



Facultad
Militar
Conjunta

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Edición: Bib Alejandra Castillo



ISSN: 2718-6245

<https://undef.edu.ar/fmc/ciberespacio/boletines.php>

AÑO 8 N°57

Septiembre/Octubre
2025

OAC Boletín N° 57 – SEPTIEMBRE/OCTUBRE 2025

- 1) Un robot no debe dañar a un humano ni dejar que un humano sufra daño por no actuar,
- 2) Un robot debe seguir las órdenes humanas, siempre y cuando no contravengan la primera ley, y
- 3) Un robot debe proteger su existencia siempre que no vaya en contra de las dos primeras leyes.

Isaac Asimov (Círculo Vicioso, 1942)

Tabla de Contenidos

ESTRATEGIA	3
• La batalla cognitiva del engaño	3
• Una estrategia de ciber estrategia para el Reino Unido	3
• La IA general estaría próxima a estar entre nosotros	3
CIBERGUERRA	4
• Ciber guerra e IA en el conflicto Irán-Israel	4
• La IA y el impacto sobre las tecnologías de operación	5
• La ciber guerra empleando IA desde el sector privado	5
• IA militarizada y el futuro de la guerra autónoma	5
• Las Operaciones Multidominio y los efectos no letales	5
CIBERSEGURIDAD	6
• La ciber seguridad y la falta de talentos	6
• El costo de la IA en la seguridad nacional de EE.UU:	6
CIBERDEFENSA	7
• La IA está a punto de alterar radicalmente las estructuras de mando militar	7
• La IA introduce cambios radicales en los sistemas de Comando y Control	7
CIBERCONFIANZA	7



• Albania tiene una IA con nivel de ministro.....	7
• La IA plantea un punto de inflexión en la era del comercio electrónico	8
TECNOLOGÍA.....	8
• Avances en las interfaces cerebro computadoras.....	8
• Láser para enriquecimiento de uranio.....	9
• El arte en la guerra irregular; el poder de los simbólico	9
CIBERFORENSIA.....	10
Informes de Vulnerabilidades	9
Video y lecturas recomendadas	10

El Observatorio Argentino del Ciberespacio (OAC), es un micro-sitio de la
Facultad Militar Conjunta de las Fuerzas Armadas,
editado y publicado por el Instituto de Ciberdefensa de las Fuerzas Armadas
URL: <https://undef.edu.ar/fmc/ciberespacio/boletines.php>

Esta publicación mensual se encuentra inserta en el
Nodo Territorial de Defensa y Seguridad de la Red Nacional de
Nodos Territoriales (NT) de Vigilancia Tecnológica e Inteligencia Estratégica (VTeIE) del
Ministerio de Ciencia, Tecnología e Innovación de la Nación y es
administrado por el Centro de Estudios de Prospectiva Tecnológica Militar
“Grl Mosconi” de la Facultad de Ingeniería del Ejército Argentino.
Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial
distintas perspectivas de este nuevo ambiente operacional,
aportando novedades, reportes e informes que permitan a la comunidad educativa
y a la sociedad en general conocer más acerca del mismo.

ESTRATEGIA

La batalla cognitiva la dialéctica del engaño

Imagine un sistema de IA que analiza el historial de redes sociales de un soldado desplegado y su esposa. En cuestión de segundos, identifica una vulnerabilidad a los celos y la violencia. Con un coste insignificante, genera un video deepfake de infidelidad conyugal y lo envía al dispositivo del soldado. Una hora después, el soldado —un veterano combatiente— queda psicológicamente neutralizado, impulsado a cometer un acto personal catastrófico. Este escalofriante escenario captura el nuevo campo de batalla del siglo XXI: la mente humana. El centro de gravedad ya no son las flotas ni las fábricas, sino la comprensión compartida de la propia realidad. El centro de gravedad ya no son las flotas ni las fábricas, sino la comprensión compartida de la propia realidad.

