

OAC Boletín NÚMERO 56 de agosto de 2025

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, es un esquema conceptual que relaciona eventos y ayuda a poner en orden las ideas

Henry Kissinger

Tabla de Contenidos

ESTRATEGIA	3
El auge de las fuerzas armadas con inteligencia artificial: dentro de los sistemas de defensa del futuro	
La revolución de la IA en el análisis de la inteligencia	
CIBERGUERRA	3
La guerra cognitiva en la competencia continua	
La guerra Adaptativa	
CIBERSEGURIDAD	2
Ciberseguridad e Inteligencia Artificial en el Escenario Global Contemporáneo	
CIBERDEFENSA.....	4
Las empresas de IA de EE-UU- se pliegan al sistema de defensa	
CIBERCONFIANZA	3
Los jóvenes la información, la IA y la Revolución de la confianza	
Razonamiento auto adaptativo para la ciencia	
TECNOLOGÍA.....	4
Codificador cerebral trimodal para la predicción de la respuesta	
Computación Cuántica	
CIBERFORENSIA	5
Informes de Vulnerabilidades	



ESTRATEGIA

El auge de las fuerzas armadas con inteligencia artificial: dentro de los sistemas de defensa del futuro

Los aviones a gran escala y los programas de defensa multimillonarios se están volviendo obsoletos ante la tecnología militar inteligente, escalable y automatizada. Este artículo explora cómo empresas como Edge Group lideran una nueva era de guerra autónoma con drones que operan sin pilotos humanos, coordinan misiones y permanecen en el espacio aéreo durante más de 24 horas. Sistemas como drones de enjambre, vehículos aéreos no tripulados (UAV) furtivos y plataformas logísticas inteligentes se están desarrollando e implementando rápidamente. Estas innovaciones no solo están transformando las fuerzas aéreas, sino que también desafían la economía y la estrategia de defensa tradicionales.

<https://www.msn.com/en-us/news/technology/the-rise-of-ai-militaries-inside-the-defense-systems-of-tomorrow/vi-AA1ETiPc?ocid=msedgntp&pc=U531&cvid=5ad1782f8e134975a5a8c413ee06621b&ei=162>

La revolución de la IA en el análisis de inteligencia

Edgardo C Glavinich explica en este artículo que: “La inteligencia artificial ha alcanzado un punto de inflexión crítico en su aplicación al análisis de inteligencia, transformando no solo las metodologías operacionales sino redefiniendo fundamentalmente las capacidades estratégicas tanto en el sector público como privado. Esta revolución tecnológica trasciende la simple automatización de procesos, estableciendo nuevos paradigmas donde la velocidad de procesamiento, la precisión analítica y la capacidad de síntesis de información compleja determinan ventajas competitivas decisivas en un entorno geopolítico y empresarial cada vez más dinámico”.

<https://www.linkedin.com/pulse/la-revoluci%C3%B3n-de-ia-en-el-an%C3%A1lisis-inteligencia-c%C3%B3mo-los-glavinich-vzhxf/>

CIBERGUERRA

La guerra cognitiva en la competencia continua

El artículo comenta que: “*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*” (Haitao, 2022). El artículo explora acerca de cómo la cuestión cognitiva se inserta en la competencia continua como una línea de acción en la que se construye la estrategia, cuáles serían las tácticas, qué herramientas se aprecian y dar algunos ejemplos de sus resultados.

<https://www.pucara.org/post/la-guerra-cognitiva-en-la-competencia-continua>

<https://geoestrategia.eu/noticia/44591/defensa/guerra-cognitiva:-detengamos-la-competencia-mundial-por-el-control-del-cerebro-humano.html>



La guerra Adaptativa

Mick Ryan aborda este tema desde “Pucará de defensa” y es continuado con otros artículos relacionados con esta manera de hacer la guerra que parece consolidarse en las capacidades de las tecnologías de la cuarta revolución industrial, el autor se pregunta ¿Se trata de una nueva revolución en los asuntos militares?

