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 5 N° 46
Julio 2022

OAC Boletín de Julio 2022

"En contraste con otras formas y métodos de oposición, la confrontación de la información es llevada a cabo constantemente en tiempo de paz''

Slipchenco, "Future War".

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), **micro-sitio de la Escuela Superior de Guerra Conjunta de la Facultad Militar Conjunta.**

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

Se encuentra inserto en el **Nodo Territorial de Defensa y Seguridad** de la Secretaría de Ciencia y Tecnología 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 ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

ESTRATEGIA

Asegurar el aprendizaje automático requiere un enfoque socio-técnico (Interesantes artículos publicados por la revista SIGNAL que nos hacen reflexionar profundamente sobre la temática y sus consecuencias)

Las técnicas de aprendizaje automático (ML) no fueron diseñadas para competir con oponentes inteligentes; por tanto, sus propias características que las hacen tan interesantes representan también su mayor riesgo

Las características técnicas de la inteligencia artificial introducen vulnerabilidades y prestan la tecnología al uso contrario al que se pretende. La implementación segura de la inteligencia artificial depende de la integración en las estructuras organizativas existentes. Aprovechar y asegurar el aprendizaje automático requiere entonces un enfoque socio-técnico. Al parecer, la inteligencia artificial (IA) y el aprendizaje automático (ML) podrían ser la solución para cambiar el equilibrio "ofensivo-defensa" a favor de los ciberdefensores. Pero la realidad es más compleja.

Imagine los siguientes escenarios: un artefacto explosivo, un avión de combate enemigo y un grupo de rebeldes son identificados erróneamente como una caja de cartón, un águila o un rebaño de ovejas. Un sistema letal de armas autónomas identifica erróneamente a los vehículos de combate amigos como vehículos de combate enemigos. Las imágenes satelitales de un grupo de estudiantes en el patio de una escuela se malinterpretan como tanques en movimiento. En cualquiera de estas situaciones, las consecuencias de tomar acción son extremadamente aterradoras. Este es el tema importante del campo emergente del aprendizaje automático contradictorio.

https://www.afcea.org/signal-media/cyber-edge/securing-machine-learning-requires-sociotechnical-approach

MCDP 8, Información. Una nueva doctrina del Cuerpo de Marines para la función de guerra de información

El lanzamiento del Marine Corps Doctrinal Publications 8 (MCDP 8), Publicación Doctrinal 8 del Cuerpo de Marines sobre Información, marca el establecimiento de la primera doctrina para describir el propósito y mecánica de la séptima función de guerra de la Infantería de Marina, LA INFORMACIÓN. El propósito de MCDP 8, Información, es introducir un marco conceptual y dinámico para comprender y emplear la función de combate de información, además de proporcionar a los infantes de marina una mayor flexibilidad en sus enfoques operativos en todas las fases de la competencia continua, en todos los dominios de combate.

Publicamos aquí sus 126 páginas en cuya introducción, el Comandante del Cuerpo de Marines General, US Marine Corps DAVID H. BERGER expresa: "…el mundo ha profundizado nuestra dependencia colectiva de la información en la medida en que una mínima vulnerabilidad en la forma en que manejamos, almacenamos, o transmitamos información podría poner en peligro a los Marines, sus familias, y todo lo que hemos jurado defender…"

https://mca-marines.org/wp-content/uploads/MCDP-8-Information.pdf

https://www.marines.mil/Portals/1/Publications/MCDP%208.pdf

La informática y el desafío del campo de batalla

La conectividad, las redes y la gestión técnica se encuentran entre las principales prioridades de los diseñadores de informática robusta para combatientes móviles. Es una tendencia el centrado de las fuerzas armadas en la conectividad del comando y control conjunto de todos los dominios (JADC2) a medida que el sector de la computación militar-aeroespacial toma vigencia en el año 2022. El objetivo de JADC2 es compartir datos en todos los dominios de forma rápida y segura. El entorno operativo actual requiere redes compatibles con todas las fuerzas, para permitir una óptima conciencia situacional y toma de decisiones.

https://www.militaryaerospace.com/computers/article/14232798/military-aerospace-rugged-computing-computers?

CIBERSEGURIDAD

Fuerza Laboral de Educación Cibernética de la Casa Blanca

La nueva ley es una oportunidad para hacer crecer la experiencia cibernética. El programa de fuerza laboral permitirá a los empleados federales avanzar en las habilidades cibernéticas a través de puestos rotativos.

