



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 9 N°60

Marzo-Abril 2026

OAC Boletín NÚMERO 60 de abril de 2026

“Guerra cognitiva: Una guerra permanente y silenciosa dirigida contra cada persona”

<https://rebellion.org/guerra-cognitiva-una-guerra-permanente-y-silenciosa-dirigida-contra-cada-persona/>

Tabla de Contenidos

ESTRATEGIA.....	2
¿Hacia dónde se dirige la IA?	2
CIBERGUERRA.....	2
La revolución de la IA en el Ciberconflicto	2
El conflicto Iraní y la IA.....	3
La IA en el espacio	3
CIBERSEGURIDAD	4
El poder de las criptomoedas en la guerra.....	4
CIBERDEFENSA.....	4
CIBERCONFIANZA.....	5
Estadísticas acerca de lo que la gente espera de la IA.....	5
TECNOLOGÍA.....	5
La infraestructura de los datos para soportar IA.....	5
Brecha de infraestructuras de datos: centros de datos y preparación para la IA en Oriente Medio	5
El impacto de la IA en la toma de decisiones.....	6
CIBERFORENSIA.....	6
Informes de Vulnerabilidades	6
EVENTO 55 Jornadas Argentinas de Informática (JAIIO).....	7
Lecturas y Videos recomendadas.....	7
La empresa agente: cómo los agentes de IA están transformando los negocios con Adam Evans de Sale..	
https://www.youtube.com/watch?v=bsxrTa9YL3Y	8



Facultad
Militar
Conjunta



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

¿Hacia dónde se dirige la IA?

La inteligencia artificial deja de ser una mera experimentación para convertirse en un motor de reestructuración corporativa profunda. Según BCG (Boston Consulting Group) y el Foro Económico Mundial, el verdadero valor no está en automatizar tareas, sino en rediseñar los modelos de toma de decisiones, volviéndolos más descentralizados y continuos. La integración operativa a gran escala en flujos de trabajo diarios potencia resiliencia y productividad, como ya demuestran casos exitosos de colaboración humano-máquina en cadenas de suministro. El desafío ahora es cultural, operando con la guía de la evidencia numérica y fáctica, no solo de la corazonada, en tal caso, las empresas que asimilen la IA como capacidad nativa la convertirán en un diferenciador estratégico permanente.

<https://www.weforum.org/stories/2026/03/where-is-ai-moving-beyond-experimentation-leaders-scaling/>

<https://www.worldbank.org/en/publication/dptr2025-ai-foundations/report>

<https://www.bcg.com/publications/2026/the-corporate-strategy-function-in-an-ai-first-world>

CIBERGUERRA

La revolución de la IA en el Ciberconflicto

Los algoritmos ya detectan mentiras mejor que los polígrafos: analizan sudor, voz y gestos. Pero hay trampa: los datos reflejan poca diversidad cultural y lingüística. Otro problema más sutil: ¿cómo distinguir una mala intención real de un simple juego de roles sugerido por el usuario? Los expertos proponen mirar los procesos internos de la máquina y estudiar conductas en contextos reales. La tecnología avanza, pero el gran desafío



sigue siendo filosófico: atribuir creencias y metas a sistemas que solo imitan inteligencia. Detectar el engaño artificial puede ser la tarea más compleja y un verdadero desafío.

<https://www.lawfaremedia.org/article/the-ai-revolution-in-cyber-conflict>

<https://www.sciencedirect.com/science/article/abs/pii/S0957417425012230>

https://www.researchgate.net/publication/383950901_Cyber_Deception_State_of_the_art_Trends_and_Open_challenges

<https://arxiv.org/html/2511.22662v1>

El conflicto Iraní y la IA

La inteligencia artificial (IA) es fundamental en la guerra contra Irán. Por un lado, los ejércitos de Estados Unidos e Israel utilizan masivamente tecnologías de IA para combatir a Irán. Sin embargo, Irán responde atacando a los países del Golfo Pérsico. Irán ataca objetivos, entre otros, infraestructuras de IA, y amenaza directamente las oficinas y el personal de las empresas estadounidenses de IA. A mayor escala, las consecuencias económicas y energéticas de la guerra ponen en peligro el desarrollo mismo del sector de la IA.

La "Operación Epic Fury" no es solo un ejercicio de prospectiva para el año 2026; es una advertencia sobre un presente donde la Inteligencia Artificial ha dejado de ser una herramienta para convertirse en el epicentro de la soberanía y la estabilidad global.

