OAC Boletín de Enero-Febrero 2023

Tabla de Contenidos

ESTRATEGIA

- El acuerdo Five Eyes y la confianza cero en las redes

CIBERSEGURIDAD

- La Inteligencia Artificial y el etiquetado de datos

CIBERGUERRA

- Los drones son críticos para la guerra de información de EE. UU
- La Ciberinteligencia y la Ciber-contrainteligencia
- El ciberespacio en tiempos de guerra: la IT Army ucraniana

CIBERDELITO

- Manual de estudio sobre cibercrimen y delitos informáticos

CIBERCONFIANZA

- Los hackers nos aventajan porque hay poca gente especializada en ciberseguridad

TECNOLOGÍA

- IA Generativa

CIBERFORENSIA

- Informes CISA

Informes de interés:

- Actualizaciones de seguridad para Mozilla Vulnerabilidades de seguridad corregidas en Firefox ESR 102.6: https://www.mozilla.org/en-US/security/advisories/mfsa2023-02/

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: http://www.esgcffaa.edu.ar/esp/oac-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
El acuerdo Five Eyes y la confianza cero en las redes

Un evento de tres días en Fort Meade, Maryland, sede de la Agencia de Sistemas de Información de Defensa y el Comando Cibernético de EE. UU., reunió a representantes del Departamento de Defensa y socios de Five Eyes Australia, Canadá, Nueva Zelanda y el Reino Unido. El tema tratado: confianza cero, nuevo paradigma asumiendo que las redes ya están comprometidas y, como resultado, requieren una validación continua de usuarios y dispositivos.
https://www.c4isrnet.com/cyber/2023/01/06/pentagon-hosts-five-eyes-partners-for-zero-trust-cybersecurity-talks/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch

¿Qué es la Confianza Cero?:
https://www.bing.com/ck/a?!&&p=29a04ca5f306b071JmltdHM9MTY3NTIwOTYwMCZpZ3VpZD0yODczNmE4Yi1jNWQ1LTYxZDEtMDE4MC03YjgyYzQwODYwYTAmaW5zaWQ9NTM5Ng&ptn=3&hsh=3&fclid=28736a8b-c5d5-61d1-0180-7b82c40860a0&psq=concepto+confiaza+cero+en+redes&u=a1aHR0cHM6Ly93d3cuaWJtLmNvbS9teC1lcy90b3BpY3MvemVyby10cnVzdCM6fjp0ZXh0PSVDMiVCRlF1JUMzJUE5JTIwZXMlMjBsYSUyMGNvbmZpYW56YSUyMGNlcm8lM0YlMjBMYSUyMGNvbmZpYW56YSUyMGNlcm8sY29uJTIwdW4lMjBlbmZvcXVlJTIwZXhoYXVzdGl2byUyMHBhcmElMjBjb250cmFycmVzdGFyJTIwZXNhcyUyMGFtZW5hemFzLg&ntb=1

CIBERSEGURIDAD
La Inteligencia Artificial y el etiquetado de datos

Para superar a China en el juego cada vez más competitivo de la inteligencia artificial, EE. UU. debe impulsar drásticamente sus esfuerzos para recopilar, etiquetar y clasificar gran cantidad de datos que finalmente se utilizarán en regímenes de entrenamiento de máquinas, dijo el director digital y de inteligencia artificial del Pentágono, Craig Martell, el 26 de enero en el Simposio del Centro de Estrategia y Guerra en Colorado. "Si vamos a vencer a China, y tenemos que vencer a China en IA, tenemos que encontrar una manera de etiquetar a escala. Porque si no etiquetamos a escala, no vamos a ganar".
https://www.c4isrnet.com/artificial-intelligence/2023/01/26/pentagons-ai-chief-says-data-labeling-is-key-to-win-race-with-china/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch

CIBERGUERRA
Los drones son críticos para la guerra de información de EE. UU

El general de tres estrellas que encabeza los esfuerzos de guerra de información de la Fuerza Aérea de EE. UU. prevé un futuro sostenido para los drones en las fuerzas armadas, a medida que las naciones monitorean, analizan e intentan superarse entre sí desde distancias cada vez mayores.
El despliegue de drones se ha disparado en la guerra entre Rusia y Ucrania poniendo su uso en el centro de atención popular. Las imágenes capturadas por drones no solo pueden informar la planificación militar y los ataques, sino que también pueden impulsar narrativas y dar forma a las percepciones públicas, una faceta de la guerra de información.
https://www.c4isrnet.com/unmanned/uas/2022/12/16/drones-critical-to-us-info-warfare-playbook-air-forces-kennedy-says/

La Ciberinteligencia y la Ciber-contrainteligencia

La ciberinteligencia y la cibercontrainteligencia son activideades que generan productos de inteligencia orientados a apoyar la toma de decisiones para protegerse y hacer frente a las ciberamenazas. Ambas actúan de forma transversal en las operaciones que se conducen en el ciberespacio, tanto en los sistemas adversarios como en los sistemas propios.
https://totalnewsagency.com/2021/12/22/la-ciberinteligencia-y-la-ciber-contrainteligencia-como-piedra-angular-de-las-operaciones-en-el-ciberespacio/

El ciberespacio en tiempos de guerra: la IT Army ucraniana

La agresión rusa a Ucrania en febrero de 2022 trajo consigo la vuelta de la guerra a Europa: una guerra que ya no solo se libra en el campo de batalla, sino que también se desarrolla en escenarios como el ciberespacio. Estos nuevos escenarios implican la participación de nuevos actores en los conflictos
https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO24_2023_MARALV_Ciberespacio.pdf
DE ÁLVARO MIZZIAN, María. El ciberespacio en tiempos de guerra: la IT Army ucraniana. Documento de Opinión IEEE 24/2023.
https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO24_2023_MARALV_Ciberespacio.pdf y/o enlace bie3 *(consultado 15/03/2023)*