<https://warontherocks.com/2025/09/the-dialectic-of-deception-john-boyd-and-the-cognitive-battlefield/>



<https://smallwarsjournal.com/2025/01/22/the-challenge-of-ai-enhanced-cognitive-warfare-a-call-to-arms-for-a-cognitive-defense/>

<https://www.act.nato.int/article/cogwar-concept/>

<https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/>

Una estrategia de ciber estrategia para el Reino Unido

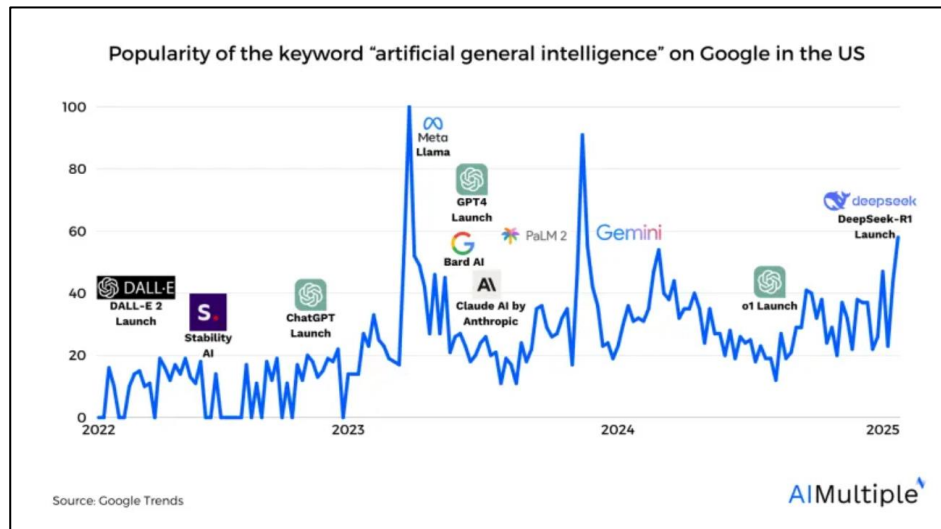
El gobierno del Reino Unido publicaría una nueva Estrategia Cibernética Nacional antes de finales de 2025, la última es el año 2022 (cuyo link también se agrega en este módulo). El artículo es parte de un proyecto de investigación en curso sobre la estrategia cibernética del Reino Unido, del grupo de investigación *Cyber and Tech de RUSI*, que reunió a seis expertos de la industria y la sociedad civil para ofrecer sus perspectivas sobre los temas e intervenciones clave que el gobierno del Reino Unido debería considerar.

<https://www.rusi.org/explore-our-research/publications/commentary/perspectives-next-uk-national-cyber-strategy>

<https://assets.publishing.service.gov.uk/media/620131fdd3bf7f78e469ce00/national-cyber-strategy-amend.pdf>

La IA general estaría próxima a estar entre nosotros

A principios de agosto, un día antes del lanzamiento de GPT-5, el director ejecutivo de OpenAI, Sam Altman, publicó una imagen de la Estrella de la Muerte en redes sociales. Era la última declaración de Altman de que su nuevo modelo de IA cambiaría el mundo para siempre. «Hemos descubierto, inventado, como quieran llamarlo, algo extraordinario que va a redefinir el curso de la historia de la humanidad», declaró Altman en una entrevista en julio. Comparó la investigación de su empresa con el Proyecto Manhattan y se sintió «inútil» en comparación con el nuevo invento de OpenAI. En otras palabras, Altman sugirió que GPT-5 acercaría a la sociedad a lo que los informáticos llaman inteligencia artificial general: un sistema de IA capaz de igualar o superar la cognición humana, incluyendo la capacidad de aprender cosas nuevas. Durante años, la creación de IA general ha sido el santo grial de muchos investigadores líderes en IA. Altman y otros tecnólogos de renombre, como Dario Amodei, director ejecutivo de Anthropic, y los profesores de informática Yoshua Bengio y Stuart Russell, llevan décadas soñando con construir sistemas superinteligentes, aunque también temiéndolos. Y recientemente, muchas de estas voces han declarado que el día del juicio final está cerca, advirtiendo a los funcionarios gubernamentales que el país que invente primero la IA general obtendrá enormes ventajas geopolíticas. Días antes de la segunda investidura del presidente estadounidense Donald Trump, por ejemplo, Altman le dijo a Trump que la IA general se lograría durante su mandato y que Washington necesitaba prepararse.