En este escenario de alta intensidad, nos enfrentamos a un entorno informativo saturado de contenido sintético y *deepfakes* que desafían nuestra capacidad de distinguir la realidad de la ilusión estratégica.

<https://smallwarsjournal.com/2026/04/10/the-iran-war/>

<https://www.brookings.edu/articles/generative-ai-as-a-weapon-of-war-in-iran/>

<https://theconversation.com/iran-war-shows-how-ai-speeds-up-military-kill-chains-278492>

https://www.elconfidencial.com/tecnologia/novaceno/2026-03-21/guerra-iran-eeuu-israel-tecnologia-inteligencia-artificial-armas_4324311/

La IA en el espacio

La inteligencia artificial (IA) ha supuesto una revolución en todos los sectores de actividad y su aplicación en el sector espacial no es una excepción. Esta tecnología ya está contribuyendo a mejorar numerosos aspectos clave en el desarrollo de misiones espaciales.

El sector espacial evoluciona rápidamente incorporando las últimas tecnologías, para conectar a las personas, explorar el universo y contribuir a la seguridad y al cuidado de nuestro planeta de forma más eficiente y fiable.

La inteligencia artificial enfrenta desafíos únicos y complejos en el espacio. Los textos también exponen los desafíos técnicos del entorno, incluyendo la radiación cósmica, la latencia en las comunicaciones y la gestión de la basura espacial. Finalmente, se destaca la colaboración con el **sector privado** para desarrollar sistemas más eficientes que garanticen la seguridad y el éxito de futuras misiones tripuladas a la Luna y Marte.

<https://www.nasa.gov/artificial-intelligence/>

https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Artificial_intelligence_in_space



<https://www.arquimea.com/es/blog/retos-aplicaciones-ia-espacio/#content>

<https://orbitaltoday.com/2026/03/01/the-rise-of-ai-in-space-20-missions-projects-defining-the-next-era-of-exploration/>

CIBERSEGURIDAD

El poder de las criptomonedas en la guerra

Rusia e Irán utilizan criptomonedas para financiar la adquisición de drones militares y evadir sanciones internacionales. Según los informes, actores estatales y milicias pro-rusas han recaudado millones en activos digitales para comprar equipos directamente a fabricantes o mediante plataformas de comercio electrónico como Alibaba. Aunque el volumen es menor que en las finanzas tradicionales, el blockchain permite rastrear estas redes de suministro opacas. Irán incluso publicita armamento avanzado aceptando cripto para eludir sanciones. Esta infraestructura digital facilita una guerra asimétrica y accesible para actores sancionados.

<https://www.chainalysis.com/blog/cryptocurrency-drones-research/>

<https://www.benzinga.com/crypto/cryptocurrency/26/03/51557991/iran-russia-crypto-drone-purchases-ecommerce-opaque-identities-report>

CIBERDEFENSA

Aplicaciones IA en el campo ISR

La integración de la Inteligencia Artificial (IA) en operaciones de Inteligencia, Vigilancia y Reconocimiento (ISR) responde al crecimiento exponencial de datos ("big data"). Sistemas como Leonardo ATOS evidencian su impacto al optimizar el ciclo OODA (Observar, Orientar, Decidir, Actuar), procesando grandes volúmenes de información mediante redes neuronales. Esto mejora la conciencia situacional, reduce la carga cognitiva y disminuye la fatiga del operador. La IA funciona como un multiplicador de fuerza, permitiendo reducir hasta en un 95% el tiempo de análisis de imágenes satelitales. No obstante, presenta riesgos significativos, como el problema de la "caja negra", que limita la comprensión humana del razonamiento algorítmico, y la vulnerabilidad al "mal aprendizaje" por datos sesgados o ataques adversarios. En este contexto, se enfatiza la necesidad de un enfoque hombre-máquina que garantice control humano significativo, cumplimiento del Derecho Internacional Humanitario y adecuada rendición de cuentas.

https://www.researchgate.net/publication/394740589_AI-Powered_Intelligence_Surveillance_and_Reconnaissance_ISR_Systems_in_Defense

https://www.airuniversity.af.edu/Portals/10/ASPI/journals/Volume-35_Special_Issue/F-Cook.pdf

<https://www.karveinternational.com/insights/revolutionising-defence-intelligence-surveillance-reconnaissance-isr-with-ai>

<https://www.pucara.org/post/ia-aplicada-el-ejemplo-de-la-mejora-en-capacidades-isr-del-sistema-de-gesti%C3%B3n-de-misiones-leonardo>



CIBERCONFIANZA

Estadísticas acerca de lo que la gente espera de la IA

El debate público sobre la IA suele centrarse en proyecciones abstractas de sus riesgos y beneficios. Lo que falta en gran medida es una visión de lo que significa que la IA funcione bien, una visión basada en las aspiraciones concretas de las personas de todo el mundo que ya la utilizan y que han empezado a comprender lo que podría aportarles.

