OAC Boletín de abril-mayo 2024

"La clave para enfrentar el conflicto futuro es el desarrollo de nuevas habilidades cognitivas"–.

Operaciones en el ambiente de la Información Pag. 139

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: 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

¿Es el momento de discutir acerca de las implicancias de IA o de profundizar su desarrollo?

Infobae de la mano de la pluma de Jonathan Tirone del Washington Post plantea este interrogante a través del artículo “La IA se enfrenta a su ‘momento Oppenheimer’ durante la carrera armamentista de robots asesinos”

https://www.infobae.com/wapo/2024/04/29/la-ia-se-enfrenta-a-su-momento-oppenheimer-durante-la-carrera-armamentista-de-robots-asesinos/

Biden firma un proyecto de ley que podría prohibir TikTok

Dentro del extenso paquete de seguridad nacional de 95 mil millones de dólares que el presidente Joe Biden firmó, hay una disposición que podría prohibir TikTok, con un importante inconveniente: no sucederá antes de las elecciones de 2024. Eso significa que TikTok, que cuenta con 170 millones de usuarios estadounidenses, seguirá siendo una fuerza durante toda la campaña, proporcionando una plataforma para que los candidatos lleguen a votantes predominantemente más jóvenes

https://www.nbcnews.com/politics/congress/congress-biden-bill-ban-tiktok-when-2024-election-rcna148792

https://edition.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html

https://www.npr.org/2024/04/24/1246663779/biden-ban-tiktok-us

La inteligencia artificial y el interés de la gente

Los interesados en la IA como para escribir o leer boletines al respecto, ven la IA en todas partes. Sin embargo, la gran mayoría de la gente no lo sabe o no parece importarle demasiado. "*Pew Research*" informó que, en marzo, solo el 23 % de los adultos estadounidenses habían probado ChatGPT y el 34 % nunca había oído hablar de él . Es mas *Bob Knorpp*, en un artículo para "*Datos Research*" sobre el impacto de la IA en la búsqueda, muestra que "el usuario típico (ChatGPT) investigará la herramienta, la probará varias veces y luego aparentemente perderá el interés. Aquí los artículos

https://www.pewresearch.org/short-reads/2024/03/26/americans-use-of-chatgpt-is-ticking-up-but-few-trust-its-election-information/?utm_source=ai-logs.beehiiv.com&utm_medium=newsletter&utm_campaign=meta-brings-ai-to-billions-chatgpt-gets-memories-and-why-everyone-was-talking-about-gpt2

https://link.mail.beehiiv.com/ls/click?upn=u001.m4cV1TH-2F8Js0SJPTQ-2BdOamOjHcD-2FdEq9XVJGT6tvWYpLdZ-2Bl278X2Fp7BtsdIq4fE7W585r9cubyHk5dmyJI-2FyM-2FGqtUJj7Phtt2og9TpVUTj-2F7yfo7wQDssmI0TWCURObCeJeFEQSqmqPGDHIz1EJs2L3z99xqlBq4SL8qQXHPVII-2FbZdyrXhvIfx5MifCKPG0XK4giBwECg-2FnB6EEX2Txdhin80ECajBzJeRMpN6fAIdo-2B-2BiAlDd4DLBcMl1-2FH5YXThwdteztOmqam7ryJFdcJ-2FOLSCBuMRo6FKtgyIU7ih0t-2FoDm8hzlYRdb2Ees8Gl01_sSRfrzRYP4KMox5-2BzxXuddmbJ5G-2BuZeO2ngXsvUaIDbc99Sl6R91COrvR-2FJ3SO-2FML-2BqXhnbB8tbMErmGdz-2FDO-2B71tbKSMoPho4WL1HyCiXsg-2FswNsul23XsO-2BLrMgAKWTMliby8F4OpGA5p8kxMM9V6YuJJVXRaO5unZ-2Fc7Fm9Y3dMqCVBHtPTLV76SuFD6atLc4bTaybkNrofP2-2FbrEiFAjSIVnJ4dFaSV569LRossiw5kRVOcgTZipMyh4C8roaGxM9z-2FUwDvRmFshOCCmA-2BVPYoY6VrSyV58UUE87NzrejJdZdY69-2FdWUCFIyjsCDuxoKg-2B-2BIer0NxlnfFjrOJThsX65SKsaon6HoTQAQC7sosUOnHaJgqb2Z0iynxSOI9wGhXtAJ-2F7AgRH-2Fj9NE5ih36BvFgJ5GadV2jjzNyZPWnuFqozSWYRZObhthW-2FxHn

CIBERSEGURIDAD

Firewall versus VPN: ¿Cuál usar y cuándo??

