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
http://www.esgcffaa.edu.ar/esp/oac-boletines.php

AÑO 8 N° 54
Abril 2025

OAC Boletín de abril de 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.

Sun ZhiyouSun Haitao.

Estimada comunidad del ciberespacio,

El Observatorio Argentino del Ciberespacio (OAC) vuelve a sus labores de análisis y divulgación con un nuevo enfoque, después de un período de ajustes operativos y una pausa forzada.

En esta edición y las futuras, analizaremos los ejes que definen los conflictos contemporáneos: **el espectro electromagnético, la inteligencia artificial (IA) y el dominio cognitivo**, pilares de la guerra moderna que operan en el ámbito de las percepciones y los datos.

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://www.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 inteligencia artificial y el consumo energético

"La descarbonización de las economías del planeta puede terminar todavía más demorada con la irrupción a gran escala de la Inteligencia Artificial (IA), cuya voracidad de energía dispara la demanda global, aunque también pueda abrir la puerta a una apuesta generalizada por las fuentes renovables".

https://www.embajadaabierta.org/post/la-ia-un-gigante-hambriento-de-energia

Los falsos profetas de Silicon Valley

Si bien la IA ofrece beneficios como la mejora de la atención médica, la agricultura y los servicios públicos, su desarrollo enfrenta desafíos. La tecnología está limitada por la escasez de datos, factores económicos y la imposibilidad de comprender completamente su funcionamiento interno. El artículo sugiere que el progreso de la IA puede no cumplir con las expectativas utópicas de sus defensores y que sus beneficios pueden ser más difusos de lo anticipado.

https://www.politicaexterior.com/los-falsos-profetas-de-silicon-valley/

La IA y su capacidad de replicarse

El artículo resume la preocupación por la autorreplicación autónoma de sistemas de IA como un posible riesgo límite para la humanidad. Aunque existen herramientas básicas para crear clones digitales a partir de videos (como Kapwing y EmulateMe), aún distan de ser "gemelos digitales" avanzados.

Investigadores chinos publicaron estudios en arXiv advirtiendo que la capacidad de autorreplicarse sin ayuda humana podría ser un paso crítico para que la IA supere a los humanos y un indicio temprano de IA no controlada. Empresas como Open AI y Google evalúan sus modelos (GPT-4 y Gemini Pro) y consideran bajo el riesgo de autorreplicación.

Sin embargo, los investigadores descubrieron que modelos más pequeños pero populares, como:

- Llama3-70B-Instruct (Meta)

- Qwen2-72B-Instruct (Alibaba),

lograron autoreplicarse con éxito en el 50% y 90% de los ensayos, respectivamente, cruzando así una "línea roja" de riesgo. Esto sugiere que incluso modelos con menos capacidad podrían volverse autónomos, planteando desafíos éticos y de seguridad.

https://essanews.com/ai-self-replication-sparks-new-fears-of-tech-autonomy,7139675797239425a

DeepSeek la IA de China ¿podría ser empleada en la guerra cognitiva?

El artículo analiza DeepSeek como un arma cognitiva, una herramienta de IA diseñada para influir en la percepción pública. Con un discurso aparentemente neutral, su algoritmo prioriza narrativas que benefician a ciertos intereses geopolíticos. Se expone cómo la tecnología se usa para manipular el consenso, erosionando la autonomía del pensamiento crítico. Bajo la fachada de innovación, se esconde un poder blando que redefine la batalla por la hegemonía cultural. ¿Inocente asistente digital o soldado de la guerra psicológica del siglo XXI? La respuesta podría alterar tu próximo prompt.

Lo que parece un simple asistente, puede ser un **soldado invisible** en la guerra cognitiva que define nuestro tiempo. La batalla ya no es por la información, sino por el sentido. Y cada *prompt* que escribimos es, quizás, un nuevo campo de combate.

https://govciomedia.com/opinion-the-deepseek-saga-analyzed-as-a-cognitive-weapon/

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

https://www.infobae.com/tecno/2025/03/28/califican-a-deepseek-la-ia-china-como-un-arma-de-destruccion-masiva-estas-son-las-razones/

CIBERGUERRA

La guerra de la Información en el Indo-Pacífico

Librar una guerra de información para obtener una ventaja asimétrica: aumentar la velocidad, la supervivencia y la letalidad de múltiples dominios en el Indo-Pacífico.

