Revista del Instituto Español de Estudios Estratégicos
ISSN-e: 2255-3479

Tania Vidal López
Doctora en Derecho, Ciencia Política y Criminología por la Universitat de València

Correo: taniavidallopezphd@gmail.com

Tecnología y conflicto armado: la transformación de la guerra en el siglo XXI

Technology and armed conflict: the transformation of war in the 21st century

Resumen

En las últimas décadas, la guerra ha experimentado una profunda transformación impulsada por la digitalización y el acelerado desarrollo tecnológico. Estos avances no solo han modificado las capacidades operativas de los Estados, sino que también han alterado las dinámicas globales de seguridad y defensa. La tecnología ha redefinido los escenarios bélicos, dando lugar a conflictos que trascienden los medios convencionales y exigen una reconfiguración de las estrategias tácticas y operativas militares. En este contexto, surge el concepto de guerra híbrida, caracterizado por la combinación de tácticas tradicionales y no convencionales, incluyendo operaciones cibernéticas, desinformación y ataques a infraestructuras críticas. Este nuevo paradigma busca explotar vulnerabilidades sistémicas y desestabilizar a los Estados sin recurrir necesariamente al enfrentamiento directo. Como consecuencia, la ciberseguridad y la ciberdefensa se han convertido en pilares esenciales de las políticas de defensa contemporáneas. Instituciones internacionales, como la Unión Europea, han reconocido la urgencia de fortalecer su resiliencia ante estas amenazas emergentes, desarrollando estrategias

integrales que integren la tecnología, la inteligencia y la cooperación internacional para proteger la estabilidad y la seguridad global. En suma, la era digital ha redefinido la naturaleza misma de la guerra y de la seguridad internacional.

Palabras clave

Amenazas híbridas, Defensa, Estrategia de Seguridad Nacional, Unión Europea, Zona gris.

Abstract

In recent decades, warfare has undergone a profound transformation driven by digitalisation and rapid technological development. These advances have not only altered the operational capabilities of states, but have also changed the global dynamics of security and defence. Technology has redefined the theatre of war, giving rise to conflicts that transcend conventional means and demand a reconfiguration of military tactical and operational strategies. In this context, the concept of hybrid warfare has emerged, characterised by the combination of traditional and unconventional tactics, including cyber operations, disinformation and attacks on critical infrastructure. This new paradigm seeks to exploit systemic vulnerabilities and destabilise states without necessarily resorting to direct confrontation. As a result, cybersecurity and cyber defence have become essential pillars of contemporary defence policies. International institutions, such as the European Union, have recognised the urgency of strengthening their resilience in the face of these emerging threats, developing comprehensive strategies that integrate technology, intelligence and international cooperation to protect global stability and security. In short, the digital age has redefined the very nature of warfare and international security.

Keywords

Hybrid threats, Defence, National Security Strategy, European Union, Grey zone.

Citar este artículo:

Vidal López, T. (2026). Tecnología y conflicto armado: La transformación de la guerra en el siglo XXI. *Revista del Instituto Español de Estudios Estratégicos*. 27, pp. 69-88.

1 Introducción

En las últimas décadas, hemos sido testigos de una profunda transformación en la forma de concebir y ejercer la guerra, impulsada principalmente por la digitalización y el acelerado avance y desarrollo tecnológico. Esta evolución no ha modificado exclusivamente las capacidades operativas de los países, sino que ha conllevado a un cambio significativo de las dinámicas globales de seguridad y defensa.

En el contexto internacional, cada vez más multipolar y competitivo, han surgido nuevos actores, tanto estatales como no estatales, que emplean novedosos e innovadores mecanismos y herramientas no convencionales capaces de perturbar el *statu quo* y desestabilizar los cimientos de las sociedades modernas. Este fenómeno, sin duda, tiene un impacto directo en el ámbito de la defensa y la seguridad que conlleva a una reconfiguración de las estrategias tácticas y operativas militares, generando nuevas formas de conflicto que transcienden de los medios convencionales.

Una de las manifestaciones más evidentes de este avance y transformación en la forma de hacer guerra es la aparición de un nuevo escenario en estos conflictos, hablamos del ciberespacio. Lejos de limitarse a los escenarios de batalla tradicionales, los enfrentamientos actuales se trasladan también al ámbito digital con el ciberespacio y el empleo de las tecnologías emergentes. Por tanto, el ámbito cibernético se convierte en una pieza clave del conflicto bélico que tiene la capacidad de desestabilizar, influir o menoscabar las infraestructuras críticas o sistemas de información de un país, como estamos observando en la guerra de agresión de Rusia contra Ucrania. Esta realidad ha dado lugar a la modernización del conflicto y la transformación de la estrategia y organización de defensa de un país, caracterizada no solo por las tácticas militares convencionales, sino también por la inclusión de mecanismos y herramientas digitales.

Este nuevo paradigma de los conflictos bélicos se enmarca en el concepto de *guerra híbrida* (GH), que combina numeras técnicas y métodos con el fin de atentar contra las posibles vulnerabilidades sistemáticas de un país. En esta nueva forma de hacer guerra se halla el escenario del ciberespacio, que ha cobrado un gran protagonismo en los últimos años, cuya identificación y atribución de acciones resulta especialmente complicado. En este escenario se combinan las estrategias militares tradicionales con los nuevos mecanismos tecnológicos, dando lugar a la modernización del conflicto y la conocida GH, y, en consecuencia, ha convertido en un problema estratégico central la capacidad real de respuesta de las instituciones internacionales, en particular de la Unión Europea (UE) y la Organización del Tratado del Atlántico Norte (OTAN), frente a amenazas híbridas que combinan acción militar, presión informativa y ciberataques

Por ello, en este artículo se parte de una pregunta de investigación concreta: ¿en qué medida la guerra de Ucrania ha modificado la comprensión y el diseño de la defensa europea frente a amenazas híbridas y ciberataques? A partir de esta cuestión, se sostiene que el conflicto ha revelado tanto el valor estratégico de la tecnología como los límites de las respuestas institucionales de la UE y la OTAN. El interés del caso ucraniano no reside únicamente en su dimensión militar, sino en su capacidad para

mostrar cómo la combinación de ciberataques, desinformación, guerra electrónica e innovación tecnológica altera la lógica tradicional del conflicto y obliga a repensar los marcos de defensa.

2 Metodología

Este trabajo adopta un enfoque de análisis documental cualitativo basado en fuentes institucionales, estratégicas y académicas. El corpus analizado incluye estrategias de seguridad y ciberseguridad de la UE, documentos estratégicos de la OTAN, informes especializados y bibliografía reciente sobre GH, desinformación, innovación militar y conflicto ruso-ucraniano.

