OAC Boletín de Marzo-Abril-Mayo 2023

Las actividades características de la guerra pueden dividirse en dos categorías principales: aquellas que son meramente preparatorias para la guerra y la guerra propiamente dicha.

-Carl von Clausewitz (del libro On War)

"Lo único que sabemos con certeza es que este tipo de capacidades serán absolutamente cruciales. Y quien tenga las mejores capacidades de tipo ChatGPT será dominante por toda una serie de razones"

John Ridge,
Director de innovación de defensa del Ministerio de Defensa Reino Unido de Gran Bretaña.
https://www.nationaldefensemagazine.org/articles/2023/3/8/pentagons-top-ai-official-addresses-chatgpts-possible-benefits-risks

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

Porqué el Pentágono no confía en ChatGPT

Imagine una versión militarizada de ChatGPT, entrenada en inteligencia secreta. En lugar de reconstruir laboriosamente entradas de bases de datos dispersas, transmisiones interceptadas e informes de noticias, un analista escribe una consulta rápida en un lenguaje sencillo y obtiene, en segundos, un resumen conciso: una predicción de acción hostil, por ejemplo, o un perfil de un terrorista. ¿Pero esa salida es verdadera? Con la tecnología actual, no puede contar con ella en absoluto. Por ahora, al menos, la IA generativa tiene un defecto fatal: inventa cosas. "Estoy entusiasmado con el potencial", dijo el teniente general (retirado) Jack Shanahan, director fundador del Centro Conjunto de Inteligencia Artificial (JAIC) del Pentágono de 2018 a 2020. "Juego con Bing AI, uso ChatGPT con bastante regularidad, [pero] no hay ningún analista de inteligencia en este momento que use estos sistemas de otra manera que no sea con cierta precaución".

https://www.c4isrnet.com/artificial-intelligence/2023/03/01/chatgpt-can-make-short-work-of-pentagon-tasks-air-force-cio-says/

El principal funcionario de IA del Pentágono aborda los posibles beneficios y riesgos de ChatGPT

por Stew Magnuson

La persona clave del Departamento de Defensa para la inteligencia artificial dijo que el nuevo hatbot ChatGPT que está tomando al mundo por sorpresa podría ser una bendición para la seguridad nacional y un motivo de preocupación.

"Hay muchas cosas buenas allí en términos de cómo podemos utilizar grandes modelos de lenguaje como este para incluir en funciones críticas en todo el departamento", dijo Kimberly Sablon, directora principal de IA confiable y autonomía en la oficina del subsecretario de defensa para investigación e ingeniería, el 7 de marzo en la Conferencia de Ciencia y Tecnología Operacional del Pacífico en Hawai.

Pentagon's Top AI Official Addresses ChatGPT's Possible Benefits, Risks (nationaldefensemagazine.org)

https://www.nationaldefensemagazine.org/articles/2023/3/8/pentagons-top-ai-official-addresses-chatgpts-possible-benefits-risks

Las comunicaciones en red y las constelaciones Satelitales

El aislamiento histórico de los sistemas heredados creó una arquitectura que en los EU dio en llamarse "tubo de estufa", que ya no satisface las necesidades de las capacidades espaciales y de la guerra modernas. Los sistemas que no se comunican entre sí son más lentos para recibir y procesar información, lo que afecta la toma de decisiones y las capacidades de respuesta. En consecuencia, es fundamental generar una arquitectura de red que conecte a la perfección las capacidades terrestres con las espaciales conformando una arquitectura multidominio.

Los extraordinarios volúmenes de datos, los requisitos de interoperabilidad y la necesidad de procesos analíticos a la velocidad de la misión son herramientas que permiten a los líderes de la defensa y el espacio tomar decisiones mejores y más seguras, pero las mismas deben ser apoyadas por una red que permita una rápida recopilación y colaboración.

La técnica Joint All Domain Command and Control (JADC2) del Departamento de Defensa de los EEUU (DoD) es un ejemplo de esta reinvención de la colaboración.

https://www.defenseone.com/sponsors/2022/12/communication-constellation-integrated-network-and-ussf/381351/

La ciudad de Buenos Aires tiene su plan de Inteligencia Artificial

Primer plan de la Ciudad que busca generar un impacto positivo en todos los ámbitos de la vida de los ciudadanos a través del desarrollo y uso de la inteligencia artificial. Centros de Formación Profesional (CFP) y Trayectos Formativos, Formación Técnica Superior y Educación No Formal

https://buenosaires.gob.ar/jefaturadegabinete/innovacion/plan-de-inteligencia-artificial

