

REPORTES DE INVESTIGACIÓN

Starlink en el escenario bélico: innovación, ética y desafíos para la seguridad global con implicaciones en la defensa nacional

Starlink in the Context of War: Innovation, Ethics, and Challenges Regarding Global Security with Implications for National Defense

YAMILA ITATÍ RECALDE MELNECHENKO

Universidad de la Defensa Nacional (UNDEF) y Universidad Nacional del Nordeste (UNNE), Argentina

yamilamelnfashionbusiness@gmail.com

Resumen

La irrupción de tecnologías comerciales en conflictos bélicos ha transformado la seguridad global, como ilustra el caso de Starlink, la constelación satelital de SpaceX liderada por Elon Musk. Este artículo analiza su papel durante el conflicto Rusia-Ucrania de 2022, cuando Starlink restauró comunicaciones críticas tras ciberataques rusos, pero también generó controversias por su uso en operaciones militares, como el ataque frustrado en Crimea. A través de un estudio de caso, se exploran los dilemas éticos, estratégicos y geopolíticos que plantea la privatización de capacidades defensivas, que incluye la creación de Starshield para usos militares. El análisis incorpora teorías de seguridad internacional y ética tecnológica, con foco en la tensión entre innovación y responsabilidad. Desde la perspectiva argentina, se discuten las

implicaciones para la ciberdefensa, la soberanía tecnológica y la vigilancia del Atlántico Sur. Los resultados subrayan la necesidad de marcos regulatorios que equilibren los beneficios de la tecnología dual con los riesgos de escalada bélica. El presente artículo concluye con recomendaciones para fortalecer las capacidades nacionales frente a la creciente influencia de actores privados en la defensa.

Palabras clave: Starlink — ciberdefensa — ética tecnológica — seguridad global — defensa nacional

Abstract

The incursion of commercial technologies into armed conflicts has reshaped global security, as exemplified by Starlink, SpaceX's satellite constellation led by Elon Musk. This article examines its role during the 2022 Russia-Ukraine conflict, where Starlink restored critical communications after Russian cyberattacks but sparked controversies due to its use in military operations, such as a thwarted attack in Crimea. Through a case study, the ethical, strategic, and geopolitical dilemmas posed by the privatization of defense capabilities were explored, including the establishment of Starshield for military purposes. The analysis draws on theories of international security and technological ethics, highlighting the tension between innovation and responsibility. From an Argentine perspective, it discusses the implications of this event for cyberdefense, technological sovereignty, and surveillance in the South Atlantic. The findings underscore the need for regulatory frameworks to balance the benefits of dual-use technologies with the risks of conflict escalation. The article concludes with recommendations to strengthen national capabilities in response to the growing influence of private actors in defense.

Keywords: Starlink — cyberdefense — technological ethics — global security — national defense.

Introducción

En la era digital, la convergencia entre tecnología y defensa ha redefinido los paradigmas de la seguridad global. Empresas privadas, tradicionalmente ajenas a los conflictos bélicos, han emergido como actores clave al proporcionar capacidades estratégicas que antes eran exclusivas de los Estados. Un caso paradigmático es el de Starlink, la constelación de satélites de Space Exploration Technologies Corporation, liderada por el empresario Elon Musk y diseñada para ofrecer conectividad global de alta velocidad. Sin embargo, su intervención en el conflicto Rusia-Ucrania de 2022 reveló el potencial y los riesgos de la tecnología comercial en escenarios bélicos. Cuando ciberataques rusos paralizaron las comunicaciones ucranianas, Starlink restauró redes críticas, lo que permitió operaciones civiles y militares. No obstante, su uso en un ataque frustrado con drones submarinos contra la flota rusa en Crimea desató una controversia sobre los límites éticos y estratégicos de tales intervenciones (Isaacson, 2023). Este texto analiza el papel de Starlink en contextos bélicos, mientras que explora cómo la innovación tecnológica puede tanto fortalecer la seguridad como generar riesgos de escalada geopolítica. El caso plantea preguntas fundamentales: ¿qué responsabilidad tienen las empresas privadas en conflictos armados? ¿Cómo afecta la privatización de capacidades defensivas a la soberanía estatal? ¿Qué aprendizaje puede extraer un país como Argentina, con intereses estratégicos en ciberdefensa y el Atlántico Sur? A través de este caso de estudio, se examinan los aportes de Starlink en Ucrania, los dilemas éticos de su uso militar y las implicaciones para la seguridad global y regional. La relevancia del tema radica en la creciente dependencia de tecnologías duales, de uso