Con la Ley Federal del Programa rotativo de la fuerza laboral cibernética (Ley Pública 117-149) en vigor, los empleados federales tendrán la oportunidad de rotar a puestos relacionados con el ciberespacio en otras agencias. El programa de cinco años permitirá que el personal en tecnología de la información, ciberseguridad u otros puestos relacionados con la cibernética se postule a un puesto de fuerza laboral cibernética.

https://www.afcea.org/signal-media/cyber-edge/new-law-opportunity-grow-cyber-experience

CIBERDEFENSA

Conociendo al Comando Conjunto de Ciberdefensa – Entrevista con el Gral. Anibal Intini

Victoria Pierucci - 26 julio, 2022

En el intercambio que tuvo el General Intini con **Zona Militar** se pudo abordar la importancia que tiene el Comando Conjunto de Ciberdefensa en materia de ciber-amenazas contra las infraestructuras críticas y sobre los sistemas que poseen las Fuerzas Armadas Argentinas, además de repasar conceptos de las dinámicas de seguridad que existen en la actualidad.

https://www.zona-militar.com/2022/07/26/conociendo-al-comando-conjunto-de-ciberdefensa-entrevista-con-el-gral-anibal-intini/

Criptografía Poscuántica

El término "criptografía poscuántica" a menudo se denomina "criptografía resistente a la cuántica" e incluye "algoritmos o métodos criptográficos que se evalúan como no específicamente vulnerables al ataque de un CRQC [computadora cuántica criptoanalíticamente relevante] o computadora clásica".

Si bien la computación cuántica promete una velocidad y potencia sin precedentes en la informática, también plantea nuevos riesgos.

Reflexiones acerca de cómo prepararse para la transición ahora siguiendo la hoja de ruta de criptografía poscuántica.

https://www.dhs.gov/quantum

Prepárese para un nuevo estándar criptográfico para protegerse contra futuras amenazas basadas en la cuántica

El Instituto Nacional de Estándares y Tecnología (NIST) ha anunciado que un nuevo estándar criptográfico poscuántico reemplazará la criptografía de clave pública actual, que es vulnerable a los ataques basados en la cuántica.

El término "criptografía poscuántica" a menudo se conoce como "criptografía resistente a la cuántica" e incluye "algoritmos o métodos criptográficos que se evalúa y que no son específicamente vulnerables al ataque de una CRQC [computadora cuántica criptoanalíticamente relevante] o sea una computadora clásica".

https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum

Memorandum de Seguridad Nacional sobre la Promoción del Liderazgo de los Estados Unidos en computación cuántica al tiempo que mitiga los riesgos para los sistemas criptográficos vulnerables

MAYO 04, 2022•DECLARACIONES Y COMUNICADOS

Este memorándum describe las políticas e iniciativas del Presidente de las US relacionadas con la computación cuántica. Identifica los pasos claves necesarios para mantener la ventaja competitiva de la nación en la ciencia de la información cuántica (QIS), al tiempo que mitiga los riesgos de las computadoras cuánticas para la seguridad cibernética, económica y nacional de la nación.

https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Los sistemas convergentes amplían la superficie de ataque. (*Por George I. Seffers)*

La Internet de las Cosas (IoT) está creciendo. Permite que humanos y también todos los dispositivos y objetos del entorno se conecten a través de Internet para compartir sus datos y crear nuevas aplicaciones y servicios que resulten en un estilo de vida más conveniente y conectado. Sin embargo, la arquitectura IoT centralizada enfrenta varios problemas. Por ejemplo, todas las operaciones informáticas de todos los nodos de la red se llevan a cabo utilizando un único servidor, creando un punto de falla único, si el servidor se cae, todo el sistema deja de estar disponible.

La arquitectura centralizada de IoT es un objetivo fácil de varios tipos de ataques de seguridad y privacidad, ya que todos los datos de IoT recopilados desde diferentes dispositivos están bajo la autoridad total de un único servidor. La integración del sistema IoT con la tecnología blockchain puede proporcionar varios beneficios que pueden resolver los problemas asociados con la arquitectura centralizada de IoT.

https://www.sciencedirect.com/science/article/abs/pii/S0065245818300688

TECNOLOGÍA

Google y la Inteligencia Artificial (IA)

Por Bernardo Marr

Las herramientas de IA de Google Cloud cuentan con lo mejor de la investigación y tecnología de Google para ayudar a los desarrolladores a enfocarse de forma exclusiva en resolver problemas importantes.

Cada vez que usted busca algo en Google, la inteligencia artificial está trabajando entre bastidores para generar respuestas a su consulta.

Un sistema de aprendizaje profundo llamado RankBrain ha cambiado la forma en que funciona el motor de búsqueda. En muchos casos, RankBrain maneja las consultas de búsqueda mejor que las reglas algorítmicas tradicionales codificadas a mano por ingenieros humanos, y Google se dio cuenta hace mucho tiempo de que la IA es el futuro de su plataforma de búsqueda.

https://bernardmarr.com/how-does-google-use-artificial-intelligence/

CIBERCONFIANZA

Google niega haber creado una inteligencia artificial sintiente, como alerta uno de sus ingenieros

Por Carlos del Castillo

La multinacional suspende a un trabajador por defender que uno de sus programas puede ser el primer ejemplo de "vida inteligente artificial", algo en lo que los expertos discrepan.

¿Es LaMDA la inteligencia artificial autoconsciente que soñaron investigadores y aficionados a la ciencia ficción durante décadas?