La comparación entre firewall y VPN atrae la atención de los usuarios de Internet preocupados por la seguridad. Muchos de los que han oído hablar de estas herramientas saben que de alguna manera están relacionadas con la seguridad y la privacidad de la red. ¿Pero cómo exactamente? ¿Y cuál es la diferencia entre los dos? Encontrarás las respuestas a estas preguntas a continuación.

https://nordvpn.com/es-mx/blog/firewall-vs-vpn/

https://www.vpn.com/guide/vpn-vs-firewall/

https://revistaseguridad.cl/2024/04/26/mejor-firewall-o-vpn/

https://www.expressvpn.com/blog/firewall-vs-vpn-whats-the-difference/

FBI denuncia posibles ataques a sus infraestructuras críticas

El director del FBI, Christopher Wray, advirtió sobre posibles ciberataques disruptivos por parte de China contra la infraestructura crítica de Estados Unidos. Según informes de CyberScoop, se alertó sobre la preparación de operaciones de ciberespionaje chinas, como Volt Typhoon, con el objetivo de realizar intrusiones de gran alcance en la infraestructura estadounidense para el año 2027. Especialmente si interfiere en el conflicto de China con Taiwán.

https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

https://www.escenariomundial.com/2024/04/27/fbi-alerta-sobre-ciberataques-chinos-a-la-infraestructura-critica-de-estados-unidos/

https://www.theguardian.com/world/2024/apr/19/fbi-china-hack-infrastructure

https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/

Los problemas de Ciberseguridad también llegan a las grandes corporaciones

En una dura crítica a la seguridad y transparencia corporativa de Microsoft, una junta de revisión designada por la administración de Biden emitió un informe el martes diciendo que “una cascada de errores” por parte del gigante tecnológico permitió a los ciberoperadores chinos respaldados por el estado acceder a cuentas de correo electrónico de altos funcionarios estadounidenses, incluido el Departamento de Comercio. Secretaria Gina Raimondo.

https://www.c4isrnet.com/it-networks/cybersecurity/2024/04/03/microsoft-ripped-over-shoddy-security-in-chinese-hack-of-feds/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-cyber

El reporte: https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023

CIBERDEFENSA

Capacidades cibernéticas: el Indo-Pacífico

El Indo-Pacífico, que comprende aproximadamente 40 economías, representará más del 50% del PIB mundial para 2040, los PIB combinados de China, Japón, India, Corea del Sur y Australia ya suman más que el conjunto de la UE . A lo largo de los últimos años, esta vasta y diversa región también se ha vuelto central para el compromiso estratégico de los países de Five Eyes en una variedad de temas. Canadá , el Reino Unido , Estados Unidos , Australia y otros han publicado sus propias estrategias para el Indo-Pacífico y han forjado asociaciones de seguridad como la iniciativa trilateral AUKUS, que también se han centrado en "desarrollar una gama de capacidades, para compartir y aumentar la interoperabilidad entre Fuerzas Armadas, donde las capacidades cibernéticas, la inteligencia artificial, la tecnología cuántica y otras tecnologías emergentes son un pilar de la acción. Pero a medida que aumentan las tensiones geopolíticas, los gobiernos de la región del Indo-Pacífico se apresuran a desarrollar mayores capacidades cibernéticas para garantizar su seguridad y prosperidad futuras. Pero, ¿qué implicaciones tiene esto para las normas sobre el comportamiento estatal responsable y la transparencia en torno a las operaciones cibernéticas?

https://rusi.org/explore-our-research/publications/commentary/cyber-capabilities-indo-pacific-shared-ambitions-different-means