En esta línea, el estudio se estructura como un caso ilustrativo centrado en Ucrania, utilizado para extraer implicaciones más amplias sobre la transformación contemporánea de la guerra y sobre la adaptación de la defensa europea. Con este fin, el análisis se organiza en cuatro dimensiones principales: el ciberespacio, la desinformación, la innovación tecnológica y la respuesta institucional. Este enfoque permite comparar el discurso estratégico de la UE y la OTAN con la evidencia empírica del conflicto y detectar brechas entre ambición normativa y capacidad operativa.

La selección de documentos se ha realizado atendiendo a su relevancia estratégica, actualidad y relación directa con el objeto de estudio.

3 La defensa en el ciberespacio

Es importante señalar que, en España, tanto la Estrategia Nacional de Seguridad de 2018, como la Estrategia Nacional de Ciberseguridad de 2019, han alertado sobre el auge de las denominadas amenazas híbridas. Con base en estos documentos, las amenazas híbridas deben entenderse como aquellas acciones deliberadas que persiguen atentar contra las vulnerabilidades sistemáticas de un Estado democrático y sus instituciones, mediante el empleo de una variedad de métodos, entre los que se incluyen operaciones militares convencionales, campañas de desinformación o ciberataques.

La UE ha impulsado diversas medidas e iniciativas para tratar de fortalecer sus capacidades frente a las ciberamenazas; sin embargo, la cuestión decisiva no es solo la existencia de estos instrumentos, sino su grado real de coordinación, implementación y eficacia operativa frente a ataques complejos y persistentes.

Entre ellas, cabe destacar la propuesta de un marco común de certificación en ciberseguridad, la modernización de la Agencia de Ciberseguridad de esta institución (ENISA), así como la promoción de la cooperación entre los Estados miembros (EEMM) y las agencias de la UE en caso de ciberataques. En este contexto, también encontramos el desarrollo de una plataforma específica de formación y educación con el fin principal de potenciar la colaboración de los esfuerzos conjuntos en materia de ciberdefensa.

De hecho, en 2020, la Comisión Europea, junto con el Servicio Europeo de Acción exterior (SEAE), revelaron una nueva Estrategia de Ciberseguridad para la UE. El propósito principal de esta nueva estrategia consiste en fortalecer la resiliencia de Europa frente a las crecientes ciberamenazas. La propuesta incluye propuestas específicas, las cuales se orientan a la implementación de medidas de carácter normativo, operativo y de inversión.

Posteriormente, en el año 2021, el Consejo de la UE adoptó unas conclusiones sobre esta estrategia de ciberseguridad, donde se acentuaba que la ciberseguridad es un elemento esencial e imprescindible para garantizar una Europa resiliente, digital y sostenible. En este marco, los ministros de la UE establecieron como prioridad alcanzar una autonomía estratégica sin comprometer otros aspectos como la economía, con los que ser capaces de reforzar el liderazgo digital y en consiguiente, aumentar su capacidad estratégica en materia de ciberseguridad.

Con todo ello, observamos que el desarrollo de la resiliencia frente a las actuaciones en el ciberespacio que son hostiles depende en gran medida de la coordinación entre los actores, en este caso, entre los EEMM y el resto de las organizaciones internacionales, en particular cabe resaltar la cooperación con la OTAN.

En este contexto, la OTAN, ya en el año 2015 expuso una estrategia con el fin de combatir las amenazas híbridas, orientando los esfuerzos hacia una adaptación tanto política como militar. Iniciativas que trataron y valoraron favorablemente acabando en diversos acuerdos tras celebrar la Cumbre de Varsovia del año 2016, considerando la GH como una amenaza real contra la que hay que reforzar los mecanismos de disuasión, fomentando la preparación y la defensa (Gutiérrez, 2021). Por tanto, podemos afirmar que fue la OTAN quien comenzó a asentar los pilares básicos para contrarrestar las acciones hostiles llevadas a cabo en el ciberespacio que tienen un gran potencial para dañar y menoscabar la integridad de un Estado.

En la cumbre realizada en Madrid en el año 2022, volvió a tratarse la temática de las amenazas híbridas, motivada por la guerra de agresión rusa hacia Ucrania donde se observa el potencial estratégico de las amenazas híbridas incluso en un contexto de conflicto bélico, con la consiguiente amenaza rusa para la estabilidad euroatlántica.

En suma, ante este contexto inestable, la UE y la OTAN trazan rumbo hacia la autonomía estratégica guiados por dos documentos esenciales, en primer lugar, la *Brújula Estratégica,* que se trata de un plan de acción a 2030, y, en segundo lugar, el *Nuevo Concepto Estratégico de la Alianza Atlántica*. Ambos instrumentos recogen los desafíos actuales y apuestan por una defensa común más sólida y coordinada.

En este punto, aparece una de las principales tensiones del marco europeo: el avance normativo no siempre se traduce en una capacidad de respuesta homogénea entre EEMM.

4 La estrategia de la zona gris

Los conflictos en el marco de la *zona gris* (ZG), representan una de las formas más características de la confrontación contemporánea, precisamente porque

permiten alcanzar objetivos estratégicos sin necesidad de desencadenar una guerra abierta (Gutiérrez, 2021). Esta realidad conlleva numerosas implicaciones para la planificación y la ejecución de las operaciones militares en todos los niveles del conflicto. Su valor analítico reside en que explica bien la ambigüedad, la gradualidad y la dificultad de atribución que caracterizan muchas de las operaciones híbridas actuales.

La primera aproximación a este concepto, de forma consensuada, se plantea *a sensu contrario*, esto es, como el empleo de actitudes e instrumentos que no son *blancos*, como la paz, ni *negros*, como la guerra abierta, ya sea híbrida o convencional. En otras palabras, se trata de un escenario intermedio al que se denomina *gris*, pudiéndose considerar como una variante *sui generis* de la GH (Baqués, 2017).

Por tanto, hablamos de ZG cuando el escenario de las actividades hostiles no conlleva una confrontación armada directa, sino el empleo de mecanismos con potencial lesivo suficiente para desestabilizar un país, como las tácticas de desinformación, el empleo de amenazas híbridas o ciberataques. Estas acciones sin violencia física son cada vez más frecuentes, aunque no se puede descartar que finalmente estas operaciones hostiles y su desarrollo en el tiempo escalen hacia un enfrentamiento armado.

Las estrategias de la ZG se llevan a cabo con el objetivo de alcanzar un propósito similar que cuando se inicia un conflicto armado, en suma, esta estrategia se apoya en la evolución tecnológica que actúa de multiplicador, empero, sin sobrepasar el umbral que justificaría una respuesta militar tradicional. La eficacia de estas tácticas, por tanto, radicaría en la capacidad lesiva junto con la difícil detección, atribución y respuesta oportuna.

De hecho, la *Multinational Capability Development Campaign* (MCDC), afirma que los actores que emplean estas estrategias lo hacen de forma sincronizada con diversos instrumentos de poder, los cuales se encuentran dimensionados con la finalidad de explorar las vulnerabilidades específicas del país objetivo del ataque.