Acerca de los tipos de Inteligencia Artificial

¿Cuáles son los 3 tipos de Inteligencia Artificial? Esta es una de las tecnologías más innovadoras y disruptivas de nuestro tiempo. Gracias a ella, se pueden crear sistemas capaces de aprender, adaptarse y realizar tareas que antes solo eran posibles para los seres humanos. En términos generales, se pueden identificar tres tipos de IA: la IA débil, la IA fuerte y la IA superinteligente.

https://www.msn.com/es-ar/noticias/tecnologia/conoce-los-3-tipos-de-inteligencia-artificial-y-c%C3%B3mo-se-usan-en-tu-vida-diaria/ar-AA19ANnZ

'Tengo que estar allí temprano': lecciones estadounidenses de operaciones especiales de Ucrania

El comandante entrante del Comando de Operaciones Especiales de los Estados Unidos (USSOCOM), General del Ejército Bryan Fenton, habla durante una ceremonia de Cambio de Mando de USSOCOM

Dijo que Estados Unidos se enfrentaba a una colisión sin precedentes de amenazas al orden internacional, lo que llamó "olas de consecuencia".

Ayudando a contrarrestar esas amenazas, está el enfoque de las operaciones especiales en las tecnologías emergentes: integración de inteligencia artificial, procesamiento de lenguaje natural, capacidades "basadas en datos", sistemas robóticos y autónomos no tripulados.

Señaló además la importancia del ciberespacio y el espacio mismo en las operaciones modernas, tan integrales que Forman una tríada SOF-ciberespacio.

https://breakingdefense.com/2023/05/gotta-be-there-early-american-special-ops-lessons-from-ukraine/

CIBERDEFENSA

Informe Acerca de las Capacidades Rusas en el Ciberespacio

Rafael García Hernández, comandante del Mando Conjunto de Ciberespacio del Estado Mayor de la Defensa de España, en una sesión organizada por la Universidad Internacional de La Rioja. habló de la protección del espacio cibernético del reino y sobre la guerra de Ucrania,

"Habíamos sobrevalorado las capacidades de Rusia, tanto las clásicas de su ejército como sus habilidades en el ciberespacio. Todos pensamos que la gran potencia iba a machacar a Ucrania, pero "Ucrania ha sido capaz de mantener su libertad en el ciberespacio y ha demostrado como esto condiciona la geoestrategia", afirmó Rafael García Hernández, general de división del Ejército del Aire y del Espacio y comandante del Mando Conjunto de Ciberespacio del Estado Mayor de la Defensa de España, hizo esta reflexión en la "El espacio cibernético, una dimensión de los conflictos del siglo XXI", Se adjunta hipervínculo de la clase referenciada.

"Ucrania empezó a desarrollar su estrategia en el ciberespacio desde la invasión de Crimea. Actualmente, cuenta con un Ministerio de Tecnología e Innovación y ha sabido establecer las alianzas estratégicas -por ejemplo con Microsoft- que le han ayudado a estar donde está", prosiguió el comandante.

https://www.unir.net/actualidad/vida-academica/el-maximo-responsable-de-la-ciberseguridad-en-el-estado-mayor-de-la-defensa-de-espana-en-unir-habiamos-sobrevalorado-las-capacidades-de-rusia-en-el-ciberespacio/

https://www.unir.net/evento/openclass/espacio-cibernetico/

Hacia inteligencias artificiales realmente inteligentes

Este artículo de Ramón López de Mántaras, contiene algunas reflexiones sobre inteligencia artificial (IA), explicando las diferencias entre la IA fuerte y la débil y los conceptos relacionados de IA general y específica.,El autor señala que todas las manifestaciones actuales de IA son débiles y específicas. A lo largo del mismo se describen brevemente los principales modelos, insistiendo en la importancia de la corporalidad como aspecto clave para conseguir una IA de naturaleza general.

https://www.bbvaopenmind.com/articulos/el-futuro-de-la-ia-hacia-inteligencias-artificiales-realmente-inteligentes/

CIBERGUERRA

Rusia versus Ucrania y el papel de las radios definidas por software

Se presenta un interesante resumen de la situación de Guerra Electrónica (GE) en el conflicto Rusia-Ucrania.

Con la guerra actual en Ucrania, está claro que el programa de modernización de Rusia ha involucrado la guerra electrónica y la inteligencia de señales y jugó un papel importante en los avances de combate de Rusia y el posicionamiento general que condujo a la invasión real.