La defensa de operaciones OT contra hackers

CISA ha publicado una hoja con información y propuestas de mitigaciones asociadas con operaciones cibernéticas realizadas por hackers que buscan comprometer los sistemas de control industrial (ICS) y los sistemas de tecnología operativa (OT) en pequeña escala sobre sectores de infraestructura crítica de América del Norte y Europa, incluidos el agua y las aguas residuales. sistemas, represas, energía y alimentación y agricultura. En general la actividad parece limitada a técnicas poco sofisticadas que manipulan equipos ICS para crear efectos molestos. Sin embargo, las investigaciones han identificado que estos actores son capaces de utilizar técnicas que plantean amenazas físicas contra entornos OT inseguros y mal configurados.

https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity

https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf

CIBERDELITO

Nuevo troyano par Android

Un grupo de investigadores de CRIL han identificado un nuevo **troyano bancario para Android**, apodado **«**Brokewell**»**, que imita ser una actualización del navegador Google Chrome. Este *malware* posee funciones avanzadas como grabación de pantalla, registro de teclas y la capacidad de ejecutar más de 50 comandos remotos, apuntando principalmente a usuarios en Alemania, pero con indicativos de una posible expansión global. Este troyano destaca por sus múltiples capacidades maliciosas, incluyendo la grabación de pantalla y audio, registro de teclas, recolección de datos del teléfono, y gestión de llamadas. También utiliza técnicas de superposición para capturar credenciales bancarias mediante una falsa pantalla de PIN

https://unaaldia.hispasec.com/2024/04/nuevo-troyano-bancario-para-android-brokewell-disfrazado-de-una-actualizacion-de-chrome.html

CIBERCONFIANZA

La Inteligencia Generativa en el trabajo

Puede que un *chatbot* no le quite su trabajo, pero es casi seguro que lo cambiará. A continuación, le explicamos cómo empezar a pensar en poner la inteligencia artificial a trabajar para usted. La inteligencia artificial (IA) hoy accesible y amigable puede cambiar nuestra forma de trabajar. El artículo presentado *sobre* las posibilidades y los obstáculos de usar la IA generativa y su relación con las tareas propias del área de recursos humanos (RRHH), desde el reclutamiento hasta la gestión del desempeño y el crecimiento profesional habilitado por *chatbot*.

https://www.mckinsey.com/featured-insights/destacados/la-ia-generativa-y-el-futuro-de-los-rrhh/es

https://revistabyte.es/actualidad-it/amazon-q/

https://aws.amazon.com/es/q/

Los riesgos en espacios de trabajo compartido

Los espacios de coworking son ambientes muy colaborativos. Lugares donde freelancers, emprendedores, y empleados de grandes corporaciones, encuentran flexibilidad y oportunidades de networking en un entorno compartido y dinámico. Sin embargo, este mismo diseño abierto y colaborativo, que hace de los espacios de coworking lugares tan atractivos para trabajar, los expone a su vez a una serie de riesgos cibernéticos. Con el acceso libre a las redes Wi-Fi compartidas, las vulnerabilidades son abundantes y los riesgos muy reales.

https://revistabyte.es/ciberseguridad/riesgos-ciberneticos-de-los-espacios-de-coworking/

https://www.coworkingresources.org/blog/5-risks-your-coworking-business-should-address-in-2020-and-beyond

https://www.forbes.com/sites/theyec/2021/09/27/guidelines-for-coworking-spaces-in-2021/?sh=30677b0a7864

TECNOLOGÍA

Dispositivos de almacenamiento de energía deformables y miniaturizados

La creciente popularidad de la tecnología portátil ha puesto de relieve una necesidad crítica de fuentes de energía que puedan igualar la flexibilidad y el movimiento de estos dispositivos innovadores. Los investigadores han dado un importante paso adelante al abordar este desafío con el desarrollo de un dispositivo de almacenamiento de energía a pequeña escala capaz de estirarse, torcerse, doblarse y arrugarse. Este interesante avance allana el camino para dispositivos portátiles verdaderamente adaptables y cómodos

https://www.nature.com/articles/s41528-024-00306-2#Abs1
https://interestingengineering.com/energy/stretchy-power-wearables-get-flexible-energy-storage-in-new-

breakthrough?utm_source=theblueprintbyie.beehiiv.com&utm_medium=newsletter&utm_campaign=lasers-detect-illegal-ivory-river-salt-battery-self-righting-boat

