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°58
Noviembre 2025

OAC Boletín Nº58 Noviembre 2025

El arma y la munición de la guerra en el dominio cognitivo es la información. Dominar la iniciativa en la generación, identificación, adquisición, difusión y retroalimentación de información es la clave para obtener ventaja en el campo de batalla en el dominio cognitivo.

ZhiyouSun Haitao

Red Militar de China del Ministerio de Defensa Nacional

Tabla de Contenidos

ESTRATEGIA
- ¿Hay que limitar la autonomía de las armas con IA?
- El gran pacto de la IA. Lo que Estados Unidos necesita para ganar la carrera por la innovación

CIBERGUERRA
- IA en la guerra contra insurgencia
- La IA en la toma de decisiones militares
- Algoritmos de guerra: El uso de la inteligencia artificial en la toma de decisiones en conflictos armados
- La nueva frontera de la IA en la planificación de guerras

CIBERSEGURIDAD
- La ciberseguridad y poder
- Proteger los sistemas eléctricos modernos: Implementar estrategias integrales para mejorar la resiliencia y fiabilidad frente a los ciberataques
- Ciberseguridad en el sector eléctrico 2025

CIBERDEFENSA
- Reconfigurando la estrategia cibernética de EE. UU. tras el Tifón Salt
- Un experto explica qué es Salt Typhoon y su ataque a las redes de telecomunicaciones de las Estados Unidos
- La importancia de los ciberataques a las redes de telecomunicaciones

CIBERCONFIANZA
- Reacción contra la IA
- Resistencia a la IA: ¿Quién dice que no a la IA y por qué?
- Por qué crece la resistencia a la inteligencia artificial

TECNOLOGÍA
- Una solución en la generación de energía para IA

CIBERFORENSIA
- Informes de Vulnerabilidades y recomendaciones de ENDURECIMIENTO de CISA

Video recomendado
Lecturas recomendadas

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

¿Hay que limitar la autonomía de las armas con IA?

La inteligencia artificial es una tecnología transformadora que moldea la civilización. Su integración en el ámbito militar conlleva profundas implicaciones para la conducción de los conflictos armados, incluyendo la toma de decisiones y la gestión de responsabilidades en uno de los ámbitos más trascendentales de la actividad humana. Las implicaciones van más allá del campo de batalla, introduciendo mayores riesgos en el contexto de la paz y la seguridad internacionales. Aprovechando el impulso generado por la Cumbre REAIM de 2023 en La Haya y reforzado por las deliberaciones mundiales sobre la gobernanza de la IA en el ámbito militar, este informe constituye el principal resultado de GC REAIM hasta la fecha.

CITACIÓN: La Comisión Global sobre Inteligencia Artificial Responsable en el Ámbito Militar, Responsable por Diseño: Informe de Orientación Estratégica sobre los Riesgos, Oportunidades y Gobernanza de la Inteligencia Artificial en el Ámbito Militar, La Haya, 2025
https://hcss.nl/news/new-gc-reaim-strategic-guidance-report-on-responsible-ai-in-the-military-domain/
https://www.nature.com/articles/d41586-025-03357-1
https://blogs.bath.ac.uk/iprblog/2025/03/11/how-the-risk-of-ai-weapons-could-spiral-out-of-control/

El gran pacto de la IA. Lo que Estados Unidos necesita para ganar la carrera por la innovación

La inteligencia artificial se ha consolidado como el núcleo de la competencia tecnológica y geopolítica del siglo XXI, definiendo capacidades económicas, militares y de seguridad con una velocidad sin precedentes. En este contexto, Ben Buchanan y Tantum Collins proponen una reflexión estratégica fundamental: la necesidad de un Gran Pacto de la IA, un acuerdo integral que permita a Estados Unidos sostener su liderazgo en un entorno donde la innovación por sí sola ya no basta.

Si bien Estados Unidos conserva ventajas claras —empresas líderes, talento científico excepcional y acceso privilegiado a hardware crítico—, estas fortalezas conviven con vulnerabilidades crecientes. La concentración del poder computacional en un pequeño número de corporaciones, la competencia de modelos estatales dirigidos como el de China y la falta de coordinación estratégica interna plantean riesgos estructurales. Por ello, Buchanan y Collins argumentan que el país necesita un pacto sólido entre gobierno, industria, academia y aliados democráticos que combine seguridad y competencia, innovación y estabilidad, rapidez tecnológica y responsabilidad estratégica.