<https://www.foreignaffairs.com/united-states/cost-delusion-artificial-general-intelligence>

<https://www.foreignaffairs.com/tags/artificial-intelligence>

<https://research.aimultiple.com/artificial-general-intelligence-singularity-timing/>

[https://www.reddit.com/r/singularity/comments/142xwaz/on a 110 scale how likely is agi by 2030/](https://www.reddit.com/r/singularity/comments/142xwaz/on_a_110_scale_how_likely_is_agi_by_2030/)

CIBERGUERRA

Ciberguerra e IA en el conflicto Irán -Israel

En junio de 2025, Israel e Irán se enfrentaron en un breve pero intenso conflicto de 12 días, que incluyó diversas operaciones cibernéticas. Estos enfrentamientos cibernéticos constituyen un caso práctico convincente para examinar cómo la inteligencia artificial (IA) puede potenciar las estrategias asimétricas de ciberguerra, en particular las dirigidas contra infraestructuras civiles vulnerables.

La integración de tecnologías de IA en las operaciones cibernéticas promete mejorar significativamente la eficacia de las estrategias asimétricas. La IA facilita la automatización, la escalabilidad y la sofisticación en operaciones ofensivas como campañas de desinformación, ingeniería social y la disrupción de infraestructura civil. Por lo tanto, los objetivos civiles más vulnerables, con ciberdefensas menos formidables, se enfrentan a mayores riesgos por parte de actores asimétricos potenciados por la IA.

<https://trendsresearch.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/>

<https://www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/>

La IA y el impacto sobre las tecnologías de operación

La inteligencia artificial (IA) está acelerando el ritmo y la escala de las amenazas ciberfísicas; la tecnología de operación (TO) obsoleta proporciona una superficie de ataque vulnerable que las redes terroristas y criminales pueden explotar con mayor rapidez que la capacidad de respuesta de los defensores. Las vulnerabilidades documentadas públicamente, junto con el reconocimiento y la generación de exploits basados en la IA, crean



una hidra de atacantes y vectores de infección que se retroalimenta. Este artículo, parte de un análisis continuo de las implicaciones del doble uso de la IA, describe la intersección entre la TO tradicional, la innovación adversaria y los mercados ilícitos, y describe medidas prácticas en materia de políticas de IA, inversión en infraestructura, preparación de la fuerza laboral y diseño de sistemas para prevenir fallos en cascada en infraestructuras críticas.

<https://cybertlabs.com/risks-of-ai-in-operational-technology/>

<https://smallwarsjournal.com/2025/09/01/ai-and-the-hydra-effect-securing-outdated-ot-before-the-threat-swarm-arrives/>

<https://www.paloaltonetworks.com/blog/2024/08/ai-in-ot-security/>

La ciberguerra empleando IA desde el sector privado

En un estudio publicado en enero del año pasado, investigadores de la Universidad Jiao Tong de Shanghái mostraron cómo se podría utilizar la inteligencia artificial para desplegar sistemas de armas en “redes de exterminio” automatizadas que se ajustarían en tiempo real a los cambios en el campo de batalla durante el combate en el mar.

