Codirector: TC (R) Ing Carlos Amaya
Edición: Bib Alejandra Castillo

ISSN: 2718-6245
https://undef.edu.ar/fmc/ciberespacio/boletines.php

AÑO 8 N°59
Diciembre 2025

OAC Boletín número 59 diciembre de 2025

El futuro de la guerra no se trata de combatir con mayor inteligencia. Se trata de no combatir en absoluto.

Coronel Mietta Groeneveld (directora de C2COE)

Tabla de Contenidos

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

Ciberataques, sabotajes, interferencias, drones ¿guerra híbrida?

El sistema internacional se ha ido transformando desde principios del siglo XXI, pasando de un modelo bipolar, vigente desde el final de la Segunda Guerra Mundial, a un mundo multipolar en formación. Esto ha dado lugar al surgimiento de una nueva forma de conflicto: la guerra híbrida.

Esta táctica combina acciones militares convencionales con otras no militares, como ciberataques, interferencia de información, sabotaje de infraestructura enemiga y sobrevuelos con drones. Nunca se declara oficialmente, lo que dificulta la atribución oficial y una respuesta específica.

https://theconversation.com/cyberattaques-sabotage-ingerence-drones-bienvenue-a-lere-de-la-guerrehybride-269454 https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

https://www.researchgate.net/publication/373118996_HYBRID_WARFARE_AS_A_NEW_TYPE_OF_WAR_THE_EVOLUTION_OF_ITS_CONCEPTUAL_CONSTRUCT https://otralectura.com/2025/01/13/la-guerra-hibrida-un-enfoque-moderno-de-conflicto/

Explorando el vacío: La psicología de la propaganda moderna

En lugar de hablar de "explotar el vacío", ¿no sería más preciso decir que la propaganda actual "aprovecha verdades posibles" o "aprovecha el cambio de papeles después de la Guerra Fría"?

Durante la Guerra Fría, los conservadores estadounidenses veían a la URSS como un "imperio del mal" que traía influencias culturales destructivas. Por el contrario, veían a Estados Unidos como el protector que evitaba que el mundo cayera en el comunismo sin Dios y en el caos.

https://warroom.armywarcollege.edu/podcasts/modern-propaganda/

El dominio del espectro electromagnético: Diez años después de "Winning the Airwaves"(WAW)

Reyes Rodríguez, Jesús Miguel (2025), "El dominio del especto electromagnético: Diez años después de "Winning the Airwaves" (WAW)", *Global Strategy Report*, 15/2025.

En este artículo el autor da forma a notas y apuntes que ha acumulado en la preparación de clases introductorias para el Curso de Especialista Universitario en Defensa Electrónica de la Universidad de Cantabria. En él se analiza el trabajo "Winning the Airwaves" (WAW), publicado hace diez años por el Centre for Strategic and Budgetary Assessments (CSBA). Además, se contextualiza la situación geopolítica existente en el momento de la publicación del trabajo de referencia, vinculándola con la

3ª Estrategia de Compensación. El artículo resume y comenta las tres fases históricas en las que WAW se apoya para explicar la evolución de la competencia en el espectro electromagnético. Asimismo, se examina y analiza la propuesta de Clark y Gunzinger para avanzar en la tercera fase mediante una estrategia basada en operaciones de baja o nula emisión electromagnética, orientada a recuperar la ventaja estadounidense en el dominio del espectro electromagnético. Finalmente, se analiza dicha propuesta a la luz de la evolución observada en los últimos años en la competencia por el espectro electromagnético, especialmente marcada por la guerra de Ucrania y por la relevancia creciente de la inteligencia artificial y de la EW cognitiva.

https://global-strategy.org/dominio-espectro-electromagnetico/

CIBERGUERRA

Israel emite una alarmante advertencia de ciberguerra tras los ataques a Irán

El Director General (DG) de la Dirección Nacional de Ciberseguridad de Israel (INCD) **general de brigada Yossi Karadi** pintó una profecía alarmante al dirigirse a la conferencia de la Semana del Ciber en Tel Aviv la semana pasada. No había sido tan alarmista públicamente ni tan abierto sobre Irán antes. La advertencia, a través de su dirección, se vio marcada por "los métodos de ataque e influencia que Irán ha desplegado contra Israel en los últimos seis meses."

El director general dijo a su audiencia que el mundo se dirige hacia la "primera guerra basada en el ciberespacio", en la que no se dispararán disparos y "un estado podría ser atacado exclusivamente a través del ciberespacio, lo que podría paralizar sistemas críticos" y crear un "asedio digital". Israel Issues Chilling Cyber Warfare Warning After Iran Attacks

CIBERSEGURIDAD

Las 7 tendencias de ciberseguridad de 2026

Los expertos afirman que si la ciberdelincuencia fuera una nación en 2026, sería la tercera economía más grande del mundo, después de Estados Unidos y China, con un coste estimado para las empresas de 20 billones de dólares.