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiY64vY_KP5AhXNtJUCHfBxCcoQFnoECAgQAQ&url=https%3A%2F%2Fwww.eldiarioar.com%2Fmundo%2Fgoogle-niega-haber-creado-inteligencia-artificial-sintiente-alerta-ingenieros_1_9083638.html&usg=AOvVaw1REll2s2gq113aeWBYPJsS

Informes de interés:

1. Maui Ransomware de ataque a la salud Pública: https://www.cisa.gov/uscert/ncas/current-activity/2022/07/06/north-korean-state-sponsored-cyber-actors-use-maui-ransomware
2. Actualizaciones de Chrome: https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop.html
3. Ransomware MedusaLocker: https://www.cisa.gov/uscert/ncas/current-activity/2022/06/30/stopransomware-medusalocker
4. Las 25 debilidades más peligrosa del software: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

CIBERFORENSIA

Informes Semanales

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)

Semana del 20 de junio de 2022: https://www.cisa.gov/uscert/ncas/bulletins/sb22-178

Semana del 27 de junio de 2022: https://www.cisa.gov/uscert/ncas/bulletins/sb22-185

Semana del 4 de julio de 2022: https://www.cisa.gov/uscert/ncas/bulletins/sb22-192

Semana del 11 de julio de 2022: https://www.cisa.gov/uscert/ncas/bulletins/sb22-199

Semana del 18 de julio de 2022: https://www.cisa.gov/uscert/ncas/bulletins/sb22-206

CIBERCRIMEN

APT norcoreanos en busca y captura por los EE.UU.

Por Luciano Miguel Tobaría

El gobierno estadounidense ha decidido aumentar la recompensa ofrecida por cualquier tipo de información relacionada con los grupos de amenazas avanzadas persistentes (APT, *Advanced Persistent Threat*) norcoreanos. El gran impacto que están suponiendo las actividades ilícitas de estos grupos debido, entre otros, al robo de criptomonedas y al espionaje industrial ha motivado el incremento de las recompensas hasta los diez millones de dólares.

Los grupos APT que más preocupan al Departamento de Estado son: Grupo Lazarus, Andariel, Bluenoroff (APT38) y Kimsuky, debido a que sospechan que están involucrados en ataques contra infraestructuras críticas de los EE.UU.

https://unaaldia.hispasec.com/2022/07/apt-norcoreanos-en-busca-y-captura-por-los-ee-uu.html

LockBit reclama ataque de ransomware a la agencia tributaria italiana

Por **Sergiu Gatlan**

Las autoridades italianas están investigando las afirmaciones hechas por la banda de ransomware LockBit de que violaron la red del Servicio de Impuestos Internos italiano (L'Agenzia delle Entrate).

LockBit afirma que robaron 100 GB de datos (incluidos documentos de la compañía, escaneos, informes financieros y contratos) que se filtrarán en línea si la agencia tributaria italiana no paga una demanda de rescate hasta el 1 de agosto.

https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-italian-tax-agency/

Usan códigos QR para atacar redes sociales

El gigante web chino Tencent admitió un importante ataque de secuestro de cuentas en su plataforma de mensajería y redes sociales QQ.com.

Todo comenzó el domingo por la noche, el cual en la plataforma de mensajería y redes sociales QQ.com de Tencent advirtieron que un número no identificado de usuarios reportaban que sus credenciales no les permitían acceder a sus cuentas. Los hechos señalaban a un ataque de secuestro de cuentas dirigido a usuarios de QQ.

Usted no debiera escanear códigos QR de origen desconocido y siempre prestar especial atención cuando se solicitan credenciales en un entorno no habitual.

https://www.theregister.com/2022/06/28/tencent_qq_qr_code_attack/

NOVEDADES

El próximo capítulo de la saga criptográfica

Elena Kozhemyakina | Eduardo R. Abreu I Dr. Stylianos Kampakis I Igor Ilyinsky

18 de mayo de 2022 | 62 minutos

En el episodio 21 de Driving Fintech Forward, te unirás a los líderes de Crypto y DeFi mientras comparten una guía completa del mundo de los DAO (Organización Automática Descentralizada) y ofrecen información exclusiva sobre el futuro de las finanzas en el contexto de DeFi.
Los temas de discusión incluyen:
- Criptoeconomía y el impacto de los DAO en el crecimiento de los cripto -
Toma de decisiones descentralizada: comprender los DAO y cómo funcionan
- Una guía para principiantes para invertir en DAO
- El impacto de los DAO en las finanzas tradicionales: ¿Disrupción o transformación?
- Ejemplos de DAO y oportunidades de innovación - Y más...

https://www.brighttalk.com/webcast/18463/524673?player-preauth=znM6xvkq09BamAIdGXmF5am84%2F55Iwwvs%2B1KOobsvKA%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience356479&utm_campaign=AUD-11724&utm_content=2022-05-2