La finalidad de las acciones de la ZG es llevar a cabo iniciativas destinadas a ejecutarse sin que puedan ser detectadas, pasando inadvertidas o sin que justifiquen una reacción militar por su bajo perfil, pero que, sin embargo, tengan un potencial de causar efectos reales de forma significativa. De hecho, en ocasiones, aún identificado el ataque, es difícil atribuir su responsabilidad.

En todo caso, cuando algún actor opta por el empleo de la estrategia de la ZG, es conocedor de que los resultados no van a obtenerse de forma inmediata, sino que se trata de una meta a largo plazo, donde puede aludirse al concepto de *strategic gradualism*, sirviendo incluso como preparador de la guerra abierta (Baqués, 2017).

Por todo ello, resulta evidente que entre los principales desafíos de la defensa en la ZG se encuentran la falta de claridad sobre la naturaleza del conflicto, la dificultad de identificar con precisión las partes implicadas, así como la incertidumbre de la aplicación de políticas públicas o marco legal aplicables (Silva, 2022). Así pues, para esta estrategia resulta fundamental el papel del entorno cognitivo, ya que la percepción social e internacional pueden influir, y, por consiguiente, resulta necesario controlar la

información para obtener la superioridad en este ámbito (Gutiérrez, 2021). De ello se deriva que para hacer frente a estas amenazas en el entorno de la ZG es esencial contar con un planeamiento centralizado y coordinado, además de contar con estructuras resilientes y una visión estratégica de las Fuerzas Armadas que permita detectar y responder ante este tipo de ataques de una forma temprana y eficaz.

No obstante, el concepto de ZG presenta también límites explicativos cuando se aplica a conflictos de alta intensidad, donde las operaciones híbridas conviven con ataques convencionales de gran escala.

5 El nuevo paradigma bélico

El vertiginoso avance de las tecnologías, en convergencia con un mundo cada vez más digitalizado, ha generado profundas transformaciones en todos los ámbitos de la sociedad, así como en el ámbito de la defensa y seguridad (Rodríguez, *et al.*, 2023). Esta evolución tecnológica como factor transformador ha supuesto la inclusión de nuevas herramientas digitales como los sistemas autónomos, la inteligencia artificial (IA), el análisis predictivo o la ciberseguridad, entre otras, que afectan directamente al ámbito de la seguridad y defensa, redefiniendo no solo las amenazas existentes, sino también las estrategias y capacidades necesarias para enfrentarlas.

En este contexto, estas tecnologías emergentes han pasado a ocupar un papel central en la configuración de las capacidades estratégicas de los Estados, así como en la forma de hacer guerra, ejemplo de ello es el empleo de ciberataques, drones armados, o la propia IA aplicada al análisis de inteligencia y operaciones militares, que ilustran cómo los conflictos contemporáneos se libran en escenarios cada vez más complejos y digitalizados, generando un cambio de paradigma en el que la superioridad tecnológica puede ser un elemento decisivo en el escenario de la batalla.

Esto es, el avance tecnológico no transforma únicamente las herramientas disponibles para garantizar la seguridad y defensa de un Estado, sino que, en paralelo, conlleva además la necesidad de repensar los marcos organizativos y normativos para tener capacidades óptimas para gestionar estos nuevos entornos, requiriendo un claro enfoque multidisciplinar.

Este acelerado progreso de las tecnologías ha modificado de forma sustancial la concepción de los conflictos armados, dando lugar al concepto de GH, un término ampliamente adoptado por la comunidad internacional de defensa (Franco, 2023), para representar una situación de confrontación que combina elementos de la guerra convencional con las nuevas herramientas del entorno cibernético. Esto es, permite comprender cómo la tecnología amplía y diversifica los instrumentos de coerción disponibles para los actores estatales y no estatales.

A diferencia de los conflictos armados tradicionales, que se desarrollan principalmente en un terreno físico mediante operaciones militares directas, la GH integra múltiples dimensiones, incluyendo la militar, política, informativa y cibernética. De esta forma, en combinación con las acciones tradicionales se despliegan

tácticas como los ciberataques o la desinformación, con el fin de desestabilizar al adversario sin necesidad de recurrir en exclusiva al uso explícito de la fuerza.

Por ello, el empleo de estas nuevas tecnologías conlleva a un cambio paradigmático de la naturaleza de la guerra, donde se diluyen las fronteras físicas. La GH suele desarrollarse en un escenario complejo con actores que emplean técnicas más sofisticadas, donde podemos hallarnos ante acciones de difícil atribución de responsabilidades, y, por consiguiente, donde las respuestas legales y estratégicas más tradicionales resultan en muchos casos, insuficientes.

Esto implica que la guerra contemporánea ya no puede analizarse únicamente desde la perspectiva del enfrentamiento cinético, sino también desde la capacidad de influir en sistemas de información, redes digitales, percepción pública y resiliencia institucional.

En consecuencia, esta transformación plantea retos significativos para el derecho internacional humanitario, así como para el derecho internacional público en general. Ejemplo de ello es el caso de la guerra de agresión rusa contra Ucrania, que representa un caso paradigmático para reflexionar sobre el papel clave que desempeñan las tecnologías en la configuración y desarrollo de la guerra contemporánea.

Por lo tanto, el caso ucraniano no solo ilustra la transformación tecnológica de la guerra, sino también la necesidad de repensar los marcos doctrinales, jurídicos y estratégicos con los que se interpreta el conflicto armado.

Más allá de la dimensión geopolítica y humanitaria del enfrentamiento, el territorio ucraniano se ha transformado en un verdadero escenario de operaciones donde se ensayan y perfeccionan las nuevas formas de guerra basadas en el uso principal, e incluso central, de las herramientas y mecanismos digitales que proporcionan las tecnológicas emergentes.

Dicho conflicto ha evidenciado cómo las nuevas tecnologías se han integrado en la estrategia militar junto con las tradicionales estrategias, adquiriendo una relevancia notable, desde ataques a infraestructuras críticas, a la difusión de campañas de desinformación y manipulación de la opinión pública a nivel global.

Esta realidad convierte a Ucrania no únicamente en un espacio de confrontación armada, sino también en un laboratorio tecnológico de innovación en seguridad y defensa donde diversos actores, estatales y no estatales, ponen a prueba las tecnologías emergentes en el contexto real de la guerra. Esta situación deriva en múltiples interrogantes fundamentales sobre la ética y el uso de las tecnologías, así como su regulación y consecuencias a largo plazo en su aplicación a este tipo de escenarios de alta hostilidad y, especialmente, de cara a conflictos futuros.

En suma, cabe subrayar que, en este contexto, como es el caso de Ucrania, se ilustra con claridad cómo la guerra del siglo xxi ha dejado de ser un fenómeno exclusivamente desarrollado en un terreno físico, para convertirse en un complejo escenario multidimensional, donde la supremacía de la tecnología puede ser indicador de resistencia efectiva ante el conflicto.