El “Gran Trato con la IA” propuesto por Buchanan y Collins es, en esencia, un llamado urgente a reorganizar la arquitectura del poder tecnológico estadounidense. No se trata solo de avanzar rápido, sino de avanzar con visión, cohesión y propósito en una era que definirá la primacía global.
https://www.foreignaffairs.com/united-states/artificial-intelligence-grand-bargain-buchanan-collins

---

CIBERGUERRA

IA en la guerra contra la insurgencia

La reciente campaña israelí en Gaza marca un punto de inflexión en la guerra moderna: la fusión de la contrainsurgencia y la inteligencia artificial. ¿Se verán influenciados los estados occidentales, con sus distintas tradiciones de contrainsurgencia que priorizan la legitimidad y el control de la población, por el modelo algorítmico israelí? Esta pregunta es de suma importancia. Si el enfoque israelí, caracterizado por la automatización, la escalada y el desgaste, se convierte en un modelo para las democracias liberales, podría normalizar una forma de guerra que valora la eficiencia computacional por encima del juicio humano.
https://warontherocks.com/2025/10/¿Proliferará la contrainsurgencia algorítmica de Israel hacia Occidente?
https://aiweapons.tech/el-ascenso-de-palantir-military-ai-from-counterinsurgency-to-kill-chains/
https://debuglies.com/2025/10/30/la-contrainsurgencia impulsada por la IA de Israel en Gaza: implicaciones para los militares occidentales y la gobernanza global de 2025
https://esoc.princeton.edu/publications/irregular-warfare-podcast-artificial-intelligence-and-counterinsurgency
https://www.brookings.edu/articles/wars-of-none-ai-big-data-and-the-future-of-insurgency/

La IA en la toma de decisiones militares

La inteligencia artificial está transformando la toma de decisiones militares. Cómo los sistemas con IA pueden mejorar el conocimiento de la situación y acelerar las decisiones operativas críticas, incluso en entornos dinámicos y de alta presión. Sin embargo, también destaca la necesidad fundamental de contar con ámbitos operativos claros, una formación sólida y una mitigación de riesgos rigurosa para contrarrestar los desafíos inherentes al uso de la IA, como los sesgos en los datos y las dificultades de la automatización. Este informe ofrece un marco equilibrado para ayudar a los líderes militares a integrar la IA de forma responsable y eficaz.
https://cset.georgetown.edu/publication/ai-for-military-decision-making/

Algoritmos de guerra: El uso de la inteligencia artificial en la toma de decisiones en conflictos armados

En esta publicación, el asesor militar del CICR Ruben Stewart y la asesora legal Georgia Hinds buscan examinar críticamente algunos de los beneficios promocionados de la IA cuando se utilizan para apoyar decisiones de actores armados en la guerra.

La integración de la Inteligencia Artificial (IA) en el ámbito militar promete revolucionar las operaciones, ofreciendo una aceleración crítica en el tiempo y mejorando la conciencia situacional de los comandantes. Herramientas avanzadas, incluida la IA generativa, buscan automatizar y optimizar el proceso de planificación para generar cursos de acción complejos.

Sin embargo, esta tecnología conlleva profundos dilemas éticos y de seguridad. Los expertos advierten sobre el riesgo inherente de los mensajes en los datos y la incertidumbre irreductible en las predicciones. El Derecho Internacional Humanitario (DIH) es claro: la IA debe ser una herramienta de apoyo que nunca desplace el juicio humano. La responsabilidad final recae en los comandantes, exigiendo mitigación de riesgos, capacitación rigurosa y la definición de límites operativos estrictos para proteger a la población civil.
https://blogs.icrc.org/law-and-policy/2023/10/24/algoritmos-de-guerra-uso-de-inteligencia-artificial-toma-de-decisiones-conflicto-armado/

La nueva frontera de la IA en la planificación de guerras

El teniente coronel del ejército de EEUU Rich Farnell y la teniente coronel de la fuerza aérea de EEUU Kira Coffey, analizan en el artículo la adaptación lenta a entornos dinámicos ha sido históricamente catastrófica en la guerra.