Así que preguntamos a nuestros usuarios sobre sus esperanzas y preocupaciones respecto a la IA, así como sobre cómo sus perspectivas se relacionan con sus experiencias reales con la tecnología. Durante una semana de diciembre, invitamos a todos los usuarios con una cuenta de Claude.AI a participar en una entrevista con Anthropic Interviewer —una versión de Claude diseñada para realizar una entrevista conversacional— y a compartir su visión sobre la IA. 80.508 personas, de 159 países y 70 idiomas, respondieron a la entrevista. Creemos que este es el estudio cualitativo más grande y multilingüe jamás realizado.

https://www.anthropic.com/features/81k-interviews?utm_source=www.therundown.ai&utm_medium=newsletter&utm_campaign=how-81k-people-really-feel-about-ai&bhlid=d4b3de28a60fae883edb46ed5f926453d4c59857

TECNOLOGÍA

La infraestructura de los datos para soportar IA

A medida que las empresas se apresuran a adoptar la IA con capacidad de gestión para impulsar la innovación y aumentar la eficiencia, la creación de la infraestructura de datos empresariales adecuada se ha convertido en un componente fundamental para el éxito. En la carrera por adoptar la IA y demostrar su valor, las empresas están avanzando más rápido que nunca para implementar IA con capacidad de agencia como copilotos, asistentes y ejecutores de tareas autónomos. A finales de 2025, casi dos tercios de las empresas estaban experimentando con agentes de IA, mientras que el 88 % utilizaba IA en al menos una función empresarial, frente al 78 % en 2024, según el informe anual de IA de McKinsey. Sin embargo, aunque los primeros proyectos piloto suelen tener éxito, solo una de cada diez empresas logró escalar sus agentes de IA.

El auge de la IA ha desatado una carrera tecnológica a nivel mundial, que se está acelerando en la región de Oriente Medio y Norte de África (MENA). El Consejo de Cooperación del Golfo (CCG) e Israel lideran la carrera tecnológica en comparación con sus vecinos regionales, desarrollando numerosos centros de datos para alcanzar sus objetivos tecnológicos. Sin embargo, la región en su conjunto se caracteriza por profundas desigualdades derivadas de las diferencias en recursos, desarrollo y gobernanza.

<https://www.technologyreview.com/2026/03/10/1134083/building-a-strong-data-infrastructure-for-ai-agent-success/>

<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>

Brecha de infraestructuras de datos: centros de datos y preparación para la IA en Oriente Medio

La brecha digital en el Medio Oriente en el contexto de la infraestructura para inteligencia artificial. Los países del Consejo de Cooperación del Golfo (CCG) e Israel dominan la infraestructura tecnológica regional, concentrando la mayoría de los centros de datos existentes.

El desarrollo está impulsado principalmente por inversores locales y organismos nacionales, con participación limitada de capital extranjero.



Existe una brecha profunda entre naciones con recursos abundantes y aquellas con déficits en gobernanza o desarrollo económico.

Los países menos favorecidos enfrentan el riesgo de quedar excluidos del ritmo de innovación global en IA.

La disponibilidad de infraestructura tecnológica se perfila como un factor determinante del futuro geopolítico y técnico de la región.

<https://www.iiss.org/charting-middle-east/2025/05/data-infrastructure-gap-data-centres-and-ai-preparedness-in-the-middle-east/>

El impacto de la IA en la toma de decisiones

Ángel Rojo presenta este interesante análisis en LinkedIn. El proyecto analiza el impacto de la inteligencia artificial en la toma de decisiones dentro de operaciones militares modernas, con énfasis en su integración en el ciclo Kill Chain. A través de estudios de caso y análisis cualitativo, examina cómo tecnologías como el aprendizaje automático y las redes neuronales permiten automatizar etapas clave: detección, seguimiento, selección de objetivos, ataque y evaluación.