civil y militar. Según Singer (2009), la incorporación de actores no estatales en la guerra tecnológica introduce asimetrías que desafían las normas tradicionales de conflicto. En Ucrania, Starlink no solo restauró las comunicaciones, sino que también habilitó operaciones tácticas, como el uso de drones, lo que llevó a Musk a limitar ciertas funciones para evitar una escalada nuclear (Isaacson, 2023). Esta decisión, aunque pragmática, evidenció la falta de marcos regulatorios claros para empresas tecnológicas en escenarios bélicos. En respuesta, SpaceX creó Starshield, una división dedicada a aplicaciones militares bajo supervisión estatal, y, de esta manera, se trasladó la responsabilidad al gobierno estadounidense. Desde la perspectiva argentina, el caso de Starlink es particularmente pertinente. La defensa nacional, según la Ley 23554 (1988), prioriza la protección de la soberanía, los recursos naturales y los espacios estratégicos como el Atlántico Sur. En un contexto de amenazas cibernéticas crecientes, con ataques a infraestructuras críticas en la región y la necesidad de vigilancia marítima en áreas como las Islas Malvinas, la conectividad satelital y la ciberdefensa son prioridades. Sin embargo, la dependencia de tecnologías extranjeras plantea riesgos para la autonomía estratégica, lo que subraya la importancia de desarrollar capacidades propias, como las promovidas por empresas como ARSAT o INVAP (Calle, 2020).

Para lograr un análisis completo, el artículo se estructura en cinco secciones. Primero, se presenta un marco teórico en el que se articulan conceptos de seguridad internacional, ciberdefensa y ética tecnológica. Segundo, se describe la metodología, basada en el caso de estudio. Tercero, se analiza el rol de Starlink en Ucrania, sus dilemas éticos y su impacto estratégico. Cuarto, se exploran las implicaciones para la defensa argentina, con énfasis en ciberdefensa y soberanía tecnológica. Finalmente, se ofrecen conclusiones y recomendaciones para equilibrar innovación y responsabilidad en la seguridad global.

El análisis del papel de Starlink en conflictos bélicos requiere-

re un marco teórico que integre perspectivas de seguridad internacional, ciberdefensa y ética tecnológica. Asimismo, tres conceptos centrales guían este estudio: la privatización de la defensa, la tecnología dual y los dilemas éticos en la guerra tecnológica.

Privatización de la defensa

La privatización de capacidades defensivas ha transformado la naturaleza de los conflictos modernos. Según el realismo en relaciones internacionales, los Estados buscan maximizar su poder y seguridad en un sistema anárquico (Waltz, 1979). Sin embargo, la irrupción de actores no estatales, como empresas tecnológicas, introduce nuevas dinámicas. Singer (2009) argumenta que la externalización de funciones militares a empresas privadas (desde logística hasta inteligencia) genera asimetrías de poder, ya que los Estados dependen de actores cuyos intereses no siempre coinciden con los nacionales. En el caso de Starlink, SpaceX proporcionó una capacidad estratégica (conectividad satelital) que influyó directamente en el curso del conflicto ucraniano y dejó en evidencia el peso de los actores privados en la geopolítica.

Tecnología dual y ciberdefensa

Las tecnologías duales, diseñadas para usos civiles pero aplicables a contextos militares, son un pilar de la guerra moderna. Nye (2017) define la ciberdefensa como la protección de infraestructuras digitales frente a amenazas que combinan tácticas convencionales y digitales, como los cibertaqueros rusos en Ucrania. La conectividad satelital, como la ofrecida por Starlink, es un ejemplo de tecnología dual: su propósito original (acceso global a internet) se transformó en una herramienta táctica para comunicaciones militares y

operaciones con drones. Este fenómeno plantea desafíos regulatorios, ya que las empresas comerciales no están sujetas a las mismas normas que los actores estatales (Buchanan, 2020). En América Latina, donde la ciberdefensa es una prioridad emergente, la dependencia de tecnologías extranjeras puede limitar la autonomía estratégica (Calle, 2020).