A continuación, se presenta las que serán las principales tendencias que impulsarán esta ola de delincuencia mundial sin precedentes durante los próximos 12 meses.

https://www.forbes.com/sites/bernardmarr/2025/09/26/the-7-biggest-cyber-security-trends-of-2026-thateveryone-must-be-ready-for/

El manual del ransomware: extorsión con IA y auge de ataques centrados en datos

El ransomware está atravesando una transformación radical impulsando la extorsión con IA. Entre abril de 2024 y abril de 2025, la infraestructura en la nube de Zscaler bloqueó más de 10.8 millones de intentos de ransomware, lo que representa un asombroso aumento interanual del 145,9%, y marca el volumen más alto desde que comenzamos a registrar estos datos

Lo que antes eran ataques generalizados basados en el cifrado de sistemas, ahora son campañas altamente dirigidas que se enfocan en robar información sensible y utilizarla para extorsionar, generando presión psicológica y reputacional. Además, los cibercriminales están utilizando inteligencia artificial generativa para automatizar la recopilación de información, crear malware y lanzar campañas de phishing con una eficiencia sin precedentes.

https://revistabyte.es/tendencias-tic/ransomware-extorsion-con-ia/

CIBERDEFENSA

IA para defenderse de ciberataques

A fines de noviembre, el Instituto de Estudios de Ciberseguridad e Infraestructura Resiliente (ICARIS), una asociación entre el Laboratorio Nacional del Pacífico Noroeste (PNNL) del Departamento de Energía y el Instituto de Tecnología de Georgia, están a punto de publicar los resultados de un estudio de cinco años que aplica inteligencia artificial (IA) para proteger controladores lógicos programables, o sistemas informáticos industriales, que están integrados en las redes de infraestructura crítica del país.

Los controladores lógicos programables (PLC) son, en esencia, computadoras industriales especializadas que leen datos de sensores y los utilizan para automatizar el control de procesos electromecánicos, como el control de interruptores eléctricos y válvulas de gas. Son omnipresentes en todos los sectores de la infraestructura crítica de cualquier nación, como la banca, las comunicaciones, el transporte y la energía.

El programa de IA que utiliza el equipo traduce dinámicamente las especificaciones de PLC en reglas lógicas temporales, asegurando adaptabilidad a configuraciones cambiantes y escenarios de amenazas. "Eso reduce la carga del operador humano para hacer estas abstracciones en cada PLC. El objetivo es que la IA lo haga a gran velocidad y a gran escala, para que así podamos ir tras sistemas de sistemas", afirmó Danny Herrera, codirector de ICARIS de PNNL.

La adopción generalizada de herramientas de inteligencia artificial (IA) está impulsando la innovación en diversos sectores, y la ciberseguridad no es una excepción. En los últimos años, la IA ha tenido un impacto significativo en las responsabilidades laborales y los requisitos de competencia para los puestos de ciberseguridad.

https://www.afcea.org/signal-media/cyber-edge/researchers-apply-ai-defend-against-stuxnet-cyberattacks?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=QrrS A

https://cloudsecurityalliance.org/blog/2025/07/01/ai-in-cybersecurity-5-practical-use-cases-for-strongerdefense

https://online.middlebury.edu/resources/article/ai-cybersecurity-defense-transformation/

CIBERCONFIANZA

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

GPT-5.1-Codex-Max, es un nuevo modelo de vanguardia para programación autónoma con agentes, ya disponible en Codex. Basado en una actualización de nuestro modelo fundamental de razonamiento, está entrenado para abordar tareas autónomas en ingeniería de software, matemáticas, investigación y mucho más. Ofrece mayor rapidez, inteligencia y eficacia en el uso de tókenes en todas las fases del ciclo de desarrollo, y supone un nuevo paso para convertirse en un asistente de programación confiable.

GPT-5.1-Codex-Max está diseñado para trabajos extensos y detallados. Es nuestro primer modelo entrenado de forma nativa para operar en múltiples ventanas de contexto mediante un proceso denominado *compaction* (compactación de texto), lo que permite trabajar de manera coherente con millones de tókenes en una misma tarea. Gracias a esto, se pueden realizar refactorizaciones a escala de proyecto, sesiones de depuración profundas y bucles de agentes de varias horas.

https://openai.com/es-419/index/gpt-5-1-codex-max/

https://www.youtube.com/watch?v=lV2DVqBTkp0&t=1s

https://www.youtube.com/watch?v=e41afiVM4YY

TECNOLOGÍA

Nuevas fuentes de energía

Una nueva batería biodegradable y estirable hecha con gelatina y ácidos naturales podría alimentar dispositivos portátiles flexibles y reducir los desechos electrónicos. Investigadores del Instituto Trottier de Sostenibilidad en Ingeniería y Diseño de la Universidad McGill han creado una batería flexible y ecológica que se dobla, se estira y se descompone naturalmente en el medio ambiente. El diseño tiene como objetivo reducir el desperdicio masivo de baterías que generan los dispositivos portátiles.

https://interestingengineering.com/innovation/mcgill-biodegradable-stretchable-battery

https://newatlas.com/energy/lemons-kirigami-inspired-stretchy-biodegradable-battery-mcgill/

https://www.youtube.com/watch?v=x_A179djvcM&t=4s

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 08 de diciembre https://www.cisa.gov/news-events/bulletins/sb25-349
2. Vulnerabilidades semana del 01 de diciembre https://www.cisa.gov/news-events/bulletins/sb25-342
3. Vulnerabilidades semana del 24 de noviembre: https://www.cisa.gov/news-events/bulletins/sb25-335

Video recomendado

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

Lecturas recomendadas

1. . 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
2. Economía de defensa, ciberseguridad yciberdefensa https://www.academia.edu/99051800/Econom%C3%ADa_de_defensa_ciberseguridad_y_ciberdefensa?email_work_card=view-paper
3. Auge de la IA en el ámbito militar y sus riesgos; Mario de Diego y Pablo Fernándezhttps://www.unav.edu/web/global-affairs/auge-de-la-ia-en-el-ambito-militar-y-sus-riesgos
4. 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 |**