Este artículo presenta el modelo teórico de las Células de Efectos Convergentes (CEC) para organizar y emplear las capacidades de guerra de información (IW) en el Indo-Pacífico necesarias para el éxito del Empleo Ágil de Combate (ACE) y el Mando y Control Conjunto de Todos los Dominios (JADC2). Este constructo operacionaliza las ideas del Teniente General Timothy Haugh y el Brigadier General George Reynolds para lograr la convergencia contra competidores de poder estratégico y superar las limitaciones actuales en la conducción de la IW en entornos modernos y disputados.

El constructo CEC se basa en el modelo de explotación global implementado a principios de 2016 por elementos del Comando de Operaciones Especiales de los Estados Unidos (USSOCOM). También incorpora las realidades operativas de la empresa criptológica y las operaciones cibernéticas ofensivas (OCO) en el Comando Indo-Pacífico de los Estados Unidos (USINDOPACOM). Este modelo incluye (1) la revitalización del Servicio Central de Seguridad (es decir, la integración P2/P3), (2) la reorganización de las capacidades orgánicas de la

16.ª Fuerza Aérea, (3) la integración de fuerzas conjuntas, interinstitucionales (IA), de la comunidad de inteligencia (IC) y de los socios aliados, (4) operaciones persistentes en todo el espectro de competencia, y (5) la selección de objetivos y disparos en el horizonte. Este modelo crea una capacidad dinámica y escalable que difumina la línea entre operaciones cinéticas y no cinéticas, al tiempo que añade flexibilidad, resiliencia y letalidad a la actual arquitectura de guerra de inteligencia vulnerable y estática en el Indopacífico.

https://www.airuniversity.af.edu/JIPA/Display/Article/2979934/waging-information-warfare-for-asymmetric-advantage-increasing-multi-domain-spe/

Lecciones preliminares de la ciberguerra rusa en Ucrania

El 24 de febrero de 2022 marcó un hito trascendental con el inicio de la invasión rusa a Ucrania. Bajo la justificación de desmilitarización y desnazificación, este conflicto bélico se desarrolla con características inesperadas. Si bien la mayoría de los analistas anticipaban un rol preponderante del componente informativo ruso, integrando dimensiones cibernéticas, electromagnéticas y psicológicas, en consonancia con su doctrina de "guerras de nueva generación" evidenciada desde 2008 y 2014, las operaciones cibernéticas ejecutadas hasta la fecha no han alcanzado la magnitud del "ciber Pearl Harbor" previamente pronosticado. Este evento subraya la complejidad y la naturaleza inherentemente impredecible de los conflictos contemporáneos.

https://produccioncientifica.ugr.es/documentos/6450b8e87bb1586d2f052cf6

https://www.academia.edu/79091470/Lecciones_de_ciberguerra_en_Ucrania

https://news.microsoft.com/es-xl/defender-a-ucrania-primeras-lecciones-de-la-guerra-cibernetica/

https://www.infodefensa.com/texto-diario/mostrar/4117753/infodefensa-lanza-especial-sobre-lecciones-aprendidas-ucrania

https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=319157

Se crean centros de operaciones de Guerra de Información

El Centro de Operaciones de Guerra de Información (IWOC), se anunció el año pasado y se está consolidando, operará para defender la Red de Información de la Fuerza Aérea, ejecutando el comando y control (C2) de las fuerzas y proporcionando conocimiento y perspectivas situacionales globales. El centro realizará C2 en el nivel operacional y coordinará operaciones para los efectos y resultados de la guerra de información (IW), sincronizando todas las actividades en los componentes aéreos y alas del servicio. Se trata de lograr la combinación correcta de IW en todas las operaciones del servicio, cómo se hace, qué se debe interrumpir y qué se revela u oculta contra el adversario.

https://www.afcea.org/signal-media/cyber-edge/air-forces-work-create-information-warfare-operations-center-advances?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=rcjw9

https://defensescoop.com/2024/08/29/air-force-maturing-information-warfare-enterprise-thomas-hensley/

La guerra cognitiva y la capacidad del ciberespacio para potenciarla

La guerra ha evolucionado más allá de las operaciones cinéticas tradicionales. Actualmente, nos encontramos en una era descrita por los expertos como guerra cognitiva, un tipo de conflicto cuyo objetivo es influir en el pensamiento y la acción de las personas, afectando las instituciones democráticas y la seguridad nacional. Las operaciones cognitivas buscan "capturar la mente" de los enemigos, moldeando sus pensamientos, percepciones y decisiones. A diferencia de la guerra de información, que manipula nuestro pensamiento, la guerra cognitiva modifica nuestra forma de pensar. Utiliza neurociencia, análisis de datos y estrategias basadas en algoritmos para obtener una ventaja estratégica. Es esencial desarrollar un marco para enfrentar esta amenaza de manera efectiva y pronta.