Robótica y el control en primera persona

Las siglas FPV provienen de la denominación “First Person View”, que se traduce al español como “Vista en Primera Persona”. Esto quiere decir que el significado de FPV en drones se refiere a que el piloto tiene la capacidad de visualizar el panorama desde la perspectiva del dron durante el vuelo, como si estuviera en el aire desplazándose por donde pasa el drone.

https://umilesgroup.com/que-es-un-drone-fpv/

https://advdron.com/que-es-el-fpv-en-drones-vuelo-inmersivo/

https://www.youtube.com/watch?v=x2J0S3888vM

Cables submarinos el alma de Internet

Internet consta de pequeños fragmentos de código que se mueven por el mundo, viajando a lo largo de cables tan delgados como un mechón de cabello tendido en el fondo del océano. Los datos viajan de Nueva York a Sydney, de Hong Kong a Londres, en el tiempo que lleva leer esta palabra. Casi 750.000 millas de cable ya conectan los continentes para satisfacer nuestra insaciable demanda de comunicación y entretenimiento. Por lo general, las empresas han unido sus recursos para colaborar en proyectos de cables submarinos, como una autopista para que todos la compartan.

https://theconversation.com/undersea-cables-are-the-unseen-backbone-of-the-global-internet-226300

https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html

https://fortune.com/2024/04/02/undersea-cables-vulnerable-red-sea-houthis-west-africa-russia/

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 22 de abril: https://www.cisa.gov/news-events/bulletins/sb24-120
2. Vulnerabilidades semana del 25 de marzo: https://www.cisa.gov/news-events/bulletins/sb24-092
3. Vulnerabilidades semana del 01 de abril: https://www.cisa.gov/news-events/bulletins/sb24-099
4. Vulnerabilidades semana del 08 de abril: https://www.cisa.gov/news-events/bulletins/sb24-106
5. Vulnerabilidades semana del 15 de abril: https://www.cisa.gov/news-events/bulletins/sb24-113
6. Vulnerabilidades semana del 22 de abril: https://www.cisa.gov/news-events/bulletins/sb24-120

7. Vulnerabilidades semana del 29 de abril: https://www.cisa.gov/news-events/bulletins/sb24-127
8. Vulnerabilidades semana del 06 de mayo: https://www.cisa.gov/news-events/bulletins/sb24-134
9. Vulnerabilidades semana del 13 de mayo: https://www.cisa.gov/news-events/bulletins/sb24-141
10. Vulnerabilidades semana del 20 de mayo: https://www.cisa.gov/news-events/bulletins/sb24-149

Vulnerabilidad en el lenguaje de programación "R"

El lenguaje "R" es uno de los lenguajes de programación más utilizados en investigación científica, siendo además muy popular en los campos de aprendizaje automático (machine learning), minería de datos, econometría, investigación biomédica, bioinformática y en la inferencia estadística. A esto contribuye la posibilidad de cargar diferentes bibliotecas o paquetes con funcionalidades de cálculo y graficación. CISA a través del Centro de Coordinación CERT (CERT/CC) ha publicado información sobre una vulnerabilidad en las implementaciones del lenguaje de programación. Un actor de amenazas cibernéticas podría aprovechar esta vulnerabilidad para tomar el control de un sistema afectado.

https://kb.cert.org/vuls/id/238194

https://www.cve.org/CVERecord?id=CVE-2024-27322

https://hiddenlayer.com/research/r-bitrary-code-execution/

https://cran.r-project.org/

Operaciones en el Ambiente de la Información

Libro en formato digital disponible en:
https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_b2ce737fe7427cb279d7cb6ef4bd53c8

Posee información acerca de: (1) El conflicto, (2) Las operaciones en el espectro electromagnético, (3)La Guerra Cibernética, (4) La comunicación estratégica y la Estrategia de la Comunicación, (5) Las operaciones de la información de la Federación Rusa y de la República Popular China y (6) Interacciones de la comunicación estratégica y la Planificación Estratégica Militar