El Departamento de Defensa debe acelerar la adopción de IA Generativa en su Proceso Conjunto de Planificación Operativa. A diferencia de Modelos de Lenguaje de Gran Escala simples, la IA Generativa ejecuta tareas complejas de manera autónoma, sintetizando factores de planificación y generando Cursos de Acción mientras acelera los ciclos de decisión. Esto proporciona superioridad informativa, crea dilemas múltiples al adversario y mantiene ventaja táctica, como demuestra el conflicto Rusia-Ucrania. La IA Generativa es el nuevo facilitador tecnológico esencial para no ser superados.
https://www.lineofdeparture.army.mil/Journals/Field-Artillery/Field-Artillery-Archive/Field-Artillery-2025-E-Edition/AIs-New-Frontier-in-War-Planning/

CIBERSEGURIDAD

La ciberseguridad y poder

Las operaciones cibernéticas se han convertido en un rasgo definitorio del conflicto moderno, una línea de frente que moldea los contornos de la competencia por el poder global. Sin embargo, a pesar de los titulares diarios sobre hackers chinos que vulneran los sistemas de contratistas de defensa, el ransomware ruso que paraliza los oleoductos y los agentes cibernéticos iraníes que sondean nuestra infraestructura crítica , persiste una brecha cada vez más peligrosa entre las ambiciones cibernéticas estratégicas de Estados Unidos y la forma en que estas capacidades se integran en las operaciones bélicas. Sin una acción urgente, las fuerzas armadas podrían terminar con una fuerza cibernética de apariencia formidable, pero con bases tácticas débiles.
https://warontherocks.com/2025/10/the-things-that-bedevil-u-s-cyber-power/

Proteger los sistemas eléctricos modernos: Implementar estrategias integrales para mejorar la resiliencia y fiabilidad frente a los ciberataques

La digitalización eléctrica impulsa la eficiencia sobre el control, pero también expone nuevas vulnerabilidades críticas. El creciente riesgo de ciberataques, obliga a reforzar la resiliencia del sistema energético moderno. Este artículo examina amenazas, defensas y estrategias clave para proteger infraestructuras eléctricas esenciales en un entorno tecnológico.

Autor: Sobhy Abdelkader, Jeremiah Amissah, Sammy Kinga, Geofrey Mugerwa, Ebinyu Emmanuel, Diaa-Eldin A. Mansour, Mohit Bajaj, Vojtech Blazek, Lukas Prokop
Publicación: Resultados en ingeniería
Editor: Elsevier
Fecha: Septiembre de 2024
https://www.sciencedirect.com/science/article/pii/S2590123024009022

Ciberseguridad en el sector eléctrico 2025

La red eléctrica se ha convertido en un objetivo cibernético de alto valor, y la frecuencia de los ataques ha aumentado drásticamente en los últimos años. Las amenazas van desde malware especializado para sistemas de control industrial (ICS) como el de Ucrania en 2015-2016 hasta campañas de ransomware como la del caso Colonial Pipeline en 2021, que provocaron interrupciones reales en los servicios. El sector energético se sitúa ahora como la cuarta industria más atacada a nivel mundial, entre las industrias más atacadas por los hackers. Para defender la infraestructura crítica, las empresas de servicios públicos se adhieren a estrictos marcos de seguridad como NERC CIP, NIST, IEC y EU NIS2 e implementan mejores prácticas como segmentación de red, gestión de parches, MFA y monitoreo continuo .
https://deepstrike.io/blog/cybersecurity-in-the-power-sector-2025

CIBERDEFENSA

Reconfigurando la estrategia cibernética de EE. UU. tras el Tifón Salt

En una campaña plurianual denominada Salt Typhoon, agentes cibernéticos de la República Popular China (RPC) han vulnerado los sistemas de numerosos proveedores de telecomunicaciones importantes, entre ellos Verizon, AT&T y T-Mobile. En conjunto, 397,1 millones de usuarios están suscritos a estos tres proveedores, lo que indica que Salt Typhoon podría afectar a cientos de millones de personas. Salt Typhoon podría ser el peor ciberataque a las telecomunicaciones en la historia.
https://www.lawfaremedia.org/article/reconfiguring-u.s.-cyber-strategy-in-the-wake-of-salt-typhoon

Un experto explica qué es Salt Typhoon y su ataque a las redes de telecomunicaciones de las Estados Unidos

El complejo ciberataque, llevado a cabo por un grupo de hackers apodados Salt Typhoon, comenzó ya en 2022. Su propósito, según funcionarios estadounidenses, era dar a los operativos de los delincuentes, acceso persistente a redes de telecomunicaciones en todo EE. UU. mediante dispositivos comprometidos como routers y switches gestionados por empresas como AT&T, Verizon, Lumen y otras.
https://theconversation.com/what-is-salt-typhoon-a-security-expert-explains-the-chinese-hackers-and-their-attack-on-us-telecommunications-networks-244473

La importancia de los ciberataques a las redes de telecomunicaciones

Las redes de telecomunicaciones son el sustento de la sociedad moderna, ya que permiten las comunicaciones personales, apoyan las operaciones de seguridad nacional y sostienen las actividades económicas mundiales. Al atacar estas infraestructuras críticas, el grupo de amenazas afiliado a la RPC conocido como Salt Typhoon explota el papel central que desempeñan las empresas de telecomunicaciones en las funciones gubernamentales, el comercio y la vida cotidiana.