<https://www.wsj.com/world/china/china-military-ai-partners-7836a2bc?mod=WhatsApp>

<https://thechinabriefing.substack.com/p/briefing-chinas-growing-use-of-artificial>

<https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap>

IA militarizada y el futuro de la guerra autónoma

Las industrias de defensa contemporáneas están adoptando rápidamente la inteligencia artificial (IA) con fines estratégicos y operativos. Desde drones autónomos que realizan objetivos de forma independiente hasta herramientas de apoyo a la toma de decisiones que recopilan grandes cantidades de datos del campo de batalla, la IA está transformando la forma en que se planifican y libran las guerras. Las fuerzas armadas de los países tecnológicamente avanzados están integrando la IA en funciones críticas de vigilancia, logística, ciberseguridad y sistemas de mando. Entre las innovaciones más debatidas se encuentran los sistemas de armas autónomas letales (LAWS), los programas de predicción de objetivos y las herramientas de coordinación basadas en algoritmos de aprendizaje. Si bien estas herramientas ofrecen beneficios estratégicos, también plantean inquietudes éticas y sociales.

<https://trendsresearch.org/insight/the-backlash-against-military-ai-public-sentiment-ethical-tensions-and-the-future-of-autonomous-warfare/>

<https://warroom.armywarcollege.edu/articles/ais-growing-role/>



Las Operaciones Multidominio y los efectos no letales

Los campos de batalla modernos se ven condicionados por la saturación de datos, la complejidad multidominio y la convergencia cada vez mayor de efectos en las dimensiones físicas, informativas y humanas. Si bien los sensores avanzados y la IA prometen una toma de decisiones rápida, los comandantes a menudo se enfrentan a flujos de datos fragmentados, procesos de personal estancos y fuegos mal integrados. Esto va más allá de un problema técnico: debilita el mando de la misión al limitar la forma en que los líderes orquestan el ritmo y aprovechan las oportunidades. Por lo tanto, sincronizar las Operaciones Multidominio (MDO) con efectos no letales (NLE) y actividades no cinéticas (NKA) no es solo una innovación, sino una necesidad operativa. Si se implementa correctamente, esta integración restaura el margen de decisión de los comandantes, crea ventaja de información (IA) y obliga a los adversarios a enfrentarse a dilemas que no pueden resolver fácilmente.

<https://smallwarsjournal.com/2025/09/25/synchronizing-multi-domain-operations-non-lethal-effects/>

<https://www.japcc.org/articles/non-lethal-measures-of-effectiveness-in-targeting/>

CIBERSEGURIDAD

La ciberseguridad y la falta de talentos

Europa encara un momento crítico en materia de ciberseguridad, así lo refleja el último informe State of Cybersecurity 2025 de ISACA, donde se revela que dos de cada tres empresas en la región siguen teniendo dificultades para cubrir puestos clave en este ámbito, limitando su capacidad de defensa frente a un panorama de amenazas cada vez más complejo.

El desajuste entre la rapidez con la que avanzan los ciberataques y el ritmo al que las organizaciones logran reforzar sus equipos sitúa a muchas compañías en una posición muy frágil.

<https://revistabyte.es/actualidad-it/ciberseguridad-europa-talento/>

<https://revistabyte.es/actualidad-it/ciberamenazas-comunes/>

<https://www.isaca.org/>

El costo de la IA en la seguridad nacional de EE.UU:

Las herramientas de IA están transformando la forma en que los estadounidenses aprenden, trabajan y resuelven problemas. Estas herramientas abarcan un amplio espectro, desde el aprendizaje automático y el procesamiento del lenguaje natural que impulsan a Siri en los iPhones, hasta importantes iniciativas de defensa como el Proyecto Maven, que genera rápidamente listas de objetivos mediante la síntesis de inteligencia y una gran variedad de datos. Sin embargo, un subconjunto de estas herramientas —la IA generativa, como los chatbots y los grandes modelos lingüísticos (LLM), anunciados como apoyo para la investigación y la escritura— conlleva un riesgo particular que repercute profundamente en el personal de seguridad nacional estadounidense, cuyas decisiones pueden tener consecuencias de vida o muerte. El uso regular de programas de IA generativa puede erosionar muchas de las habilidades cognitivas de las que depende la seguridad



estadounidense. A menos que los responsables políticos actúen, las mismas herramientas que se promocionan como potenciadores de la eficiencia podrían socavar la capacidad de los profesionales de la seguridad nacional para pensar críticamente, responder con rapidez y superar en maniobras a los adversarios. Considerando la aversión al riesgo que suele presentar el sector de la seguridad nacional, esta es una consecuencia que vale la pena reconocer y abordar.