<https://www.pucara.org/post/la-nueva-guerra-de-adaptaci%C3%B3n>

<https://www.pucara.org/post/guerra-adaptativa-el-flujo-de-trabajo-simbi%C3%B3tico>

<https://www.pucara.org/post/no-todas-las-adaptaciones-son-buenas>

https://www.linkedin.com/posts/pucara-defensa_adaptaci%C3%B3n-y-aprendizaje-en-la-guerra-en-activity-7279468991750754304-pmGA/?originalSubdomain=es

CIBERSEGURIDAD

Ciberseguridad e Inteligencia Artificial en el Escenario Global Contemporáneo

Mariano Bartolomé, proporciona una visión actualizada sobre la situación de la ciberseguridad, a inicios de la tercera década del siglo 21. Para alcanzar esa meta, el trabajo se estructurará en tres partes: párrafos introductorios, un espacio de desarrollo y, por último, unas breves conclusiones. Específicamente en su desarrollo, se abordarán inicialmente los límites y contenidos de la mencionada ciberseguridad, describiendo sus diferentes aristas y algo de su terminología específica; luego se reflejará su estado de situación actual, subrayando la influencia ejercida por dos acontecimientos sucedidos en las postrimerías del decenio anterior; en tercer término, se explorará un impacto de la Cuarta Revolución Industrial – Big Data mediante – en la ciberseguridad: el que genera la Inteligencia Artificial (IA).

https://www.academia.edu/86595535/Ciberseguridad_e_Inteligencia_Artificial_en_el_Escenario_Global_Contemporáneo

CIBERDEFENSA

Las empresas de IA de EE-UU- se pliegan al sistema de defensa

Anthropic, Google, OpenAI y xAI están posicionados para recibir un máximo de 200 millones de dólares cada uno según el contrato que la Oficina Principal de Inteligencia Artificial y Digital (CDAO) del Pentágono ha adjudicado contratos a cuatro importantes empresas de inteligencia artificial con sede en Estados Unidos para acelerar la integración de inteligencia artificial avanzada en el ejército a través del Departamento de Defensa de Estados Unidos (DoD). El Departamento de Defensa aprovechará la experiencia y la innovación de estas empresas para crear flujos de trabajo generativos impulsados por inteligencia artificial para diversas misiones de seguridad nacional. Como parte del proceso 4 grandes ejecutivos de tecnología a quienes el Ejército nombró directamente tenientes coroneles, sin antecedentes militares, no se excusarán de hacer negocios con el Departamento de Defensa, mientras el Pentágono, particularmente el Ejército, se acerca a Silicon Valley.

<https://www.army-technology.com/news/us-dod-ai-companies/?cf-view>

<https://www.defenseone.com/defense-systems/2025/07/pentagon-awards-multiple-companies-200m-contracts-ai-tools/406700/>

<https://www.military.com/daily-news/2025/06/27/tech-executives-commissioned-senior-army-officers-wont-recuse-themselves-dod-business-dealings.html>



<https://tynmagazine.com/ee-uu-nombro-a-ejecutivos-de-las-big-tech-como-oficiales-de-alto-rango-para-que/>

CIBERCONFIANZA

Los jóvenes la información, la IA y la Revolución de la confianza

Millones de estudiantes universitarios de todo el mundo se preparan para comenzar clases. Para que el año escolar sea aún mejor, ponemos a su disposición nuestras herramientas de IA más avanzadas de forma gratuita, incluyendo nuestro nuevo modo de Aprendizaje Guiado. También destinamos mil millones de dólares a programas de educación, capacitación laboral e investigación en IA en EE. UU. Esto incluye ofrecer nuestra capacitación en IA y carreras profesionales de forma gratuita a todos los estudiantes universitarios de Estados Unidos a través de nuestro Acelerador de IA para la Educación; más de 100 universidades ya se han inscrito. Ofrecer las mejores tecnologías a cada estudiante siempre ha sido fundamental para la misión de Google. Por eso, creamos Chromebooks para cada aula y trabajamos en LearnLM, que ha ayudado a convertir a Gemini en el modelo de aprendizaje líder a nivel mundial. Ofrece acceso ampliado a Gemini 2.5 Pro, Investigación profunda mayor acceso a Investigación profunda en 2.5 Pro. NotebookLM Veo 3 Límites más altos al usar Jules, nuestro agente de codificación de IA asincrónica que puede corregir errores y crear nuevas funciones para sus proyectos de codificación. 2 TB de almacenamiento.

https://blog.google/products/gemini/google-ai-pro-students-learning/?utm_source=www.therundown.ai&utm_medium=newsletter&utm_campaign=u-s-govt-gets-chatgpt-for-a-buck&_bhlid=3fcc3d56f5db71b179340c9a9518d28e3a87e378