https://www.defenseone.com/ideas/2025/03/china-waging-cognitive-warfare-fighting-back-starts-defining-it/403886/

https://www.defenseone.com/ideas/2023/10/chinas-social-media-attacks-are-part-larger-cognitive-warfare-campaign/391255/

(1) http://www.81.cn/jfjbmap/content/2022-09/01/content_323230.htm

CIBERSEGURIDAD

La IA en la Guerra Cognitiva

La cognición... ese laberinto mental donde la comprensión se teje con hilos subconscientes y emociones turbulentas, ¡el verdadero motor de nuestras decisiones! Y la guerra... antes un asunto más o menos definido entre bandos identificables, ¡ahora un espectro difuso donde las sombras se enfrentan! La inteligencia artificial, esa nueva hechicera de la información bélica, nos lanza a una revolución sombría, un futuro donde la mente individual pende de un hilo. El objetivo, descarnado y frío, es la manipulación, la danza macabra para torcer el espíritu y la voluntad.

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/cognitive-warfare-strengthening-and-defending-the-mind/

La ciberseguridad como factor determinante de la guerra centrada en redes

La red actual no solo debe ser resistente a la supervivencia, sino también brindar apoyo a las tropas del Ejército que se despliegan rápidamente a distancias potencialmente grandes en todo el mundo. Y en medio del renovado diseño de la fuerza del servicio, una red unificada debe combinar redes tácticas, estratégicas y empresariales.

También debe tener una consideración global a medida que se integra en los teatros, así como adoptar el modelo de prestación de servicios centrales que debe implementarse rápidamente,.

https://www.afcea.org/signal-media/cyber-edge/cybersecurity-heart-armys-network-plan?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=Gs39A

https://apps.dtic.mil/sti/tr/pdf/ADA547453.pdf

CIBERDEFENSA

La innovación de la IA como herramienta integral en la Defensa del marco regional

Abordar el desafío de la implementación de la Inteligencia Artificial en la actualidad, es tener que forzar la imaginación para adaptarla como una herramienta en las actividades cotidianas. Sus límites aún se debaten entre la ética y la tecnología, casi como una ciencia desconocida

https://deyseg.com/analysis/1387

El problema de los sistemas de mensajería en la defensa

Funcionarios del Pentágono emitieron una advertencia sobre vulnerabilidades en la aplicación de mensajería Signal (https://signal.org/es/) . Citaron a grupos de hackers rusos que explotaban la función de "dispositivos vinculados" para espiar conversaciones cifradas. Signal respondió aclarando que el memorando no era sobre la seguridad de la aplicación sino para alertar a los usuarios sobre amenazas de phishing. El memorando del Pentágono enfatizó que si bien Signal está permitido para ciertos usos no clasificados, no está aprobado para procesar información no clasificada que no sea pública.

https://www.npr.org/2025/03/25/nx-s1-5339801/pentagon-email-signal-vulnerability

https://www.techtimes.com/articles/309783/20250326/pentagon-issues-urgent-warning-about-signal-app-amid-russian-hacking-threatbeware-phishing-links.htm

https://san.com/cc/pentagon-issued-signal-warning-before-war-group-chat-leak-report/

CIBERCONFIANZA

Advertencia sobre las vulnerabilidades de las telecomunicaciones

El FBI y la CISA alertaron sobre los peligros de la mensajería no cifrada tras una grave vulneración atribuida a hackers chinos. Este incidente afectó a importantes proveedores de telecomunicaciones de EE. UU., comprometiendo información sensible como registros de llamadas y comunicaciones en tiempo real. La advertencia subraya la vulnerabilidad inherente a las comunicaciones sin cifrar y la necesidad de adoptar medidas de seguridad más robustas para proteger la información confidencial de posibles accesos no autorizados.

https://resistthemainstream.com/fbi-and-cisa-warn-of-encrypted-messagings-vital-role-amid-major-u-s-telecom-breach/?utm_source=newsletter2

Acerca de las Ciberestafas

La Policía Nacional y la Guardia Civil han informado sobre una serie de ciberestafas que están ocurriendo a través de diversas vías como llamadas telefónicas, SMS, mensajes de WhatsApp y correos electrónicos. Los ciberdelincuentes envían grandes cantidades de mensajes o correos electrónicos a direcciones obtenidas de bases de datos ilegales alojadas en la Dark web. Estas bases de datos pueden incluir información robada de usuarios, como en el caso de Linkedin en noviembre de 2023. El objetivo de estos ataques es obtener dinero o datos personales de los ciudadanos.