6 La innovación en defensa: reflejo de la guerra de agresión rusa contra Ucrania

La transformación digital que atraviesa el mundo contemporáneo, como hemos visto, ha impactado directamente en el ámbito de la seguridad y la defensa, modificando las formas tradicionales de concebir, planificar y ejecutar los conflictos armados.

En este nuevo escenario, la guerra ya no se limita territorialmente en el plano físico, sino que se expande al terreno del ciberespacio, la información y el dominio tecnológico. Y el conflicto entre Rusia y Ucrania, como expresión concreta de este cambio, permite observar con claridad cómo la tecnología se ha posicionado como elemento clave en el desarrollo del conflicto bélico entre estos países.

Este enfrentamiento refleja cómo los conflictos armados son capaces de combinar de forma efectiva el armamento tradicional con las tecnologías emergentes de carácter disruptivo. Ambos países han recurrido a medios convencionales, como vehículos blindados o artillería pesada, al mismo tiempo que han integrado innovadoras tecnologías, como los vehículos no tripulados, sistemas de IA, ciberataques coordinados y herramientas de vigilancia digital avanzada. Esta fusión de tácticas manifiesta con claridad el carácter híbrido de los conflictos actuales y evidencia la transformación de la estrategia militar a nivel global.

En esta línea, las declaraciones realizadas al principio del conflicto por Mykhailo Fedorov, viceprimer ministro y ministro de transformación digital de Ucrania, a través de sus redes sociales, muestran una visión en la que destaca el papel crucial de las nuevas tecnologías. En esas declaraciones afirmaba que la futura victoria del país dependería no solo de la valentía de la población, sino del empleo estratégico de las nuevas tecnologías. Estas manifestaciones no son únicamente un mensaje político, sino una declaración de principios sobre el papel que los avances tecnológicos juegan en la guerra moderna, donde la superioridad ya no depende solo del volumen de tropas o del armamento convencional, sino de la capacidad para integrar información, tecnología y mando en condiciones de alta incertidumbre.

Ucrania ha logrado ejecutar significativamente tanto sus capacidades defensivas como ofensivas a través del empleo e incorporación de las tecnologías en el campo de batalla, lo que convierte su experiencia en un caso relevante de estudio, especialmente para Europa, pues este conflicto ha puesto de manifiesto el papel fundamental que desempeñan las tecnologías y la innovación en el ámbito de la defensa, al demostrar una rápida adaptación al nuevo panorama de la GH. Esta transformación profunda de la forma de hacer guerra ha cambiado por tanto la estructura y operatividad de los Ejércitos. En este contexto, la experiencia del conflicto de los ucranianos ofrece unas valiosas lecciones sobre cómo poder optimizar la capacidad de respuesta, incluyendo recursos y medios mediante la integración de las tecnologías emergentes, como son los drones, la IA, la guerra electrónica, etc., en un conflicto de alta intensidad. Esto resulta clave para profundizar en la seguridad nacional y redefinir la estrategia colectiva de defensa en el ámbito europeo.

De hecho, Ucrania ha demostrado una notable capacidad de adaptación tecnológica en el transcurso del conflicto, apoyándose, además, en colaboración directa con destacadas empresas occidentales de alta tecnología, como Palantir, Clearview AI, Delta o GIS ARTA, entre otros. Sin lugar a duda, estas colaboraciones público-privadas han facilitado el empleo de soluciones avanzadas basadas en las tecnologías, las cuales han sido clave en determinados momentos desde una perspectiva de inteligencia militar, contribuyendo de forma efectiva a la estrategia táctica y operativa del campo de batalla. Este ecosistema tecnológico ha dotado a Ucrania de una ventaja adaptativa significativa basada en la capacidad de respuesta rápida.

Por ejemplo, Palantir es un *software* que permite conseguir la superioridad de la información, esto es, ha permitido a las fuerzas ucranianas obtener un análisis de datos en tiempo real que ha facilitado una mejora destacada en la toma de decisiones, al servir como multiplicador de fuerzas que ha aumentado la eficacia y potencial de combate de las fuerzas militares. Mientras que Clearview AI ha ofrecido altas capacidades para el reconocimiento e identificación de combatientes. Por su parte, Delta es un software que permite cartografiar en tiempo real la evolución del frente. Por tanto, este programa ha permitido coordinar unidades militares de forma eficiente, incluso en entornos volátiles gracias al apoyo internacional. En cuanto a GIS ARTA, se trata de un sistema que integra la IA con el internet satelital, lo que ha permitido optimizar la respuesta de la capacidad de la artillería ucraniana, facilitando el ataque de posiciones enemigas con mayor inmediatez y eficacia.

Estas herramientas no deben interpretarse como soluciones aisladas, sino como parte de un ecosistema de adaptación tecnológica que combina inteligencia, movilidad, coordinación y capacidad de respuesta en tiempo real.

Con relación al estudio del conflicto por parte de Europa, es importante destacar que la Comisión Europea ha impulsado diversas iniciativas, como el European Defence Fund (EDF) y la Permanent Structured Cooperation (PESCO), las cuales reflejan el compromiso por fortalecer la capacidad militar conjunta y el fomento de la innovación tecnológica en el área de la defensa común. Estas herramientas buscan consolidar una base integral en materia tecnológica en el ámbito de seguridad y defensa que sea más eficiente entre los EEMM, donde prima el fomento de proyectos colaborativos en áreas clave como la IA o la ciberseguridad. Por todo ello, el análisis de la guerra de agresión rusa cobra un valor estratégico, ya que de su estudio se pueden extraer lecciones prácticas sobre la adaptación de la estrategia militar europea a los desafíos actuales, donde la tecnología desempeña un papel central en la eficacia operativa y la resiliencia de las amenazas híbridas y convencionales.

No obstante, esta transformación no está exenta de controversias. El empleo de estas nuevas tecnologías en contextos bélicos plantea importantes desafíos éticos, legales y geoestratégicos, pasando por la dificultad de probar la autoría de determinadas acciones cibernéticas y, por ende, la complejidad de acreditar e imputar la responsabilidad derivada de las mismas. Además de las implicaciones que conlleva en la estrategia militar, las cuales abarcan múltiples dimensiones, desde la

planificación táctica y logística, hasta la inteligencia, la ciberdefensa, y la gestión del propio territorio.

Además, esta transformación también introduce dependencias estratégicas, especialmente respecto de proveedores tecnológicos externos, cadenas de suministro digital y capacidades de mantenimiento y actualización permanente.

6.1 La desinformación

Las técnicas de desinformación se han visto potenciadas por el empleo de las Tecnologías de la Información y la Comunicación (TIC), las cuales se han usado como un vehículo para transmitir y difundir rápidamente la información excluyendo las barreras geográficas y ensalzando el potencial y la capacidad que tienen las TIC de llegar a un número indeterminado de personas de forma eficiente y eficaz.

