THE NAGORNO-KARABAKH WAR. *Journal Of Liberty And International Affairs*, 6(3), 102-110.
<https://doi.org/10.47305/jlia2163102m>

- Noorman, R. (2023, 27 junio). *The Russian Way of War in Ukraine: A Military Approach Nine Decades in the Making - Modern War Institute*. Modern War Institute. <https://mwi.westpoint.edu/the-russian-way-of-war-in-ukraine-a-military-approach-nine-decades-in-the-making/>
- Olivie, I., & Gracia, M. (2022). Informe Elcano de Presencia Global 2022. *Real Instituto Elcano*. [https://www.realinstitutoelcano.org/informes/informe-elcano-de-presencia-global-2022/#:~:text=La%20UE%20registra%20un%20valor,al%20de%20China%20\(1.365\)](https://www.realinstitutoelcano.org/informes/informe-elcano-de-presencia-global-2022/#:~:text=La%20UE%20registra%20un%20valor,al%20de%20China%20(1.365)).
- Onetto, R. K. (2021, 12 enero). *IMPACTO DE LOS DRONES Y REDES SOCIALES EN UN NUEVO CARÁCTER DE LA GUERRA*. <https://revistaensayosmilitares.cl/index.php/acague/article/view/254>
- Oprean, L. (2023, 15 junio). *Artillery and Drone Action Issues in the War in Ukraine*. Sciendo. <https://sciendo.com/article/10.2478/bsaft-2023-0008>
- Oryx. (2022, febrero). *Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine*. Oryx. <https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html>
- Oryx. (2023). *The Fight for Nagorno-Karabakh: documenting losses on the sides of Armenia and Azerbaijan*. Oryx. <https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html>
- Pérez Arriue, J. C. P. A., & Allende, W. A. (2021). *El conflicto de Nagorno Karabaj 2020 Munición merodeadora y sistemas de armas de artillería y morteros : lecciones para el futuro de la guerra*. <http://www.cefadigital.edu.ar/handle/1847939/2273>

- Plokšto, A., & Demeško, A. (2017). Armaments used in the Ukrainian conflict 2014–2015. *Security And Defence Quarterly*, 15(2), 54-84.
<https://doi.org/10.35467/sdq/103190>
- Popescu, A. I. C. (2021). *REMARKS ON THE FIFTH-GENERATION WARFARE AND THE SECOND NAGORNO-KARABAKH WAR*. Questa Soft.
<https://www.ceeol.com/search/article-detail?id=1007763>
- Przetacznik, J. P., & Tarpova, S. T. (2022, junio). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliamentary Research Service.
[https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2022\)733549](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549)
- Przetacznik, J., & Tothova, L. (2022). Russia's war on Ukraine: Military balance of power. *European Parliamentary Research Service*.
[https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729292/EPRS_ATAG\(2022\)729292_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729292/EPRS_ATAG(2022)729292_EN.pdf)
- Reichborn-Kjennerud, E., & Cullen, P. (2016). What is Hybrid Warfare? *Norwegian Institute For International Affairs (NUPI)*. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf
- Rostomyan, M. (2023). From Mountains to Social Media Valleys: A Thematic Analysis of Information Warfare through Telegram Data in the Nagorno-Karabakh War. *Journal Of Intelligence, Conflict And Warfare*, 6(2), 1-25.
<https://doi.org/10.21810/jicw.v6i2.6178>
- Russell, A. L. (2014). *Cyber blockades*. Georgetown University Press.

- Seskuria, N. (2022). *Russia's "Hybrid Aggression" against Georgia: The Use of Local and External Tools*. <https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools>
- Setien, S. A. (2020). Conflicto de Nagorno Karabaj 2020: ¿nos encontramos ante la solución definitiva? *Bie3: Boletín IEEE*, 20, 687-706.
<https://dialnet.unirioja.es/descarga/articulo/7772846.pdf>
- Shen, F., Zhang, E., Zhang, H., Ren, W., Jia, Q., & He, Y. (2023). Examining the differences between human and bot social media accounts: A case study of the Russia-Ukraine War. *First Monday*. <https://doi.org/10.5210/fm.v28i2.12777>
- Singer, P. (2002). Corporate Warriors: The rise of the privatized military industry and its ramifications for international security. *International Security*, 26(3), 186-220. <https://doi.org/10.1162/016228801753399763>
- Skoglund, P., Listou, T., & Ekström, T. (2022a). Russian Logistics in the Ukrainian War: Can Operational Failures be Attributed to logistics? *Scandinavian Journal Of Military Studies*, 5(1), 99-110. <https://doi.org/10.31374/sjms.158>
- Skoglund, P., Listou, T., & Ekström, T. (2022b). Russian Logistics in the Ukrainian War: Can Operational Failures be Attributed to logistics? *Scandinavian Journal Of Military Studies*, 5(1), 99-110. <https://doi.org/10.31374/sjms.158>
- Skydio. (2024). *Skydio X2*. <https://www.skydio.com/skydio-x2>
- Stone, J. (2013). Cyber War Will Take Place! *Journal Of Strategic Studies*, 36(1), 101-108. <https://doi.org/10.1080/01402390.2012.730485>
- Swed, O., & Chávez, K. (2023). Emulating underdogs: Tactical drones in the Russia-Ukraine war. *Contemporary Security Policy*, 44(4), 592-605.
<https://doi.org/10.1080/13523260.2023.2257964>

- Thomas, E., & Zhang, A. (2020). *Snapshot of a shadow war: a preliminary analysis of Twitter activity linked to the Azerbaijan–Armenia conflict*.
<https://www.jstor.org/stable/resrep26984>
- Umarach, M. S., & Muhammad, A. (2023). Azerbaijan’s Strategy to Win the Conflict over the Nagorno-Karabakh Territory with Armenia in 2020. *Journal Of Islamic World And Politics*, 7(1), 119-128. <https://doi.org/10.18196/jiwp.v7i1.49>
- Vadim, K. (2022, 19 octobre). Magyla UAV helped Ukranian Armed Forces to destroy Russians convoy. *Militarnyi*. <https://mil.in.ua/en/news/magyla-uav-helped-ukranian-armed-forces-to-destroy-russians-convoy/>
- Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, 64(5), 7-26. <https://doi.org/10.1080/00396338.2022.2126193>
- Zelinska, O. (2017). Ukrainian Euromaidan protest: Dynamics, causes, and aftermath. *Sociology Compass*, 11(9). <https://doi.org/10.1111/soc4.12502>
- Zia, H. B., Haq, E. U., Castro, I., Hui, P., & Tyson, G. (2023). An Analysis of Twitter Discourse on the War Between Russia and Ukraine. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.2306.11390>