<https://www.justsecurity.org/121289/ai-hidden-national-security-cost/>

<https://spacenews.com/pentagon-boosts-budget-for-palantirs-ai-software-in-major-expansion-of-project-maven/>

<https://spacenews.com/geospatial-intelligence-gets-smart/>

CIBERDEFENSA

La IA está a punto de alterar radicalmente las estructuras de mando militar

A pesar de dos siglos de evolución, la estructura de un estado mayor militar moderno sería reconocible para Napoleón. Al mismo tiempo, las organizaciones militares han luchado por incorporar nuevas tecnologías a medida que se adaptan a los nuevos dominios —aire, espacio e información— de la guerra moderna. Los agentes de IA (software autónomo y orientado a objetivos, impulsado por amplios modelos de lenguaje) pueden automatizar las tareas rutinarias del personal, acortar los plazos de toma de decisiones y habilitar puestos de mando más pequeños y resilientes. Pueden reducir la plantilla y, al mismo tiempo, aumentar su eficacia.

<https://theconversation.com/ai-is-about-to-radically-alter-military-command-structures-that-havent-changed-much-since-napoleons-army-262200>

<https://press.georgetown.edu/Book/Information-in-War>

<https://warontherocks.com/2025/04/agent-warfare-is-here-will-america-be-the-first-mover/>

La IA introduce cambios radicales en los sistemas de Comando y Control

El ciberespacio se encuentra en constante disputa, ya que actores maliciosos buscan cada vez más desestabilizar la sociedad mediante actividades y campañas cibernéticas maliciosas. Los adversarios potenciales buscan degradar la infraestructura crítica, interferir los servicios gubernamentales, extraer información de inteligencia, robar propiedad intelectual e impedir actividades militares. La guerra de agresión de Rusia contra Ucrania ha puesto de manifiesto hasta qué punto las actividades cibernéticas son una característica de los conflictos modernos.

<https://smallwarsjournal.com/2025/09/24/cyber-warfare-command-and-control-analogue/>

<https://sloanreview.mit.edu/article/genai-tools-and-decision-making-beware-a-new-control-trap/>



<https://www.microsoft.com/en-us/industry/blog/government/2023/06/20/enhance-command-and-control-with-ai-and-machine-learning/>

<https://www.militaryaerospace.com/computers/article/14305991/artificial-intelligence-ai-machine-learning-command-and-control>

CIBERCONFIANZA

Albania tiene una IA con nivel de ministro

Mientras otros líderes mundiales debaten sobre la regulación de la IA, Albania acaba de hacer historia al implementar un sistema de IA directamente en el gobierno, con poder de decisión a nivel de gabinete. Con "Diella" controlando ahora los contratos gubernamentales del país, ¿será este el futuro de un gobierno libre de corrupción o un desastre de ciberseguridad a punto de ocurrir?

<https://www.euronews.com/next/2025/09/12/albania-appoints-worlds-first-ai-government-minister-to-root-out-corruption>

<https://www.reuters.com/technology/albania-appoints-ai-bot-minister-tackle-corruption-2025-09-11/>

<https://www.theguardian.com/world/2025/sep/11/albania-diella-ai-minister-public-procurement>