Las TIC han revolucionado la forma en que se crea, difunde y consume la información a nivel global. Su capacidad para amplificar mensajes en tiempo real y alcanzar a un número elevado de individuos ha potenciado de forma notable la influencia en la opinión pública, no solo a nivel estatal, sino internacional. Por ello, esta transformación en la comunicación ha dado lugar a un escenario informativo más amplio con una gran facilidad de acceso, que, además, permite moldear la percepción social de forma deliberada.

En este contexto, los actores estatales y no estatales han aprovechado las TIC para desarrollar campañas de desinformación altamente efectivas, que no solo distorsionan los hechos, sino que también que buscan erosionar la confianza en las instituciones, deslegitimarlas, así como polarizar a la sociedad internacional y generar confusión en momentos críticos como los de una guerra (Alastuey *et al.*, 2024).

Los mecanismos que se suelen emplear en estas campañas de desinformación se basan en la difusión deformada de la realidad con datos falsos, tergiversándola, o directamente manipulándola. La facilidad con la que puede manipularse esta información que afecta directamente a la opinión pública es un reto latente, ya que estas campañas de desinformación proporcionan inestabilidad sobre la seguridad informativa y, en consecuencia, sobre la seguridad a nivel integral, de hecho, nuestra Estrategia de Seguridad Nacional (ESN21) prevé esta táctica como una grave amenaza para la seguridad nacional.

En la guerra de agresión rusa se han empleado estas campañas con fines propagandísticos, con el objetivo de llegar tanto a los afectados como a posibles cooperantes del conflicto armado.

Habitualmente, estas campañas de desinformación con uso propagandístico se destinan a minar la moral del adversario y ensalzar las fortalezas de uno. Del mismo modo, el uso de múltiples fuentes de información, como los medios de comunicación tradicionales o incluso las redes sociales, se han consolidado como un vehículo idóneo para llevar a cabo estas acciones de desinformación. Herramientas como las *fake news* ilustran cómo estos canales pueden ser instrumentalizados para deslegitimizar las

acciones del adversario, y, al mismo tiempo, justificar las propias, en un intento claro de manipular la percepción pública y condicionar la opinión internacional.

Estas herramientas comunicativas no solo buscan confundir o engañar, sino que tienen el fin principal de moldear el relato dominante del conflicto, influyendo a actores clave de la comunidad internacional y generar en consecuencia la división global. Con todo ello, la desinformación es un arma más dentro del abanico de tácticas empleadas por un Estado dentro de la GH, con un gran impacto y con un potencial devastador sobre la legitimidad y cohesión social, además de poder alterar potencialmente los procesos de toma de decisiones de la comunidad internacional.

La lucha contra la desinformación constituye un complejo desafío que exige una respuesta combinada y coordinada. En esta línea, podemos destacar que España ha desarrollado un marco jurídico y operativo integral y sólido, que cuenta con la participación de instituciones gubernamentales y actores sociales (Alastuey *et al.*, 2024). No obstante, la eficacia de este enfoque no es estática, sino que depende de la capacidad de adaptación a la evolución de las nuevas tecnologías. En este sentido, resulta esencial hacer hincapié en que para combatir adecuadamente la desinformación es preciso fortalecer la implicación cívico-militar para fortalecer los sistemas de comunicación y dotarlos de la mayor transparencia, especialmente con los medios de comunicación.

En el plano internacional, resulta esencial contar con la colaboración de la UE y la OTAN para reforzar las capacidades de los Estados y dar una respuesta eficaz ante estas amenazas que transcienden las fronteras y comprometen la estabilidad global. Estas alianzas permiten compartir conocimientos y coordinar los esfuerzos, además de demostrar el compromiso global y proactivo ante estas amenazas híbridas. Solo un enfoque integral, basado en la educación, la transparencia y la colaboración podrá contribuir a una sociedad más resiliente frente a los retos de la desinformación contemporánea.

En este sentido, la desinformación no debe entenderse como un fenómeno auxiliar, sino como un instrumento estructural de la GH, cuya eficacia depende tanto de la capacidad del emisor para producir contenidos manipulados como de la vulnerabilidad del ecosistema informativo en el que dichos contenidos circulan.

6.2 El ciberespacio

El ciberespacio, prácticamente inexplorado en los conflictos armados del siglo xx, se ha convertido en un escenario estratégico central en las guerras modernas del siglo xxi, como se evidencia tanto en el conflicto entre Rusia y Ucrania como en otros recientes ataques cibernéticos relacionados con la escalada en Gaza.

En el caso de Ucrania, desde los primeros días de la invasión, Rusia desplegó una serie de ciberataques dirigidos contra las infraestructuras críticas del Estado ucraniano, en un intento de desestabilizar sus capacidades institucionales y logísticas. Entre estos ciberataques perpetrados destaca el que se llevó a cabo contra la principal compañía de telecomunicaciones del país, Ukrtelecom, mediante la acción de denegación de

servicios (DoS). Con este ataque, Rusia logró interrumpir las comunicaciones, dejando amplias zonas de la población incomunicadas durante varias horas (SSSCIPU, 2022).

Este caso ilustra que el ciberespacio no funciona como un dominio separado de la guerra, sino como un multiplicador de efectos que puede alterar la logística, la moral y la continuidad institucional.

No obstante, Ucrania ha sabido articular una defensa digital relativamente eficaz que, pese a la asimetría de recursos, ha permitido contener, neutralizar e incluso revertir parte de las operaciones hostiles. Es decir, Ucrania respondió con una combinación de resiliencia digital, cooperación con aliados occidentales y apoyo de empresas tecnológicas, lo que permitió mantener la operatividad institucional y reforzar la defensa del espacio informativo.

Un hecho especialmente relevante es que esta presión tecnológica ha forzado incluso al Ejército ruso a tomar decisiones menos seguras, como el empleo de frecuencias de radio abiertas y no cifradas para realizar sus comunicaciones tácticas, lo que permitió su interceptación. Este hecho pone de relieve no solo las debilidades operativas rusas, sino que también demuestra el alto grado de competencia tecnológica alcanzado por Ucrania, incluso en un entorno tan complejo y hostil como el campo de batalla cibernético.

Estos acontecimientos han captado la atención de la comunidad internacional, no solo por el impacto del desarrollo del conflicto en sí mismo, sino también por el valor que ofrece para el análisis estratégico y la formulación de nuevas políticas de cooperación en materia de seguridad y defensa en el ámbito digital. Un ejemplo claro es la extraordinaria colaboración de Ucrania entre sus aliados de Occidente y las grandes empresas tecnológicas como Microsoft o Google, que han proporcionado apoyo en materia de infraestructura digital, ciberseguridad y almacenamiento en la nube.