La guerra electrónica se puede dividir en tres componentes: ataque electrónico, protección electrónica o contramedidas y apoyo electrónico. El objetivo es detectar, interceptar, identificar, ubicar, grabar/reproducir y/o analizar fuentes de energía electromagnética radiada para el reconocimiento inmediato de amenazas y ayudar en la inteligencia general y la toma de decisiones estratégica.

La guerra electrónica está ahora en el corazón de la guerra moderna, un componente o incluso un reemplazo del combate tradicional. Las batallas y las guerras se pueden ganar o perder en función de derrotar la ventaja tecnológica del oponente en el espectro de frecuencia y también se pueden usar para infiltrarse en las comunicaciones en tiempos de paz. Las tecnologías de radiofrecuencia (radios tácticas, radar, señales de posicionamiento y navegación, sistemas de armas y varios detectores para coordinar operaciones y encontrar al enemigo) son fundamentales para las fuerzas militares.

https://www.afcea.org/signal-media/cyber-edge/russia-versus-ukraine-and-role-software-defined-radios?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=dHfn8

Sistemas EW de avanzada de los F 39 Gripen E Brasileños

Saab habla sobre cómo el sistema de guerra electrónica del caza F-39 Gripen E, el nuevo caza de la Fuerza Aérea Brasileña crea dominio aéreo.

https://www.saab.com/products/gripen-e-series

https://aeroin.net/saab-fala-sobre-como-o-sistema-de-guerra-eletronica-do-caca-gripen-e-cria-a-dominancia-do-ar/

La inteligencia de fuente abierta para contrarrestar las amenazas

Cuando la mayoría de las personas escuchan la palabra inteligencia en un contexto político, inmediatamente piensan en fuentes clandestinas, espías y reuniones secretas. Los servicios de inteligencia todavía dependen de la inteligencia de fuente humana (HUMINT) y las comunicaciones interceptadas (SIGINT). Sin embargo, en el siglo XXI, la inteligencia de código abierto (OSINT) se ha vuelto indispensable para comprender a sus adversarios y, a menudo, es la fuente principal y más valiosa de inteligencia procesable. Según un artículo detallado que destaca el poder de OSINT en el *Wall Street Journal*, "el 80% de lo que un presidente o comandante militar de EE. UU. necesita saber proviene de Fuentes abiertas OSINT".

https://nationalinterest.org/blog/buzz/open-source-intelligence-indispensable-countering-threats-206271

Los comandos cibernéticos, espaciales y de operaciones especiales del ejército, se integran bajo el nuevo concepto de “TRIADA“

El Ejército de los Estados Unidos ha estado estudiando en cómo vincular su Comando de Operaciones Especiales, su Comando de Defensa Espacial y de Misiles y su Comando Cibernético más estrechamente en el campo de batalla, bajo un nuevo concepto de "tríada".

El objetivo es, integrar mejor las capacidades de cada comando para unir operaciones más complejas y efectivas en un mundo donde los adversarios pueden operar en múltiples dominios a la vez.

Las operaciones incluyen opciones letales en el mundo físico combinadas con opciones no letales, como la guerra de información o la cibernética.

https://breakingdefense.com/2022/08/army-cyber-space-and-special-operations-commands-integrating-under-new-triad-concept/

La resiliencia en la carrera espacial

La proliferación de sistemas basados en el espacio está siendo impulsada y habilitada por nuevas tecnologías, que van desde buques y satélites hasta 5G. Las fuerzas armadas de los EE. UU. confiarán en los recursos espaciales como nodos en las redes globales para permitir su concepto de combate conjunto y todas los dominios (JADC2). Además de las aplicaciones de defensa e inteligencia, el espacio influye cada vez más en amplias franjas de las economías globales, dando forma a sectores que van desde el transporte hasta la agricultura, lo que a su vez hace que el espacio sea cada vez más un problema de seguridad económica.

https://breakingdefense.com/2021/08/amid-space-race-cybersecurity-and-resiliency-remain-concerns-experts/

CIBERCONFIANZA

Novedades sobre la inteligencia artificial (IA) generativa (ChatGPT)

ChatGPT puede expandir nuestro discurso intelectual: ¿Cómo sabremos si lo que leemos fue escrito por una IA y por qué es importante? ¿A quién respondemos cuándo comentamos un ensayo o artículo? Al observar la historia filosófica del diálogo, podemos reformular la pregunta para preguntar cómo podríamos usar estos nuevos chatbots en nuestro aprendizaje.