Dilemas éticos en la guerra tecnológica

El uso de tecnologías comerciales en conflictos plantea dilemas éticos significativos. Floridi (2014) sostiene que la ética digital debe abordar las consecuencias no intencionadas de la innovación, especialmente en contextos de alto riesgo como la guerra. En Ucrania, la intervención de Starlink salvó vidas al restaurar las comunicaciones, pero también facilitó operaciones militares que podrían haber desencadenado una escalada nuclear (Isaacson, 2023). Esto es un ejemplo del principio de doble efecto: una acción con fines benéficos que puede generar consecuencias perjudiciales como una escalada bélica. Además, la decisión unilateral de Musk de limitar el uso de Starlink en Crimea plantea interrogantes sobre la legitimidad de las empresas privadas para influir en conflictos internacionales.

Relevancia para la defensa nacional

Desde la perspectiva argentina, estos conceptos son cruciales. En la Ley de Defensa Nacional (1988), se enfatiza la protección de la soberanía y los recursos estratégicos, que incluye el ciberespacio y el Atlántico Sur. La vigilancia de áreas como las Islas Malvinas requiere capacidades satelitales y de ciberdefensa que podrían beneficiarse de tecnologías como Starlink, pero también exponen al país a riesgos de dependencia tecnológica. El constructivismo, que destaca la impor-

tancia de normas compartidas (Wendt, 1992), sugiere que Argentina debería promover marcos regionales para regular tecnologías duales y fortalecer la cooperación en foros como MERCOSUR.

En síntesis, el marco teórico combina el realismo (poder y tecnología), el análisis de tecnologías duales (ciberdefensa) y la ética digital (responsabilidad). Estos conceptos permiten analizar el caso de Starlink en Ucrania y extraer un aprendizaje para la defensa argentina.

Este artículo adopta un enfoque cualitativo basado en un estudio de caso, centrado en el papel de Starlink durante el conflicto Rusia-Ucrania de 2022. El estudio de caso es una metodología adecuada para analizar fenómenos complejos en contextos específicos, ya que permite una comprensión profunda de las interacciones entre tecnología, geopolítica y defensa (Yin, 2014). La selección del caso responde a su relevancia como ejemplo paradigmático de la intervención de una empresa tecnológica privada en un conflicto bélico, con implicaciones éticas y estratégicas que trascienden el escenario europeo. Las fuentes primarias incluyen el libro de Walter Isaacson (2023), *Elon Musk*, que documenta la intervención de Starlink en Ucrania y las decisiones de Musk frente a los dilemas éticos. Se complementan con fuentes secundarias, como reportes de prensa (p. ej.: *The New York Times*, BBC), documentos oficiales de organismos internacionales (p. ej.: ONU, OTAN) y literatura académica sobre ciberdefensa y seguridad internacional. Para contextualizar las implicaciones regionales, se utilizan estudios sobre ciberseguridad en América Latina y políticas de defensa argentina, lo que incluye publicaciones del Ministerio de Defensa y de la Universidad de la Defensa Nacional.

Los tres ejes del análisis

- Descripción del caso: reconstrucción de los eventos en

Ucrania, desde el ciberataque ruso hasta el uso militar de Starlink.

- Evaluación ética y estratégica: identificación de los dilemas generados por la tecnología dual y las decisiones de SpaceX.
- Implicaciones para la defensa: extrapolación de lecciones para la seguridad global y la ciberdefensa argentina, con énfasis en el Atlántico Sur.

La triangulación de fuentes asegura la validez de los hallazgos, ya que se combinan perspectivas periodísticas, académicas y oficiales. Las limitaciones del estudio incluyen la falta de acceso a datos clasificados sobre las operaciones militares ucranianas y las decisiones internas de SpaceX. Sin embargo, la información pública disponible permite un análisis robusto de las dinámicas tecnológicas y geopolíticas. El enfoque cualitativo privilegia la interpretación crítica sobre la generalización estadística, por lo que se alinea con los objetivos de la *Revista Defensa Nacional* de fomentar debates teóricos y empíricos en el campo de la defensa.