Los resultados muestran que la IA reduce significativamente los tiempos de decisión, mejora la precisión y aumenta la adaptabilidad en entornos complejos. Un escenario con enjambres de drones autónomos ilustra estas ventajas, destacando su resiliencia frente a guerra electrónica y su capacidad de operar con mínima intervención humana.

https://www.linkedin.com/posts/angel-rojo-b4793927_analyzing-the-impact-of-ia-on-the-decision-making-activity-7444533929946243073-GnCc/?utm_medium=ios_app&rcm=ACoAAAg0UzEB-mZL7znKMI4zKJ8gCaFrjRCz38&utm_source=social_share_send&utm_campaign=mail

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).

Vulnerabilidades semana del 13 de abril: <https://www.cisa.gov/news-events/bulletins/sb26-110>

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) analizó una muestra de malware FIRESTARTER obtenida a partir de una investigación forense. CISA y el Centro Nacional de Ciberseguridad del Reino Unido (NCSC) evalúan que los actores de amenazas avanzadas persistentes (APT) están utilizando el malware FIRESTARTER para persistencia, dirigiéndose específicamente a dispositivos Cisco Firepower y Secure Firewall de acceso público que ejecutan software Adaptive Security Appliance (ASA) o Firepower Threat Defense (FTD). CISA y el NCSC están publicando este Informe de Análisis de Malware para compartir el análisis de una muestra de malware FIRESTARTER que funciona como puerta trasera y animar a las organizaciones a tomar acciones clave de respuesta.

<https://www.cisa.gov/news-events/analysis-reports/ar26-113a>



Facultad
Militar
Conjunta



EVENTO 55 Jornadas Argentinas de Informática (JAIIO)



CYBER.AR

I CONGRESO DE CIBERDEFENSA
ARGENTINA 2026

16, 17 y 18 DE SEPTIEMBRE

FECHAS IMPORTANTES

- 30 MARZO** Apertura
Call for Papers
- 8 JUNIO** Fecha límite de
envío de resúmenes
- 24 JUNIO** Comunicación de
aceptación de resúmenes
- 24 JULIO** Fecha límite de envío de
resúmenes extendidos y
de trabajos completos
- 21 AGOSTO** Notificación de
aceptación final
- 16 SEPTIEMBRE** Comienzo
Congreso

COMITÉ ORGANIZADOR

Presidente
General de Brigada (R) Ing. Anibal Luis Intini

Vicepresidente
Coronel (R) Ing. César Daniel Cicerchia

COMITÉ TÉCNICO CIENTÍFICO

Co-Presidente CTC
Dra. Ing. Lidia Ana Otero

Co-Presidente CTC
Capitán de Navío (R) Dr. Pablo Lucio Salonio

Secretario 1º CTC
Ing. Andrés Bursztyn

Secretario 2º CTC
Coronel Mg. Juan Carlos Guerra

Secretario 3º CTC
Dra. María Pilar Llorens

SIMPOSIOS ALCANCE TEMÁTICO

Simposio I - Capacidades Tecnológicas para la Ciberdefensa
Simposio II - Ciberoperaciones y Empleo de Capacidades en el Dominio Cibernético
Simposio III - Estrategia Nacional, Militar y Marco Jurídico de la Ciberdefensa

INFORMACIÓN ENLACES

- 
MODALIDAD
- 
RESUMEN
- 
ARANCELES



Lecturas y Videos recomendadas

1. Ciberestrategia de los EE.UU.
 - a. <https://www.whitehouse.gov/articles/2026/03/white-house-unveils-president-trumps-cyber-strategy-for-america/>
 - b. <https://www.congress.gov/crs-product/IN12667>
 - c. <https://www.insideprivacy.com/u-s-national-cybersecurity-strategy/white-house-releases-new-national-cyber-strategy-and-executive-order/>
 - d. <https://www.cpomagazine.com/cyber-security/new-cyber-strategy-for-america-plan-turns-up-heat-on-international-criminal-gangs-while-directing-federal-agencies-to-adopt-ai-defenses/>
2. Operaciones en el Ambiente de la Información Libro en formato digital disponible en:
https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_b2ce737fe7427cb279d7cb6ef4bd53c8
3. La ciberseguridad es ahora una prioridad en las salas de juntas:
<https://www.youtube.com/watch?v=Jgu4VY7zyAg>



Facultad
Militar
Conjunta



La empresa agente: cómo los agentes de IA están transformando los negocios con Adam Evans de Sale..
<https://www.youtube.com/watch?v=bsxrTa9YL3Y>

*Copyright © * | 2026 | **
** | Facultad Militar Conjunta | **
Todos los derechos reservados.
** | Observatorio Argentino del Ciberespacio | **
Sitio web: [http:// https://undef.edu.ar/fmc/ciberespacio/boletines.php](http://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 |