Una lección clave que puede desprenderse de esta experiencia práctica, aún sin haber finalizado el conflicto, es, por tanto, que, a pesar de la complejidad y multidimensionalidad del ciberespacio, existen oportunidades reales para establecer mecanismos de defensa eficaces. No cabe duda de que esta defensa se fortalece gracias a la cooperación cívico-militar, público-privada e internacional, configurándose como un nuevo modelo de seguridad colectiva en el ámbito cibernético que puede servir como referente para futuros conflictos.

En otras palabras, la lección principal no es que la defensa digital elimine la vulnerabilidad, sino que una arquitectura resiliente puede reducir considerablemente el impacto de los ataques y elevar el coste estratégico del agresor.

7 El reto de modernizar la estrategia de defensa europea

Aunque la UE y la OTAN han reforzado su marco estratégico frente a las amenazas híbridas, con iniciativas como la citada Brújula Estratégica o el Nuevo Concepto Estratégico de la OTAN, el caso ucraniano evidencia una distancia persistente entre

la formulación de objetivos y la disponibilidad real de capacidades operativas. La dificultad técnica de atribuir ciberataques, la fragmentación de capacidades nacionales, la diversidad de doctrinas y la ausencia de una cadena de mando plenamente integrada limitan la rapidez y eficacia de la respuesta europea.

La invasión rusa de Ucrania ha representado un punto de inflexión para la seguridad europea, ya que, por primera vez, después del final de la II Guerra Mundial, el continente europeo se enfrenta directamente a un conflicto armado de alta intensidad en sus inmediaciones, con implicaciones profundas, tanto para la estabilidad regional como para el orden internacional.

Este escenario ha puesto de manifiesto las vulnerabilidades estructurales del sistema de defensa europeo y ha reactivado la importancia de la estrategia de la OTAN, al tiempo que impulsa el replanteamiento acelerado de las políticas de seguridad digital y defensa común dentro de la UE.

Esta urgencia de modernizar las capacidades ante un nuevo tipo de guerra multidimensional y tecnológica hace que Europa se enfrente a un desafío estratégico mayúsculo que implica repensar su estructura de defensa colectiva, así como su autonomía digital y capacidad de respuesta ante amenazas convencionales y no convencionales.

De hecho, la agresión rusa no solo ha quebrado la arquitectura de seguridad que Europa había construido tras el colapso de la Unión Soviética en el año 1991 (Artola, 2023), sino que ha puesto de manifiesto el retorno de una lógica de competencia entre grandes potencias.

En este nuevo escenario geopolítico, tanto la UE como la OTAN han intensificado sus políticas de seguridad y defensa, reforzando sus capacidades de disuasión frente a las amenazas cada vez más complejas, como las de naturaleza híbrida, pero la existencia de instrumentos estratégicos no equivale automáticamente a una capacidad de respuesta integrada, donde persisten tres limitaciones fundamentales:

1. Fragmentación militar: los 27 EEMM mantienen sistemas de armamento divergentes, doctrinas nacionales dispares y prioridades geoestratégicas distintas, lo que genera duplicidades costosas y dificulta la interoperabilidad (Segoviano, 2022).
2. Desigualdad política: no todos los Estados perciben las mismas amenazas con igual intensidad, y los intereses nacionales priman frecuentemente sobre la acción colectiva. Es decir, para que la UE desarrolle una acción exterior autónoma es preciso que los Estados estén en concordancia política, permitiendo una sólida e integral estrategia para enfrentar crisis de gran envergadura (De Castro y Borrajo, 2019).
3. Ausencia de mando integrado: a pesar de los avances institucionales, Europa carece de una estructura de mando clara y eficaz para gestionar crisis militares de forma autónoma. La ausencia de una decisión estratégica plenamente funcional para todos los Estados miembros implica una limitación en la capacidad de reacción rápida limitando el potencial de la UE como actor militar independiente en el sistema internacional.

Por consiguiente, estas limitaciones explican por qué la respuesta europea ha sido más sólida en el plano normativo que en el estrictamente operativo. Estas limitaciones dificultan la interoperabilidad entre las fuerzas armadas nacionales y, por ende, la proyección de la UE en su rol de actor autónomo de seguridad ante los escenarios hostiles. Por ello, el reto no consiste únicamente en diseñar nuevas estrategias, sino en convertirlas en capacidades efectivas, interoperables y sostenibles. Estos desafíos deben ser abordados de forma urgente y coordinada para que Europa esté capacitada para desempeñar un papel relevante en esta materia en el nuevo orden geopolítico.

En otras palabras, la seguridad europea no puede sostenerse exclusivamente en la estabilidad diplomática, sino que se hace necesario una capacidad militar interoperable y adaptable a un entorno hostil caracterizado por la volatilidad estratégica y la creciente imprevisibilidad, ya que la principal brecha sigue estando entre la ambición normativa y la capacidad operativa efectiva.

Para lograr esta transformación profunda es preciso atender a las lecciones clave que nos deja el conflicto de agresión a Ucrania, que no pueden ignorarse y que deben ser inspiradoras para mantener una postura defensiva creíble y eficaz para Europa.

7.1 Lecciones para Europa

La experiencia ucraniana ofrece cuatro lecciones principales para la defensa europea. En primer lugar, la doctrina debe integrar el ciberespacio y la desinformación como dominios centrales del conflicto. En segundo lugar, las capacidades tecnológicas deben traducirse en interoperabilidad real y no solo en programas de modernización. En tercer lugar, la cooperación público-privada debe dejar de ser excepcional y convertirse en un componente estructural de la defensa. En cuarto lugar, la coordinación entre la UE y la OTAN debe orientarse a respuestas más rápidas, integradas y sostenibles frente a amenazas híbridas.

1. Doctrina multidominio: el ciberespacio y la desinformación deben integrarse como dominios operacionales centrales, no como ámbitos auxiliares. Los ciberataques contra Ukrtelecom y las campañas de *fake news* rusas demuestran que estos instrumentos pueden degradar infraestructuras críticas y erosionar la cohesión social con efectos estratégicos equivalentes a operaciones cinéticas. En consecuencia, la ciberdefensa deja de ser un ámbito auxiliar o complementario, pasando a convertirse en una prioridad estratégica en situaciones bélicas. La capacidad de resistir, responder y recuperarse frente a amenazas híbridas constituye un componente esencial en la resiliencia nacional y europea.
2. Interoperatividad tecnológica real: las capacidades tecnológicas, como la IA, los UAV, o el análisis de datos en tiempo real deben traducirse en sistemas interoperables entre Estados y con la OTAN, no quedarse en programas nacionales aislados. La experiencia de Palantir, GIS ARTA y Delta en Ucrania evidencia el valor multiplicador de plataformas integradas.