CIBERDELITO
Manual de estudio sobre cibercrimen y delitos informáticos

Se presenta un texto de estudio preparado por la Policía de la Provincia de Buenos Aires que expone la resolución de caso puntuales para desarrollar un conocimiento práctico sobre los temas de referencia.
https://www.mseg.gba.gov.ar/areas/Vucetich/GUIAS%20DE%20MATERIAS%202021/2%20Cibercrimen.pdf

CIBERCONFIANZA
Los hackers nos aventajan porque hay poca gente especializada en ciberseguridad

Soledad Antelada Toledano se comporta como un hacker, pero de los "buenos". Hace exactamente lo mismo que un atacante haría al poderosísimo sistema de ciberseguridad para el que trabaja. Reconoce la superficie de ataque, penetra, detecta puntos débiles, estudia el riesgo. Debe anticiparse a la mente del hacker, pensar como él para defenderse.
https://www.bbc.com/mundo/noticias-57721310

TECNOLOGÍA
Las claves de ChatGPT y las inteligencias artificiales generativas: ¿Cuáles son sus riesgos y limitaciones?

La inteligencia artificial generativa, se agregó recientemente a una lista de vigilancia de la Agencia de Sistemas de Información de Defensa.
La inteligencia artificial (IA) no se instaló entre nosotros en 2022, pero sí se convirtió en un concepto popular. Por "popular" queremos decir que pasó de ser algo técnico al alcance exclusivo de empresas y expertos, difícil de traducir fuera de ámbitos profesionales, a convertirse casi en una commodity, un bien de consumo con el que experimentar, jugar y crear. La tecnología que sustenta el bot viral ChatGPT, es lo que llamamos inteligencia artificial generativa, o que significa que es capaz de crear o generar contenido nuevo y original a partir de un conjunto de datos o de una plantilla que se le haya facilitado. Este ha sido el último empujón recibido por un mercado en el que la innovación no se ha detenido y que se encuentra en un punto clave para su implantación y adopción, de forma generalizada. Ahora bien, ¿cómo funciona realmente ChatGPT y qué riesgos puede tener en el campo de la comunicación y el marketing?
https://www.bing.com/ck/a?!&&p=4f4bc334bac1cc16JmltdHM9MTY3NTIwOTYwMCZpZ3VpZD0yODczNmE4Yi1jNWQ1LTYxZDEtMDE4MC03YjgyYzQwODYwYTAmaW5zaWQ9NTQyNw&ptn=3&hsh=3&fclid=28736a8b-c5d5-61d1-0180-7b82c40860a0&psq=inteligencia+artificial+generativa&u=a1aHR0cHM6Ly9mYWN0b3JpbmNvZ25pdG8uY29tL2Jsb2cvbGFzLWNsYXZlcy1kZS1jaGF0Z3B0LXktbGFzLWludGVsaWdlbmNpYXMtYXJ0aWZpY2lhbGVzLWdlbmVyYXRpdmFzLWN1YWxlcy1zb24tc3VzLXJpZXNnb3MteS1saW1pdGFjaW9uZXMv&ntb=1

CIBERFORENSIA
Informes 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).

1. Vulnerabilidades semana del 27 de febrero 2023: https://www.cisa.gov/news-events/bulletins/sb23-065
2. Vulnerabilidades semana del 20 de febrero 2023: https://www.cisa.gov/news-events/bulletins/sb23-058
3. Vulnerabilidades semana del 13 de febrero 2023: https://www.cisa.gov/news-events/bulletins/sb23-052
4. Vulnerabilidades semana del 6 de febrero 2023: https://www.cisa.gov/news-events/bulletins/sb23-045
5. Vulnerabilidades semana del 30 de enero 2023: https://www.cisa.gov/news-events/bulletins/sb23-037
6. Vulnerabilidades semana del 23 de enero 2023: https://www.cisa.gov/news-events/bulletins/sb23-030
7. Vulnerabilidades semana del 16 de enero 2023: https://www.cisa.gov/uscert/ncas/bulletins/sb23-023
8. Vulnerabilidades semana del 9 de enero 2023: https://www.cisa.gov/uscert/ncas/bulletins/sb23-016
9. Vulnerabilidades semana del 26 de diciembre 2022: https://us-cert.cisa.gov/ncas/bulletins/sb23-002

Informes de interés:

1. Información sobre problemas de seguridad actuales, vulnerabilidades y exploits que rodean a Sistemas de control industrial (ICS):http:// https://us-cert.cisa.gov/ncas/current-activity/2023/01/24/cisa-releases-two-industrial-control-systems-advisories
2. Actualización de seguridad para productos de Apple: https://support.apple.com/en-us/HT201222
3. Actualizaciones de seguridad para Mozilla Vulnerabilidades de seguridad corregidas en Firefox ESR 102.7: https://www.mozilla.org/en-US/security/advisories/mfsa2023-02/
4. Actualizaciones de seguridad para Mozilla Vulnerabilidades de seguridad corregidas en Firefox ESR 109: https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/

*Copyright © *| 2023 | **
**| Escuela Superior de Guerra Conjunta | **
Todos los derechos reservados.
**| 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 | **

This email was sent to jparrieu@hotmail.com
why did I get this? unsubscribe from this list update subscription preferences
OAC · Luis M. CAMPOS 480 · CABA, CABA B1716 · Argentina

mailchimp