Las últimas directrices CISA que estamos publicando en el apartado de CIBERFORENCIA de esta edición, hacen hincapié tanto en las medidas preventivas como en las detectivas. Las organizaciones deben implementar las acciones recomendadas relacionadas con la visibilidad, la supervisión, la gestión de la configuración, la segmentación, los protocolos seguros, los controles de acceso y las técnicas de endurecimiento específicas de cada proveedor.
https://es.vectra.ai/blog/the-silent-storm-inside-salt-typhoons-massive-telco-cyberattack

---

CIBERCONFIANZA

Reacción contra la IA

La transformación económica impulsada por la IA ya ha comenzado. En mayo, IBM anunció el despido de cientos de empleados, a quienes reemplazó con chatbots de inteligencia artificial. Durante el verano, Salesforce redujo drásticamente su plantilla gracias a la IA; UPS, JPMorgan Chase y Wendy's también están recortando personal a medida que automatizan más funciones. Los recién graduados universitarios tienen más dificultades que nunca para encontrar empleos de nivel inicial. Y estas tendencias son solo el principio. En numerosas encuestas, empresas de todo el mundo afirman que planean utilizar la IA para transformar sus plantillas.
https://www.foreignaffairs.com/united-states/coming-ai-backlash

Resistencia a la IA: ¿Quién dice que no a la IA y por qué?

Un conjunto de datos envenenado. Una huelga de guionistas que congeló Hollywood durante 148 días. Protestas callejeras contra centros de datos. Detrás de cada uno de estos actos hay una creciente resistencia global contra la inteligencia artificial. Basándose en el reciente informe "Del rechazo a la regulación: mapeando el panorama de la resistencia a la IA", de Can Simsek y Ayse Gizem Yasar, este artículo examina cómo artistas, trabajadores, activistas y académicos desafían el diseño, el despliegue y la gobernanza de los sistemas de IA. Explora los factores que impulsan la resistencia a la IA y expone una agenda de investigación que trata estos actos no como obstáculos, sino como contribuciones vitales a la gobernanza democrática de la IA
https://www.hiig.de/en/ai-resistance/

Por qué crece la resistencia a la inteligencia artificial

Las preocupaciones sobre los riesgos de la IA —desde la pérdida de empleos y violaciones de derechos de autor hasta las armas autónomas— han provocado un creciente movimiento anti-IA. Artistas, investigadores y activistas están resistiendo mediante demandas, protestas y llamamientos a la regulación global.
https://builtin.com/artificial-intelligence/anti-ai

TECNOLOGÍA

Una solución en la generación de energía para IA

El auge de la inteligencia artificial (IA) ha generado una presión sin precedentes sobre las redes eléctricas mundiales. Ante la dificultad de cubrir la demanda energética de los centros de datos, varias compañías han encontrado una solución innovadora: reutilizar motores de aviones Boeing 747 para convertirlos en potentes generadores eléctricos que suministren energía a gran escala.
https://spectrum.ieee.org/ai-data-centers
https://www.elconfidencial.com/tecnologia/2025-11-02/turbinas-boeing-747-resuelven-problema-ia-1qrt_4237587/
https://es.slideshare.net/slideshow/b747-electrical-power/1199951

CIBERFORENSIA

Informes de Vulnerabilidades y recomendaciones de ENDURECIMIENTO de CISA

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). Hemos agregado prioritariamente y en primer término, las recomendaciones de ENDURECIMIENTO como resultado de los ciberataques por parte de Salt Typhoon
Visibilidad Mejorada y Guía de Endurecimiento para la Infraestructura de Comunicaciones | CISA
https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

---

Video recomendado

1. La verdad sobre la inteligencia artificial: https://www.primevideo.com/-/es/detail/La-verdad-sobre-la-inteligencia-artificial/0P9GS9JT3WOGWVV3A6L7HFW6NO

Lecturas recomendadas

2. 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
3. Economía de defensa, ciberseguridad y ciberdefensa https://www.academia.edu/99051800/Econom%C3%ADa_de_defensa_ciberseguridad_y_ciberdefensa?email_work_card=view-paper
4. 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
5. Operaciones en el Ambiente de la Información Libro en formato digital disponible en: https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_b2ce737fe7427cb279d7cb6ef4bd53c8

** | Observatorio Argentino del Ciberespacio | *
Sitio web: 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 |**