La IA plantea un punto de inflexión en la era del comercio electrónico

La forma en que compramos en línea está cambiando rápidamente. En lugar de simplemente escribir unas palabras en una barra de búsqueda y filtrar anuncios, millones de nosotros ahora simplemente *pedimos* recomendaciones a una IA. Este cambio de la búsqueda al chat es la idea detrás de una nueva y enorme tendencia: el comercio electrónico ChatGPT, para ello OpenAI acaba de implementar la compra directa dentro de ChatGPT para usuarios de EE. UU., lo que permite a los compradores completar transacciones sin salir de la interfaz de conversación a través de una nueva función llamada "Pago instantáneo". La empresa se asoció con Stripe para crear el sistema, que inicialmente brindó soporte a vendedores de Etsy y pronto estará disponible para más de 1 millón de comerciantes de Shopify. Los usuarios podrán hacer clic en el botón "Comprar" después de que ChatGPT sugiera productos, luego revisar los detalles del pedido y pagar en el chat. OAI convirtió en código abierto el protocolo de comercio Agentic subyacente, lo que permite que cualquier minorista lo integre (los comerciantes de Stripe solo necesitan cambios de código mínimos). **Esta nueva modalidad sugiere un punto de inflexión para la transición a la era del comercio con IA**

https://openai.com/index/buy-it-in-chatgpt/?utm_source=www.therundown.ai&utm_medium=newsletter&utm_campaign=openai-s-e-commerce-takeover&_bhlid=8e266e67a00d9dedcd31a7a38c9e52903883ada3

<https://www.eesel.ai/blog/chatgpt-ecommerce>

<https://togrowagencia.com/chatgpt-en-el-e-commerce-personalizacion-negocio/>



TECNOLOGÍA

Avances en las interfases cerebro computadora

Los ingenieros de UCLA han desarrollado un sistema de interfaz cerebro-computadora portátil y no invasivo que utiliza inteligencia artificial como copiloto para ayudar a inferir la intención del usuario y completar tareas moviendo un brazo robótico o un cursor de computadora. Las interfaces cerebro-computadora (BCI) motoras decodifican señales neuronales para ayudar a las personas con parálisis a moverse y comunicarse. A pesar de los importantes avances de las últimas dos décadas, las BCI se enfrentan a un obstáculo clave para su viabilidad clínica: su rendimiento debería superar con creces los costes y riesgos. Para aumentar significativamente el rendimiento de las BCI, utilizamos la autonomía compartida, donde *copilot* de inteligencia artificial (IA) colaboran con los usuarios de las BCI para alcanzar los objetivos de la tarea.

<https://www.nature.com/articles/s42256-025-01090-y>

https://www.eurekalert.org/news-releases/1096148?utm_source=www.therundown.ai&utm_medium=newsletter&utm_campaign=ai-gives-paralyzed-patients-robotic-control&bhlid=4d8af00e7c3f9b72cd0881eb5706705deabaeab4

Láser para enriquecimiento de uranio

Una empresa estadounidense prueba un potente láser para enriquecer uranio y obtener energía nuclear sin límites. La campaña de pruebas se llevó a cabo en las instalaciones de Test Loop de GLE en Wilmington, Carolina del Norte. Las pruebas de demostración del proceso de enriquecimiento láser SILEX comenzaron en mayo de este año. El programa continuará durante el resto de 2025 y producirá cientos de libras de uranio poco enriquecido (LEU). También seguirá ayudando a construir una base de fabricación local y una cadena de suministro para las instalaciones de enriquecimiento locales.

https://interestingengineering.com/energy/united-states-laser-uranium-enrichment?utm_campaign=13508169-The%20Blueprint%20Daily%20Subscription&utm_medium=email&hsenc=p2ANqtz-8LPj_E38-e4lqZ1eIHaS1rfGUhsEkRmuyuChioliifVmbFwsfTw7TDm_V97J8vz0IVJZL-hmo_un4OcWsZNMctY9jG8Q&hsmi=381187133&utm_content=381187133&utm_source=hs_email

El arte en la guerra irregular; el poder de lo simbólico

Estar ante *el Guernica* de Pablo Picasso en Gernika es más que contemplar una pintura; es experimentar un grito de angustia plasmado en óleo sobre lienzo. Creado en 1937 tras el bombardeo aéreo de la ciudad vasca por las fuerzas nazis e italianas aliadas con Franco, *el Guernica* trascendió sus orígenes españoles para convertirse en un emblema universal del sufrimiento civil y la brutalidad de la guerra total. Además, la insistencia de Picasso en que la pintura no fuera devuelta a España hasta que se restaurara la democracia ilustra cómo el arte puede convertirse en una herramienta de resistencia cognitiva prolongada.

