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° 45
Junio 2022

OAC Boletín de Junio 2022

"'Los estados líderes modernos manejan las comunicaciones, navegación, reconocimiento, todo el comando de las fuerzas nucleares estratégicas y de defensa aeroespacial, y armas convencionales de alta precisión a través del espacio. Interrumpir este sistema entero a través de la radio-electrónica y otros medios asimétricos podría reducir en gran medida esta ventaja del adversario''

General de Ejército Mahmut Gareyev
¿Cómo desarrollar un ejército moderno? .

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), **es un micro-sitio de la Escuela Superior de Guerra Conjunta de la Facultad Militar Conjunta, 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 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 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 Pentágono pide nuevas ideas en la "tercera ola" de la evolución de la IA

La Agencia de Proyectos de Investigación Avanzada de Defensa está solicitando formalmente contratos para su nuevo programa Enabling Confidence, una subsección dentro de su iniciativa de Exploración de Inteligencia Artificial, para mejorar el procesamiento algorítmico en los proyectos de inteligencia artificial del Pentágono. El programa se enfoca en lo que DARPA define como su "tercera ola" de investigación de inteligencia artificial, que incluye la teoría de la IA y la investigación de aplicaciones que examina las limitaciones con las teorías de reglas y aprendizaje estadístico que ocultan las tecnologías de IA.

https://www.nextgov.com/emerging-tech/2022/06/pentagon-launches-third-wave-ai-initiative-help-warfighting-effort/367736/

https://www.defenseone.com/technology/2022/06/darpas-new-3rd-wave-ai-aims-compute-accuracyand-uncertainty/367741/

CIBERSEGURIDAD

Ciberseguridad, gestión de riesgos de la cadena de suministros

Los usuarios de tecnologías de la información, las comunicaciones y las operaciones (TIC/OT) confían en un ecosistema de cadena de suministro complejo, globalmente distribuido e interconectado para proporcionar soluciones altamente refinadas, rentables y reutilizables. Este ecosistema está compuesto por varias entidades con múltiples niveles de subcontratación, diversas rutas de distribución, diversas tecnologías, leyes, políticas, procedimientos y prácticas, todos los cuales interactúan para diseñar, fabricar, distribuir, implementar, usar, mantener, desechar y de lo contrario administrar productos y servicios. Estos aspectos de la cadena de suministro incluyen TI, OT, comunicaciones, Internet de las cosas (IoT) e IoT industrial.

https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

https://www.nist.gov/news-events/news/2021/04/comments-sought-updates-cyber-supply-chain-risk-management-practices

CIBERDEFENSA

En este sitio usted puede inscribirse y obtener un informe acerca de la guerra en Ucrania, como crea un cambio fundamental en el panorama de amenazas cibernéticas, en él se analizan los eventos cibernéticos que acompañaron a la invasión rusa de Ucrania y las implicaciones potenciales para la industria de (rea) seguros.

https://insights.cybcube.com/war-in-ukraine-report?utm_term=about%20cyber%20security&utm_campaign=Report:+War+in+Ukraine+%7C+FY22_Q2&utm_source=adwords&utm_medium=ppc&hsa_acc=1114695891&hsa_cam=16498459648&hsa_grp=137145863507&hsa_ad=586331740978&hsa_src=g&hsa_tgt=kwd-5475693248&hsa_kw=about%20cyber%20security&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjw7vuUBhBUEiwAEdu2pB08l7ISjqRegWO3nLQ7RldewugZLYoc1NvfnpY9r-5Fj8Fm4OaeIRoC3ykQAvD_BwE

En este otro sitio usted puede inscribirse y obtener un informe sobre amenazas globales, actualiza la actividad de amenazas y predicciones para el primer semestre de 2022, analiza el panorama de las amenazas a la ciberseguridad, sus características importantes y sus posibles impactos.

https://insights.cybcube.com/global-threat-briefing-h1-2022?utm_term=about%20cyber%20security&utm_campaign=Report:+War+in+Ukraine+%7C+FY22_Q2&utm_source=adwords&utm_medium=ppc&hsa_acc=1114695891&hsa_cam=16498459648&hsa_grp=137145863507&hsa_ad=586331740978&hsa_src=g&hsa_tgt=kwd-5475693248&hsa_kw=about%20cyber%20security&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjw7vuUBhBUEiwAEdu2pHsOno3wF3fyNVwxbGVqVFM9U8LfEfRv1xb1lDfehi4poU22nyrNJBoCoHAQAvD_BwE