Análisis: Starlink en el conflicto Rusia-Ucrania

El conflicto Rusia-Ucrania, iniciado en febrero de 2022, marcó un punto de inflexión en la guerra moderna al combinar tácticas convencionales con estrategias digitales. Uno de los primeros movimientos de Rusia fue un ciberataque masivo contra las infraestructuras de comunicación ucranianas, el cual desactivó redes civiles y militares. Este hackeo, atribuido a grupos como Sandworm, paralizó sistemas de comando y control, y generó un desequilibrio estratégico (Greenberg, 2022). Ante la solicitud urgente del gobierno ucraniano, Elon Musk, CEO de SpaceX, autorizó el despliegue de Starlink para restaurar la conectividad. En cuestión de días, SpaceX envió miles de terminales satelitales a Ucrania, junto con pane-

les solares y equipos logísticos, que implicaron costos significativos (Isaacson, 2023). La red de Starlink, compuesta por satélites de órbita terrestre baja, ofreció una alternativa resiliente a las redes terrestres comprometidas. Los civiles utilizaron el servicio para coordinar evacuaciones y acceder a información, mientras que las fuerzas militares ucranianas lo aprovecharon para comunicaciones tácticas, inteligencia en tiempo real y operaciones con drones. Según reportes, Starlink fue crucial en la defensa de ciudades como Mariúpol y Kiev, donde las comunicaciones convencionales habían colapsado (*The Washington Post*, 2022).

Impacto estratégico: tecnología dual en acción

El despliegue de Starlink demostró el potencial de las tecnologías duales en conflictos modernos. A diferencia de los satélites geoestacionarios, los satélites LEO de Starlink ofrecen baja latencia y alta resiliencia, ideales para entornos de combate (Buchanan, 2020). En Ucrania, la conectividad satelital permitió a las fuerzas armadas coordinar ataques con drones y artillería, ya que integraba datos de inteligencia en tiempo real. Un ejemplo notable fue el uso de drones Bayraktar TB2, cuya efectividad dependía de redes estables para transmitir imágenes y coordenadas. Sin embargo, el impacto estratégico no estuvo exento de controversias. En septiembre de 2022, las fuerzas ucranianas planearon un ataque con drones submarinos contra la flota rusa en Sebastopol, Crimea, y utilizaron Starlink para la navegación y el control remoto (Isaacson, 2023). Musk, alertado sobre el riesgo de una respuesta rusa que podría incluir represalias nucleares, decidió desactivar temporalmente el servicio en la zona, lo que hizo que se cancelara la operación. Esta decisión, aunque evitó una escalada potencial, generó críticas en Ucrania, donde se interpretó como una injerencia indebida de un actor privado en decisiones militares.

Dilemas éticos: innovación vs. responsabilidad

El caso de Starlink plantea dilemas éticos fundamentales sobre el rol de las empresas tecnológicas en conflictos armados. Desde la perspectiva de la ética digital, Floridi (2014) argumenta que los innovadores deben anticipar las consecuencias no intencionadas de sus productos. Starlink, diseñado para conectar comunidades remotas, se convirtió en una herramienta militar sin que SpaceX tuviera protocolos claros para gestionar su uso en guerras. La intervención inicial de Musk fue humanitaria (restaurar comunicaciones), pero su posterior decisión de limitar el servicio en Crimea reflejó el principio de doble efecto: una tecnología benéfica puede generar riesgos catastróficos (Walzer, 2006). Además, a partir de la acción unilateral de Musk, surgen preguntas sobre la legitimidad. ¿Quién debería decidir el uso de tecnologías duales en conflictos?, ¿los Estados, las empresas o la comunidad internacional? La falta de regulación global permitió a SpaceX operar en un vacío normativo, lo que indica la necesidad de marcos legales que equilibren innovación y responsabilidad (Nye, 2017). En este sentido, el caso también expone la asimetría entre actores privados y Estados, ya que las decisiones de una empresa pueden alterar el curso de una guerra.

Starshield: una respuesta parcial

En respuesta a estas controversias, SpaceX creó Starshield, una división dedicada a aplicaciones militares de la tecnología satelital, operada bajo contratos con el gobierno estadounidense. Starshield ofrece servicios de observación terrestre, comunicaciones seguras y carga útil personalizada, y delega la responsabilidad de su uso al Pentágono (SpaceX, 2023). Esta medida buscó mitigar los riesgos éticos al transferir el control a un actor estatal, pero no resuelve el problema de fondo: las empresas tecnológicas siguen siendo

indispensables en la guerra moderna, lo que plantea desafíos para la gobernanza global.