   Esto es, el empleo de la tecnología ha alterado el equilibrio táctico convencional, obligando a una revisión urgente de la cultura de defensa y seguridad, ejemplo

claro de ello es la facilidad con la que pueden ser desplegados los drones, así como su bajo coste (en comparación a otros sistemas convencionales), plantea un desafío inmediato de integración de estas tecnologías en todas las fuerzas armadas europeas. Otro ejemplo es el empleo de la IA como potenciador de la estrategia militar por la facilidad de análisis de datos en tiempo real para la toma de decisiones, ya que supone un avance claro que constituye una supremacía del campo de batalla y las operaciones que se desarrollan en él, ya sea a nivel físico como cibernético.

3. Cooperación público-privada estructural: la colaboración con empresas tecnológicas (Microsoft, Google, Clearview AI) debe dejar de ser *ad hoc* para convertirse en componente permanente de la defensa europea. Ucrania sobrevive gracias a este ecosistema híbrido cívico-militar-tecnológico. Es decir, la cooperación de Ucrania con empresas privadas ha impulsado el potencial de las tecnologías emergentes para la mejora táctica de la guerra, permitiendo una mayor garantía de la seguridad e integridad de las tropas, así como una optimización de recursos.
4. Coordinación UE-OTAN acelerada: la movilidad militar europea debe completarse con rutas terrestres, aéreas y marítimas armonizadas que permitan despliegues rápidos. La actual fragmentación logística imposibilita respuestas efectivas ante crisis de alta intensidad.

En resumen, los planes de seguridad del siglo xxi no pueden desvincularse de la innovación tecnológica, sino que deben adaptarse a ella para ofrecer una defensa efectiva que tenga capacidad de minimizar y mitigar las posibles amenazas híbridas a las que un Estado miembro o sus aliados pueden enfrentarse, adaptándose en todo caso, a los nuevos desafíos que nos propone la GH.

Huelga decir que esta modernización estratégica de defensa común no solo requiere voluntad política y avances tecnológicos, sino que además debe hacer frente a diversos obstáculos estructurales que pueden limitar su eficacia.

Es decir, esta modernización de la política de defensa europea no es solo tecnológica, sino organizativa e institucional. Europa debe pasar de diseñar estrategias a construir capacidades efectivas, interoperables y sostenibles. La UE tiene ante sí la oportunidad de consolidarse como un actor estratégico autónomo y resiliente en el orden mundial. La pregunta estratégica ya no es si debe modernizarse, pues la respuesta es evidente, sino si lo hará con la velocidad, escala y determinación que exige el nuevo entorno geopolítico.

8 Conclusiones

El análisis desarrollado confirma que la guerra contemporánea ha trascendido el ámbito exclusivamente cinético para convertirse en un fenómeno multidominio donde se han desarrollado nuevas y potenciales amenazas capaces de desestabilizar un país, como el ciberespacio, la desinformación y las tecnologías emergentes, que contienen elementos lesivos que afectan directamente a la seguridad nacional y

colectiva y que funcionan como instrumentos estructurales de coerción estratégica, no como meros complementos operativos.

Respondiendo a la pregunta de investigación planteada sobre en qué medida la guerra de Ucrania ha modificado la comprensión y el diseño de la defensa europea frente a amenazas híbridas y ciberataques, este trabajo demuestra que el conflicto ucraniano ha actuado como catalizador de tres transformaciones fundamentales:

1. Conceptual: la GH ya no es un concepto teórico, sino una realidad operativa verificable que combina operaciones militares convencionales con ciberataques (ej. Ukrtelecom), campañas de desinformación masiva y tecnologías disruptivas (IA, drones, análisis predictivo). El conflicto en Ucrania ha evidenciado con claridad que el ciberespacio ya no es exclusivamente un escenario complementario en la guerra tradicional, sino que supone un frente central en los conflictos armados del siglo xxi. Lejos de ser un terreno reservado en exclusiva para las potencias con mayores recursos, observamos a través de la experiencia de Ucrania cómo otros Estados, con una estrategia sólida, articulada e integral en materia digital, y en este caso, junto al apoyo internacional y la cooperación con actores públicos y privados, es posible combatir los ataques en el ciberespacio y construir una defensa digital resiliente y eficaz. Pues el empleo del ciberespacio no conlleva en exclusiva ataques a infraestructuras críticas de un país, sino que abarca otras operaciones como son la desinformación o el sabotaje digital, lo que determina la necesidad de contar con una respuesta integral, ágil y multidisciplinar. Ucrania evidencia que la superioridad tecnológica depende menos del volumen de recursos que de la capacidad de integración y adaptación en tiempo real.
2. Doctrinal: el ciberespacio se ha consolidado como dominio operacional central, donde la resiliencia institucional resulta tan decisiva como las capacidades ofensivas. La defensa digital ucraniana, apoyada en cooperación público-privada (como con Palantir, Microsoft y Google), demuestra que Estados medianos pueden contrarrestar potencias cibernéticas superiores mediante arquitecturas híbridas cívico-militares.
3. Institucional: Europa enfrenta una brecha persistente entre ambición estratégica (Brújula Estratégica, Nuevo Concepto OTAN) y capacidad operativa real, condicionada por fragmentación militar, divergencias políticas y ausencia de mando integrado. La experiencia ucraniana revela que la cooperación UE-OTAN debe acelerarse hacia respuestas efectivas, interoperables y sostenibles.

En este contexto, la lucha contra las amenazas híbridas no puede realizarse de forma aislada, sino que exige una estrategia de cooperación integral estructurada en diversos niveles, pero en todo caso, basada en el conocimiento riguroso y la coordinación de expertos nacionales e internacionales. De hecho, estas evidencias imponen a Europa cuatro imperativos estratégicos ineludibles:

- Doctrina multidominio: integrar ciberespacio y desinformación como dominios centrales de planificación y operaciones.

- Interoperabilidad real: convertir programas tecnológicos en capacidades compartidas y efectivamente desplegables.
- Ecosistema híbrido: estructurar la cooperación y colaboración cívico-militar, público-privada e internacional como ejes esenciales.
- Coordinación reforzada: armonizar UE-OTAN para respuestas rápidas ante crisis de alta intensidad.

Por todo lo expuesto, podemos afirmar que la guerra de agresión rusa contra Ucrania no solo ha desatado una devastadora crisis humanitaria, sino que también ha actuado como catalizador de profundas transformaciones en lo referente a la conceptualización y naturaleza del conflicto armado en la actualidad. De hecho, es evidente que este enfrentamiento ha acelerado la transición de la guerra tradicional hacia el modelo de guerras híbridas que experimentamos en el siglo xxi, en el que se combinan operaciones militares convencionales junto con herramientas y métodos del ciberespacio, la desinformación y el uso de tecnologías emergentes como la IA o los drones.