TECNOLOGÍA

El laboratorio de IA de Meta ha creado un modelo de lenguaje nuevo y masivo

El nuevo y masivo lenguaje comparte tanto las habilidades notables como los defectos dañinos de la red neuronal pionera GPT-3 de OpenAI . Y en un movimiento sin precedentes Big Tech, lo está regalando a los investigadores, junto con detalles sobre cómo se construyó y entrenó

Joelle Pineau, una defensora de la transparencia en el desarrollo de tecnología desde hace mucho tiempo, que ahora es directora general de Meta AI, dice:“Creemos firmemente que la capacidad de que otros analicen su trabajo es una parte importante de la investigación. Realmente invitamos a esa colaboración”.

Es la primera vez que un modelo de lenguaje grande de Meta, completamente probado estará disponible para cualquier investigador que quiera estudiarlo. La noticia ha sido bien recibida por muchos preocupados por la forma en que pequeños equipos construyen esta poderosa tecnología a puertas cerradas.

https://www.technologyreview.com/2022/05/03/1051691/meta-ai-large-language-model-gpt3-ethics-huggingface-transparency/?utm_source=acquisition&utm_medium=email&utm_campaign=WKLYSUN&utm_content=06.05.22.engaged_non-subs&mc_cid=0aeba9054d&mc_eid=d7a96b5b35

CIBERCONFIANZA

Algunas exageraciones entorno a las actuales capacidades de la IA

DeepMind presentó un nuevo modelo de IA “generalista” llamado Gato . El modelo puede jugar videojuegos de Atari, subtitular imágenes, chatear y apilar bloques con un brazo robótico real, anunció el laboratorio de inteligencia artificial propiedad de Alphabet. En total, Gato puede realizar 604 tareas diferentes.

Uno de los principales investigadores de DeepMind y coautor del artículo de Gato, Nando de Freitas, no pudo contener su entusiasmo. "¡El juego ha terminado!" tuiteó , sugiriendo que ahora hay un camino claro de Gato a la inteligencia artificial general, o AGI, un vago concepto de IA de nivel humano o sobrehumano. La forma de construir AGI, afirmó, es principalmente una cuestión de escala: hacer modelos como el Gato más grandes y mejores.

“AGI habla de algo profundamente humano: la idea de que podemos llegar a ser más de lo que somos, construyendo herramientas que nos impulsen a la grandeza”, dice. “Y eso es realmente bueno, excepto que también es una forma de distraernos del hecho de que tenemos problemas reales que enfrentamos hoy y que deberíamos tratar de abordar utilizando IA”.

https://www.technologyreview.com/2022/05/23/1052627/deepmind-gato-ai-model-hype/?utm_source=acquisition&utm_medium=email&utm_campaign=WKLYSUN&utm_content=06.05.22.engaged_non-subs&mc_cid=0aeba9054d&mc_eid=d7a96b5b35

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 16 de Mayo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-143

Semana del 23 de Mayo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-150

Semana del 30 de mayo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-157

Semana del 06 de junio https://www.cisa.gov/uscert/ncas/bulletins/sb22-164

Semana del 13 de junio https://www.cisa.gov/uscert/ncas/bulletins/sb22-171

Informes de interés:

1. información del grupo de extorsión de datos de Karakurt: CISA, la Oficina Federal de Investigaciones (FBI), el Departamento del Tesoro y la Red de Ejecución de Delitos Financieros (FinCEN) han publicado un Aviso de Ciberseguridad (CSA) conjunto para proporcionar información sobre el grupo de extorsión de datos de Karakurt. Los actores de Karakurt roban datos y amenazan con subastarlos o revelarlos al público a menos que reciban el pago del rescate exigido.

   https://www.cisa.gov/uscert/ncas/current-activity/2022/06/01/karakurt-data-extortion-group