Implicaciones globales: privatización y asimetrías

El caso de Starlink ilustra la creciente privatización de la defensa, un fenómeno que Singer describe como una “revolución tecnológica” en la guerra. La dependencia de Estados —incluso potencias como Ucrania o sus aliados— de empresas privadas introduce vulnerabilidades. Por ejemplo, la decisión de Musk de limitar Starlink en Crimea podría replicarse en otros conflictos, lo cual afectaría la soberanía de los Estados clientes. Además, la hegemonía tecnológica de empresas estadounidenses refuerza las asimetrías globales, ya que los países del sur global tienen menos acceso a estas capacidades (Calle, 2020). A nivel geopolítico, el caso destaca la necesidad de cooperación internacional para regular tecnologías duales. Organismos como la ONU han propuesto tratados para limitar el uso militar de satélites, pero los avances son lentos debido a las rivalidades entre potencias (UNODA, 2021). Mientras tanto, la proliferación de constelaciones satelitales como Starlink, OneWeb o Kuiper aumenta el riesgo de congestión orbital y conflictos en el espacio, un dominio estratégico para la defensa moderna.

Perspectiva argentina: ciberdefensa y soberanía tecnológica

Para Argentina, el caso de Starlink ofrece lecciones críticas en el marco de la Ley de Defensa Nacional (1988), que prioriza la protección de la soberanía, los recursos naturales y los espacios estratégicos. La ciberdefensa es una prioridad emergente debido al aumento de ataques a infraestructuras críticas en América Latina, como el caso del hackeo a la

empresa estatal YPF en 2022 (*Clarín*, 2022). La conectividad satelital, como la ofrecida por Starlink, podría fortalecer la vigilancia marítima en el Atlántico Sur, especialmente en áreas sensibles como las Islas Malvinas, donde la pesca ilegal y las tensiones geopolíticas persisten (Bertotto, 2021). Sin embargo, la dependencia de tecnologías extranjeras supone riesgos para la autonomía estratégica. Argentina ha invertido en capacidades propias, como los satélites SAOCOM de INVAP y la red de ARSAT, pero estas no alcanzan la escala de Starlink. El caso ucraniano sugiere que la adopción de tecnologías duales requiere marcos regulatorios claros para evitar injerencias externas, como la decisión de Musk en Crimea. En este sentido, Argentina podría liderar iniciativas regionales en MERCOSUR para establecer normas sobre el uso militar de satélites; de esta manera, se fortalecería la cooperación en ciberdefensa (Calle, 2020). Además, el caso muestra la importancia de la formación en ciberdefensa. La Universidad de la Defensa Nacional y el Comando Conjunto de Ciberdefensa han avanzado en la capacitación de personal, pero se necesitan mayores inversiones para cerrar la brecha tecnológica con potencias globales. Finalmente, el Atlántico Sur, un área de interés estratégico, requiere una estrategia integral que combine conectividad satelital, inteligencia artificial y cooperación internacional para proteger sus recursos naturales y garantizar la seguridad regional.

Conclusiones

El caso de Starlink en el conflicto Rusia-Ucrania de 2022 ilustra el potencial transformador y los riesgos inherentes a la convergencia entre tecnología comercial y defensa. La intervención de SpaceX, liderada por Elon Musk, demostró cómo una red de satélites diseñada para conectar comunidades remotas puede convertirse en un activo estratégico en la guerra moderna. Al restaurar las comunicaciones ucranianas tras ciberataques rusos, Starlink salvó vidas y fortaleció