En este contexto, podemos concluir que la tecnología no solo se ha consolidado como un elemento potenciador de las capacidades militares, sino que se ha configurado como un componente estructural de la propia estrategia de seguridad y defensa. Donde resulta evidente que la experiencia de Ucrania ofrece valiosas lecciones en la actualidad, pese a que el conflicto no haya terminado, ya que delata la necesidad de adaptar las capacidades digitales e invertir en resiliencia, así como en cooperación tecnológica en escenarios de alta intensidad como es un conflicto bélico. Este conflicto pone de relieve la necesidad urgente de que Europa y sus aliados refuercen sus políticas en materia digital y tecnológica con el objetivo de aumentar sus capacidades defensivas y mecanismos de respuesta ante amenazas híbridas.

La reconfiguración del equilibrio geopolítico europeo en que ha derivado este conflicto también recalca que la seguridad no puede entenderse exclusivamente en términos militares, sino que exige una visión más amplia, que incorpore además la innovación tecnológica y la ciberdefensa, así como el refuerzo de alianzas estratégicas y una mayor integración de actores estatales y no estatales. Con todo ello, el análisis de este conflicto, hasta el momento, permite comprender que el futuro de las guerras ya ha comenzado y que se requiere preparación, cooperación y adaptación tecnológica para afrontar con mayores garantías los desafíos del nuevo orden internacional.

En definitiva, el caso ucraniano no solo ilustra el nuevo paradigma bélico del siglo xxi, sino que formula un desafío concreto: modernizar la defensa europea no con declaraciones de intenciones, sino con capacidades reales, interoperables y desplegables que permitan enfrentar amenazas híbridas con la misma velocidad y eficacia que exige el nuevo entorno geopolítico.

La principal aportación de este artículo no es solo describir la transformación de la guerra, sino mostrar que dicha transformación impone a Europa una revisión profunda de sus marcos doctrinales, industriales y organizativos. La pregunta decisiva ya no es si la tecnología cambia la guerra, sino qué tipo de arquitectura política y estratégica permite convertir esa transformación en una ventaja defensiva real.

Bibliografía

Alastuey Rivas, J. *et al.* (2024). *La desinformación como arma de guerra* [en línea]. Documento de Opinión IEEE 26/2024. [Consulta: 2026]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO26_2024_VVAA_Desinformacion.pdf

Artola Kortam M. (2023). Rusia y Ucrania: Una mirada desde la historiografía reciente [en línea]. *Cuadernos de Historia Contemporánea*. 45, pp. 423-430. [Consulta: 2026]. Disponible en: https://doi.org/10.5209/chco.87941

Aydemir, E. (2022). Ukraine's cognitive warfare operations against Russia: representation, story and micro-mythology. *Avrasya Uluslararası Araştırmalar Dergisi*. 10(32), pp. 358-367.

Baqués, J. (2017). Hacia una definición del concepto de «Gray Zone» (GZ). *Boletín Instituto Español de Estudios Estratégicos (IEEE)*.

Colom Piella, G. (2020). Anatomía de la desinformación rusa. *Historia y Comunicación Social*. 25(2), pp. 473-480.

—. (2022). Las estrategias de la OTAN en respuesta a los conflictos híbridos [en línea]. *CIDOB.* [Accessed: 2026]. Available at: https://www.cidob.org/publicaciones/las-estrategias-de-la-otan-en-respuesta-los-conflictos-hibridos

Consejo de la Unión Europea. (2024). Una Brújula Estratégica para la Seguridad y la Defensa [en línea]. *consilium.europa.eu.* [Consulta: 2026]. Disponible en: https://www.consilium.europa.eu/es/policies/strategic-compass/

—. (2025). Cómo refuerza la UE su ciberseguridad. [en línea]. *consilium.europa.eu.* [Consulta: 2026]. Disponible en: https://www.consilium.europa.eu/es/policies/cybersecurity/

De Castro, J.L. y Borrajo, D. (2019). El futuro de la seguridad y la defensa en la UE post-Brexit: el salto a la integración [en línea]**.** *Cuadernos Europeos De Deusto.* 60, pp. 187-217. [Consulta: 2026]. Disponible en: https://doi.org/10.18543/ced-60-2019pp187-217

Fiott, D. (2022). The Fog of War: Russia's War on Ukraine, European Defence Spending and Military Capabilities. *Intereconomics* [en línea]. 57, pp. 152-156. [Consulta: 2026]. Disponible en: https://doi.org/10.1007/s10272-022-1051-8

Franco, J. D. (2023). Guerra híbrida: críticas y retos del conflicto moderno. *Revista Estado, Paz y Sistema internacional.* 2(4), pp. 19-204.

Franke, U. y Söderström, J. (2023). *Star 'Tech' Enterprise: Tecnologías emergentes en la guerra rusa contra Ucrania* [en línea]. European Council On Foreign Relations. [Consulta: 2026]. Disponible en: https://ecfr.eu/madrid/publication/star-tech-enterprise-tecnologias-emergentes-en-la-guerra-rusa-contra-ucrania/

Gutiérrez de León, B. (2021). Amenazas híbridas y zona gris. OTAN, Unión Europea y España ante esta nueva forma de enfrentamiento [en línea]. *Global Strategy Reports.* [Consulta: 2026]. Disponible en: https://global-strategy.org/amenazas

-hibridas-y-zona-gris-otan-union-europea-y-espana-ante-esta-nueva-forma-de-enfrentamiento/

MCDC. (2017). *Understanding Hybrid Warfare* [en línea]. MCDC. [Consulta: 2026]. Disponible en: https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

Ministerio de Defensa. (2022). *Nuevo Concepto Estratégico de la OTAN* [en línea]. Ministerio de Defensa. [Consulta: 2026]. Disponible en: https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

OTAN. (2016). *Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016* [en línea]. Nato.int. [Consulta: 2026]. Disponible en*:* https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Rodríguez, E. *et al.* (2023). *La inteligencia artificial en la guerra híbrida como arma de desinformación* [en línea]. Documento de Opinión IEEE 61/2023. [Consulta: 2026]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO61_2023_EDUROD_Inteligencia.pdf

Segoviano Monterrubio, S. (2022). Análisis de escenario de conflicto. En: López Garrido, D. (ed.). *La defensa europea y la Europa de la defensa. Informe 2022*. pp. 23-42. Fundación Alternativas.

Silva Ramirez, F. (2022). Operaciones en la "Zona Gris": ¿de qué estamos hablando? . *Escenarios Actuales año.* 27, pp. 107-121. Centro de Estudios e Investigaciones Militares Ejército de Santiago de Chile.

State Service of Special Communications and Information Protection of Ukraine - SSSCIPU. (2022). *Cyberattack against Ukrtelecom on March 28: the details* [en línea]. [Consulta: 2026]. Disponible en : https://cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali

Unión Europea. (2025). Resolución del Parlamento Europeo, de 2 de abril de 2025, sobre la aplicación de la política común de seguridad y defensa: informe anual 2024. *Diario Oficial de la Unión Europea*.

Artículo recibido: 11 de febrero de 2026
Artículo aceptado: 28 de abril de 2026