<https://smallwarsjournal.com/2025/09/29/art-and-irregular-warfare-aesthetic-resistance-symbolic-power-and-the-battles-for-meaning/>



<https://www.swcs.mil/Special-Warfare-Journal/Article/3965910/the-three-pillars-of-irregular-warfare-education/>

CIBERFORENSIA

Informes de Vulnerabilidades

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EEUU, estos boletines proporcionan un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST).

2025

1. Vulnerabilidades semana del 1 de septiembre; <https://www.cisa.gov/news-events/bulletins/sb25-251>
2. Vulnerabilidades semana del 25 de agosto: <https://www.cisa.gov/news-events/bulletins/sb25-245>
3. Vulnerabilidades semana del 18 de agosto: <https://www.cisa.gov/news-events/bulletins/sb25-237>
4. Vulnerabilidades semana del 11 de agosto: <https://www.cisa.gov/news-events/bulletins/sb25-230>
5. Vulnerabilidades semana del 22 de septiembre: <https://www.cisa.gov/news-events/bulletins/sb25-272>
6. Vulnerabilidades semana del 15 de septiembre: <https://www.cisa.gov/news-events/bulletins/sb25-265>

Video recomendado

1. La verdad sobre la inteligencia artificial: <https://www.primevideo.com/-/es/detail/La-verdad-sobre-la-inteligencia-artificial/0P9GS9JT3WOGWV3A6L7HFW6NO>

Lecturas recomendadas

1. . "La inteligencia artificial en la geopolítica y los conflictos;" Cuaderno de Estrategia 226
<https://www.defensa.gob.es/ceseden/-/cuaderno-de-estrategia-226>
2. Auge de la IA en el ámbito militar y sus riesgos; Mario de Diego y Pablo Fernández
<https://www.unav.edu/web/global-affairs/auge-de-la-ia-en-el-ambito-militar-y-sus-riesgos>
3. La Ciberseguridad en la Era de Avances Tecnológicos: Desafíos, Vulnerabilidades y Estrategias para la Protección de Datos
https://www.academia.edu/keypass/V1p4Ry9iVkJZwUzkvdjR2NkhKbjFRRmc4QjViTUViQys4RVdzSWYya1pGTT0tLTaZOHPiYUFGc3JUaThRRk1RRjVIVmc9PQ===980d5431f282a7b54f119d9fcf0cc72bd5a3e52a/t/rPXRd-SvBienE-bxdQp7/resource/work/109063921/La_Ciberseguridad_en_la_Era_de_Avances_Tecnol%C3%B3gicos_De_saf%C3%ADos_Vulnerabilidades_y_Estrategias_para_la_Protecci%C3%B3n_de_Datos?email_work_card=title



**Facultad
Militar
Conjunta**



4. Operaciones en el Ambiente de la Información Libro en formato digital disponible en:

https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_b2ce737fe7427cb279d7cb6ef4bd53c8

5. Una respuesta a las amenazas en el ciberespacio:

https://www.academia.edu/102602502/Una_respuesta_a_las_amenazas_en_el_ciberespacio?email_work_card=view-paper

6. Economía de defensa, ciberseguridad y ciberdefensa

https://www.academia.edu/99051800/Econom%C3%ADa_de_defensa_ciberseguridad_y_ciberdefensa?email_work_card=view-paper

*Copyright © * / 2025 / **

** / Facultad Militar Conjunta / **

Todos los derechos reservados.

** / Observatorio Argentino del Ciberespacio / **

Sitio web: [http://](http://undef.edu.ar/fmc/ciberespacio/boletines.php) <https://undef.edu.ar/fmc/ciberespacio/boletines.php>

Nuestra dirección postal es:

** / Luis María Campos 480 - CABA - República Argentina / **

Nuestro correo electrónico:

** / observatorioargentinodelciberespacio@conjunta.undef.edu.ar / **