la resistencia nacional, pero su uso en operaciones militares, como el frustrado ataque en Crimea, reveló dilemas éticos y estratégicos que trascienden el ámbito tecnológico (Isaacson, 2023). En este artículo, se analizaron estas dinámicas con foco en la tensión entre innovación y responsabilidad, mientras que se extrajeron lecciones para la seguridad global y la defensa argentina. Desde una perspectiva teórica, el caso confirma las tesis de Singer sobre la privatización de la defensa. Empresas como SpaceX no solo complementan las capacidades estatales, sino que influyen directamente en el curso de los conflictos e introducen asimetrías de poder y vulnerabilidades. La decisión unilateral de Musk de limitar Starlink en Crimea evidenció la falta de marcos normativos para regular el uso de tecnologías duales, un problema que Floridi (2014) identifica como central en la ética digital. La creación de Starshield, aunque pragmática, no resuelve de fondo el siguiente desafío: las empresas tecnológicas operan en un vacío regulatorio que permite decisiones con impacto geopolítico sin rendición de cuentas. A nivel estratégico, Starlink destacó la importancia de la ciberdefensa en la guerra híbrida. La conectividad satelital, combinada con inteligencia en tiempo real, potenció las operaciones ucranianas, pero también expuso los riesgos de depender de actores privados. Para países con recursos limitados, como los del sur global, esta dependencia plantea un dilema: adoptar tecnologías extranjeras para cerrar brechas digitales o priorizar la autonomía a costa de un desarrollo más lento (Calle, 2020). La experiencia ucraniana sugiere que la resiliencia digital requiere una combinación de infraestructura propia, alianzas internacionales y formación especializada.

Para Argentina, el caso de Starlink ofrece lecciones críticas en el marco de la Ley de Defensa Nacional (1988), que prioriza la protección de la soberanía y los espacios estratégicos. La ciberdefensa es una necesidad urgente debido al aumento de ataques a infraestructuras críticas en América Latina. La conectividad satelital podría fortalecer la vigilancia del Atlántico Sur, un área clave para proteger los recursos natura-

les y contrarrestar actividades ilícitas, como la pesca ilegal en las Islas Malvinas (Bertotto, 2021). Sin embargo, depender de sistemas como Starlink implicaría riesgos de injerencia externa, como se vio en Crimea. Por ello, Argentina debe acelerar el desarrollo de capacidades propias, como los satélites SAOCOM de INVAP y la red de ARSAT, mientras fortalece su Comando Conjunto de Ciberdefensa.

El caso también subraya la importancia de la cooperación regional. En un contexto de asimetrías tecnológicas, Argentina podría liderar iniciativas en MERCOSUR para establecer normas sobre el uso de tecnologías duales y, de esta manera, promover una ciberdefensa colectiva que reduzca la dependencia de potencias extrarregionales. Asimismo, la formación de civiles y militares en ciberseguridad, a través de instituciones como la UNDEF, es esencial para cerrar la brecha tecnológica y garantizar la soberanía digital.

En el ámbito global, el caso de Starlink resalta la necesidad de marcos regulatorios internacionales. Organismos como la ONU han intentado limitar la militarización del espacio, pero las rivalidades entre potencias frenan el progreso (UNODA, 2021). Un tratado sobre tecnologías duales debería equilibrar el acceso equitativo a la innovación con medidas para prevenir escaladas bélicas. Mientras tanto, los Estados deben diversificar sus proveedores tecnológicos y fomentar la competencia para evitar que haya monopolios privados en capacidades estratégicas.

En conclusión, Starlink representa un punto de inflexión en la relación entre tecnología y defensa. Su capacidad para transformar conflictos coexiste con riesgos éticos y geopolíticos que exigen una reflexión cuidadosa. Para Argentina, el desafío es aprovechar las oportunidades de la innovación sin comprometer la autonomía estratégica. Las recomendaciones son las siguientes:

- Fortalecer la ciberdefensa nacional mediante inversiones en infraestructura digital y formación especializada.

- Promover la soberanía tecnológica a través de empresas como INVAP y ARSAT para reducir la dependencia de sistemas extranjeros.
- Liderar la cooperación regional en ciberdefensa mediante el establecimiento de normas para tecnologías duales en foros como MERCOSUR.
- Abogar por regulaciones globales que equilibren innovación y seguridad, y apoyar iniciativas en la ONU.