https://revistabyte.es/legalidad-tic/ojo-ciberestafas/

https://www.redeszone.net/noticias/seguridad/que-es-scam-estafas-comunes-defenderte/

https://www.consumerfinance.gov/ask-cfpb/what-are-some-common-types-of-scams-en-2092/

https://www.godaddy.com/resources/es/seguridad/que-es-un-scam-y-como-protegerse-ante-este-ataque

TECNOLOGÍA

Los centros de datos y la eficiencia energética

La eficiencia energética y la sostenibilidad son los dos principales problemas que tienen los centros de datos. Son numerosas las voces que ya están alertando del impacto medioambiental de los grandes data centers en un contexto en el que el mercado de centros de datos en España está en auge. Es un hecho el que más centros de datos se estná implementando de toda Europa, y las previsiones son que la potencia instalada se multiplique por seis en los próximos dos años, pasando de los actuales 160 MW a los 600 MW en 2026, según los datos de Spain DC, la asociación de data centers en España.

https://revistabyte.es/actualidad-it/eficiencia-centros-de-datos/

Caballo robot todo terreno

Kawasaki presenta a CORLEO, un robot cuadrúpedo impulsado por hidrógeno, diseñado para ser montado por personas. Su estilo futurista y propulsión sostenible lo convierten en un hito en la movilidad personal del futuro.

https://www.karmactive.com/kawasaki-corleo-4-legged-robot-horse-with-150cc-hydrogen-engine-powers-off-road-mobility-at-expo-2025/

https://www.techexplorist.com/corleo-kawasaki-hydrogen-powered-robotic-horse/98806/#google_vignette

https://newsmarketech.com/tecnologia/kawasaki-corleo-el-caballo-robotico-impulsado-por-hidrogeno/

https://www.youtube.com/watch?v=Q8TUTp0_D-I

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).

2024

1. Vulnerabilidades semana del 16 de diciembre:https://www.cisa.gov/news-events/bulletins/sb24-358
2. Vulnerabilidades semana del 23 de diciembre https://www.cisa.gov/news-events/bulletins/sb24-365

2025

3. Vulnerabilidades semana del 6 de enero https://www.cisa.gov/news-events/bulletins/sb25-013
4. Vulnerabilidades semana del 13 de enero https://www.cisa.gov/news-events/bulletins/sb25-021
5. Vulnerabilidades semana del 20 de enero https://www.cisa.gov/news-events/bulletins/sb25-026

6. Vulnerabilidades semana del 27 de enero: https://www.cisa.gov/news-events/bulletins/sb25-034
7. Vulnerabilidades semana del 3 de febrero https://www.cisa.gov/news-events/bulletins/sb25-041
8. Vulnerabilidades semana del 3 de marzo https://www.cisa.gov/news-events/bulletins/sb25-069
9. Vulnerabilidades semana del 10 de marzo: https://www.cisa.gov/news-events/bulletins/sb25-076
10. Vulnerabilidades semana del 31 de marzo https://www.cisa.gov/news-events/bulletins/sb25-097
11. Vulnerabilidades semana del 07 de abril: https://www.cisa.gov/news-events/bulletins/sb25-104

Video recomendado

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

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/V1p4Ry9iVkZwUzkvdjR2NkhKbjFRRmc4QjViTUVlQys4RVdzSWYya1pGTT0tLTAzOHpiYUFGc3JUaThRRk1RRjVIVmc9PQ==--980d5431f282a7b54f119d9fcf0cc72bd5a3e52a/t/rPXrD-SvBienE-bxdQp7/resource/work/109063921/La_Ciberseguridad_en_la_Era_de_Avances_Tecnol%C3%B3gicos_Desaf%C3%ADos_Vulnerabilidades_y_Estrategias_para_la_Protecci%C3%B3n_de_Datos?email_work_card=title

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

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

5. Boletines completos: Acceso en línea

Convocatoria a la Acción

"El OAC reafirma su compromiso con la divulgación y formación. Le invitamos a explorar nuestros recursos

la información es poder"

** | Observatorio Argentino del Ciberespacio | **

Sitio web: http://www.esgcffaa.edu.ar/esp/oac-boletines.php Nuestra dirección postal es:

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

Nuestro correo electrónico:

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