2. Microsoft ha publicado una guía de solución para la vulnerabilidad, conocida como "Follina" que afecta a la herramienta de diagnóstico de soporte de Microsoft (MSDT) en Windows. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para tomar el control de un sistema afectado. Microsoft ha informado sobre la explotación activa de esta vulnerabilidad

   https://www.cisa.gov/uscert/ncas/current-activity/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability

3. Análisis de Riesgos y Vulnerabilidades de CISA del año 2021:

   CISA ha publicado un análisis e infografía que detalla los hallazgos de las 112 evaluaciones de riesgo y vulnerabilidad (RVA) realizadas en múltiples sectores en el año fiscal 2021 (FY21).

   https://www.cisa.gov/uscert/ncas/current-activity/2022/05/19/cisa-releases-analysis-fy21-risk-and-vulnerability-assessments

NSO confirma que el spyware Pegasus ha sido utilizado por al menos 5 países europeos

La empresa israelí de ciberseguridad NSO Group declaró a los legisladores europeos el martes 21 de este mes que al menos cinco países de la UE han utilizado su software y que la empresa ha rescindido al menos un contrato con un país miembro de la UE tras el abuso de su software de vigilancia Pegasus.

Reconociendo que había «cometido errores», la empresa también hizo hincapié en la necesidad de una norma internacional que regule el uso gubernamental del software espía.

Pegasus y sus otras contrapartes, como FinFisher y Cytrox, están diseñados para instalarse sigilosamente en un teléfono inteligente mediante la explotación de vulnerabilidades desconocidas en el software conocido como día cero para tomar el control remoto del dispositivo y recopilar datos confidenciales.

https://thehackernews.com/2022/06/nso-confirms-pegasus-spyware-used-by-at.html

CIBERCRIMEN

La Inteligencia Artificial aplicada a la prevención y detección de lavado de activos y financiamiento del terrorismo – Publicado por la Ing. Laura Bonilla Murillo, San José de Costa Rica

El lavado de dinero y financiamiento del terrorismo son de los temas principales en nuestra actualidad, ya que tanto instituciones gubernamentales como privadas han emprendido una ardua lucha en contra de estas acciones. Sin embargo muchas veces es limitado el esfuerzo en contraste con el ingenio de los malhechores para colocar y movilizar dinero ilícito en nuestras redes legales. Políticas, lineamientos y procedimientos son conocidos y estudiados por los delincuentes de manera que se las ingenian para pasar desapercibidos en tanto continúan movilizando dinero de fuentes ilícitas y utilizando a las instituciones bancarias como medio para la consecución de sus fechorías. El mercado se renueva continuamente y sus avances tecnológicos son cada vez mayores, ya no enfrentamos solamente amenazas físicas sino también tecnológicas, por lo que debemos innovar nuevas estrategias y herramientas para estar un paso adelante de los malhechores en estas áreas. La Inteligencia Artificial nos brinda opciones como Sistemas Expertos, Redes Neuronales, Algoritmos Genéticos y Lógica difusa, entre otros, que amplían nuestro panorama permitiendo tener visualización completa de lo que ocurre a nuestro alrededor y en nuestros sistemas, habilitando a los encargados respectivos para detectar no solamente señales de comportamientos anómalos, sino analizando detalladamente cada movimiento y comparando con información colateral para identificar potenciales lavadores de dinero. Lo ideal es ir más allá de lo que nuestros ojos pueden ver y detectar a los lavadores de dinero antes de que intenten realizar los movimientos evidentes de una operación inusual.

http://felaban.s3.amazonaws.com/noticias/archivo20141107151058PM.pdf

https://www.oas.org/es/ssm/ddot/publicaciones/LIBRO%20OEA%20LAVADO%20ACTIVOS%202018_4%20DIGITAL.pdf

NOVEDADES

Samsung renovó su teléfono de gama media Galaxy A52 con una versión compatible con redes 5G. Es el modelo que lidera la estrategia de la compañía por reforzar su presencia en el segmento, y que en 2021 sumó una versión compatible con conectividad 5G en la Argentina.

https://www.oas.org/es/ssm/ddot/publicaciones/LIBRO%20OEA%20LAVADO%20ACTIVOS%202018_4%20DIGITAL.pdf