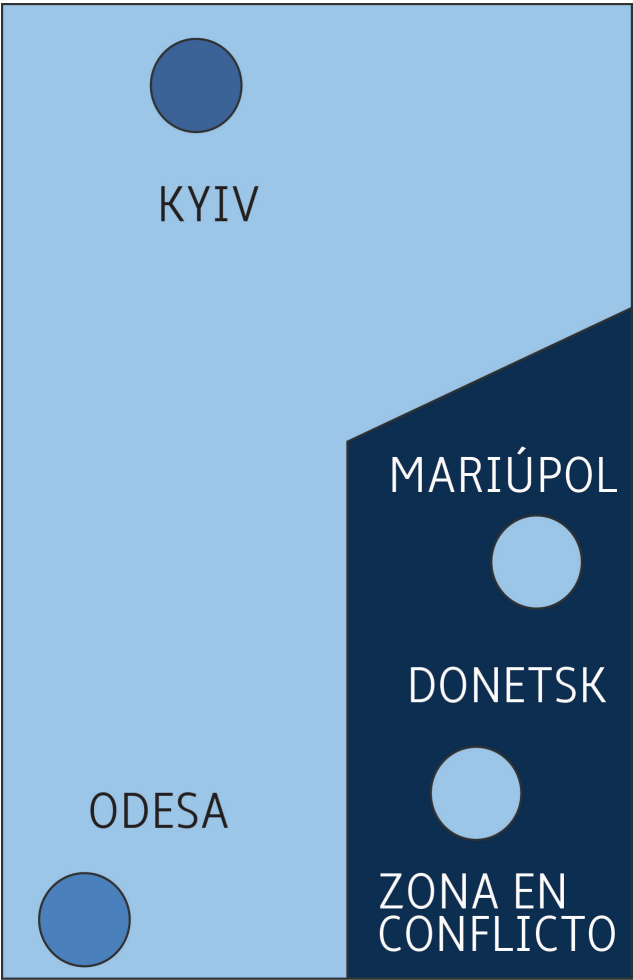
El futuro de la defensa dependerá de la capacidad de los Estados para integrar tecnologías emergentes con principios éticos y estrategias soberanas. El caso de Starlink es un testimonio de que la innovación sin una regulación específica puede convertirse en un arma de doble filo.

Comparación de ciberataques en conflictos recientes

CONFLICTO	AÑO	ACTOR PRINCIPAL	OBJETIVO	IMPACTO
Estonia	2007	Rusia (atribuido)	Infraestructura gubernamental	Paralización de servicios digitales
Georgia	2008	Rusia (atribuido)	Redes de comunicación	Descoordinación militar y civil
Ucrania	2022	Rusia (Sandworm)	Comunicaciones civiles y militares	Colapso de redes; mitigado por Starlink

Fuente: elaboración propia con base en Greenberg (2022) y Buchanan (2020).

Cobertura de Starlink en Ucrania (2022)



Mapa esquemático en blanco y negro que muestra las áreas de Ucrania con conectividad satelital de Starlink entre febrero y diciembre de 2022; se destacan regiones clave como Kiev, Mariúpol y Donetsk. Fuente: elaboración propia con base en *The Washington Post* (2022) y SpaceX (2023).

Bibliografía

Bertotto, J. (2021). *El Atlántico Sur como espacio estratégico: desafíos para la defensa argentina*. UNDEF Libros.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Calle, F. (2020). Ciberseguridad y defensa en América Latina: Desafíos para el siglo XXI. *Revista de relaciones internacionales*, 45(3), 89-112.

Clarín. (2022). Ciberataque a YPF: cómo se gestó el hackeo que afectó a la petrolera estatal.

Floridi, L. (2014). *The Ethics of Information*. Oxford University Press.

Greenberg, A. (2022). *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. Doubleday.

Isaacson, W. (2023). *Elon Musk*. Simon & Schuster.

Ley 23554 de 1988. Ley de Defensa Nacional. 26 de abril de 1988.

Nye, J. S. (2017). *The Future of Power*. Oxford University Press.

Singer, P. W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguin.

SpaceX. (2023). Starshield: Secure Space Solutions for Government. Recuperado de <https://www.spacex.com/starshield>

shield.

The Washington Post. (2022). How Starlink became Ukraine's lifeline in the war against Russia.

United Nations Office for Disarmament Affairs (UNODA). (2021). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace*.

Walzer, M. (2006). *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. Basic Books.

Waltz, K. (1979). *Theory of International Politics*. McGraw-Hill.

Wendt, A. (1992). Anarchy Is What States Make of It: The Social Construction of Power Politics. *International Organization*, 46(2), 391-425.