Razonamiento auto adaptativo para la ciencia

Los agentes LLM de larga duración, dotados de sólidas habilidades de razonamiento, planificación y ejecución, tienen el potencial de transformar el descubrimiento científico con avances de gran impacto, como el desarrollo de nuevos materiales o fármacos. A medida que estos agentes se vuelven más autónomos, garantizar una supervisión humana eficaz y una rendición de cuentas clara cobra cada vez mayor importancia, lo que plantea retos que deben abordarse para liberar todo su potencial transformador. Los enfoques actuales para el razonamiento a largo plazo se establecen durante la fase posterior al entrenamiento, antes de la implementación para el usuario final, y normalmente son establecidos por el proveedor del modelo. Como resultado, las acciones esperadas de estos agentes están preconfiguradas por el desarrollador del modelo, ofreciendo poco o ningún control al usuario final.

https://www.microsoft.com/en-us/research/blog/self-adaptive-reasoning-for-science/?utm_source=www.therundown.ai&utm_medium=newsletter&utm_campaign=u-s-govt-gets-chatgpt-for-a-buck&_bhlid=9b29dd4016f8f04fd987f1b6c0aa3070a7bd7a21



TECNOLOGÍA

Codificador cerebral trimodal para la predicción de la respuesta

Históricamente, la neurociencia ha progresado fragmentándose en dominios especializados, cada uno centrado en modalidades, tareas o regiones cerebrales aisladas. Si bien este enfoque es fructífero, dificulta el desarrollo de un modelo unificado de cognición. Presentamos TRIBE, la primera red neuronal profunda entrenada para predecir las respuestas cerebrales a estímulos en múltiples modalidades, áreas corticales e individuos. Al combinar las representaciones preentrenadas de los modelos fundamentales de texto, audio y vídeo y gestionar su evolución temporal con un transformador, nuestro modelo puede modelar con precisión las respuestas espaciales y temporales de la fMRI a los vídeos, logrando el primer puesto en la competición de codificación cerebral Algonauts 2025 con una ventaja significativa sobre sus competidores.

https://www.arxiv.org/abs/2507.22229?utm_source=www.therundown.ai&utm_medium=newsletter&utm_campaign=meta-s-mind-reading-movie-ai&_bhlid=576066369b6b04a5aefc83f8ea51999abbbf88c3a

Computación Cuántica

Las computadoras cuánticas tienen el potencial de resolver problemas que están mucho más allá del alcance de las supercomputadoras más rápidas de la actualidad. Sin embargo, las máquinas actuales son notoriamente frágiles. Los bits cuánticos, o "cúbits", que almacenan y procesan información se ven fácilmente alterados por su entorno, lo que provoca errores que se acumulan rápidamente. Uno de los enfoques más prometedores para superar este desafío es la computación cuántica topológica, cuyo objetivo es proteger la información cuántica codificándola en las propiedades geométricas de partículas exóticas llamadas anyones. Se prevé que estas partículas, cuya existencia se prevé en ciertos materiales bidimensionales, sean mucho más resistentes al ruido y a las interferencias que los cúbits convencionales.

Investigadores de la Universidad del Sur de California (USC) en EE. UU. recurrieron a una partícula a menudo pasada por alto para almacenar y procesar información cuántica para superar la fragilidad de las computadoras cuánticas y hacerlas más universales en un futuro cercano.

<https://www.msn.com/en-us/news/technology/discarded-particles-dubbed-neglectons-may-unlock-universal-quantum-computing/ar-AA1JVQ9L>

CIBERFORENCIA

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 18 de agosto: <https://www.cisa.gov/news-events/bulletins/sb25-237>



Facultad
Militar
Conjunta



2. Vulnerabilidades semana del 11 de agosto: <https://www.cisa.gov/news-events/bulletins/sb25-230>
3. Vulnerabilidades semana del 4 de agosto: <https://www.cisa.gov/news-events/bulletins/sb25-223>
4. Vulnerabilidades semana del 28 de julio: <https://www.cisa.gov/news-events/bulletins/sb25-216>
5. Vulnerabilidades semana del 21 de julio: <https://www.cisa.gov/news-events/bulletins/sb25-209>
6. Vulnerabilidades semana del 14 de Julio: <https://www.cisa.gov/news-events/bulletins/sb25-202>
7. Vulnerabilidades semana del 7 de Julio: <https://www.cisa.gov/news-events/bulletins/sb25-195>

Microsoft publica una guía sobre la vulnerabilidad de alta gravedad (CVE-2025-53786) en implementaciones híbridas de Exchange

CISA tiene conocimiento de la vulnerabilidad de alta gravedad recientemente descubierta, CVE-2025-53786 , que permite a un cibercriminal con acceso administrativo a un servidor Microsoft Exchange local escalar privilegios explotando configuraciones híbridas vulnerables. Si no se soluciona, esta vulnerabilidad podría

Copyright © * | 2025 | *

* | 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 | *