https://interestingengineering.com/culture/chatgpt-may-expand-discourse-research

Deberíamos tratar a las IA como participantes humanos en experimentos psicológicos

En su reciente entrevista con Lex Fridman , Eliezer Yudkowsky subraya la amenaza existencial que plantean las IA actuales y futuras, y lamenta el hecho de que no sabemos realmente qué está pasando dentro de estas gigantescas "matrices de números de coma flotante". Traza un paralelo con la neuroimagen, que nos permitió dar un salto en la comprensión del cerebro, con la esperanza de inventar una alternativa y aplicarla a estas IA.

https://realitybending.github.io/post/2023-04-04-psychologychatgpt/

Guía 2023 de procesamiento de modelos de lenguajes naturales

Los modelos de procesamiento de lenguaje natural (LLM, por sus siglas en inglés) han generado mucha expectación en los últimos meses. La demanda ha llevado al desarrollo

continuo de sitios web y soluciones que aprovechan los modelos lingüísticos. ChatGPT estableció el récord de la base de usuarios de más rápido crecimiento en enero de 2023, lo que demuestra que los modelos lingüísticos llegaron para quedarse. Esto también se demuestra por el hecho de que Bard, la respuesta de Google a ChatGPT, se presentó en febrero de 2023.

https://research.aimultiple.com/large-language-models/#what-is-a-large-language-model

https://www.ibm.com/mx-es/topics/natural-language-processing

ChatGPT y Bing AI. No son humanos y no les importa

Por supuesto, los chatbots de IA creados en modelos de procesamiento de lenguaje natural (LLM por sus siglas en inglés Large Language Models), como ChatGPT, Bard y Bing AI, son diferentes. Si bien la mayoría de la tecnología de inteligencia artificial que hemos encontrado durante la última década rara vez nos responde directamente (dejando de lado las respuestas de aviso único de Alexa y Siri), los Chatbots de hoy en día tienen que ver con la conversación.

https://www.techradar.com/opinion/stop-whining-about-chatgpt-and-bing-ais-mistakes-theyre-not-human-and-dont-care?ref=upstract.com

¿Quién vigila a los vigilantes?

"¿Quién vigila a los vigilantes?" Es una pregunta tan complicada que es casi imposible de responder, por la recurrencia de la situación. Siempre hay un vigilante que necesita ser vigilado. El artículo habla del origen de la frase, que ha llegado a nuestros días en múltiples formas: canciones, cómic, cine… Y todo se lo debemos al romano Juvenal, el mismo del "Pan y Circo", una frase con siglos de historia algunas reflexiones sobre ciber-vigilancia.

https://www.curistoria.com/2019/12/quien-vigila-a-los-vigilantes-la-frase-que-va-de-roma-a-watchmen.html

https://uniat.com/la-verdad-sobre-la-cibervigilancia/

¿Cuáles son los ciberataques más comunes?

Las nuevas tecnologías crean nuevas oportunidades delictivas, pero pocos tipos de delitos nuevos. ¿Qué distingue a los ciberataques de la actividad delictiva tradicional? Obviamente, una de las diferencias es el uso del computador digital, pero la tecnología por sí sola es insuficiente para cualquier distinción que pueda existir entre los distintos ámbitos de la actividad delictiva.

https://masterciberseguridadceupe.com/cuales-son-los-ciberdelitos-mas-comunes/

Compendio de ciberdelincuencia organizada

El presente compendio de casos publicado en Viena durante el año 2022 por la Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC), puede ser de utilidad para académicos, investigadores, profesionales, responsables de formular políticas, legisladores y proponentes de reformas legislativas. En última instancia, el compendio puede utilizarse como recurso sobre lo que supone la ciberdelincuencia organizada en todo el mundo e

intenta, en la medida de lo posible, que haya una representación equitativa de casos de diferentes regiones geográficas y ordenamientos jurídicos.

https://www.mpf.gob.ar/protex/files/2022/03/Digesto-de-casos-ciberdelincuencia-organizada.pdf

Como luchar contra la ciberdelincuencia y proteger a los adolescentes en internet

El Día de Internet Seguro, se celebra este 7 de febrero, una compañía de 'software' de seguridad estadounidense ha publicado consejos para que también las empresas mejoren sus defensas ante los ciberataques. La adicción a internet y a las redes sociales y el 'ciberbullying', han sido identificadas como las mayores amenazas de los adolescentes en internet, el portal advierte de los riesgos y ofrece a los padres diez consejos para proteger la seguridad 'online' de los jóvenes.

https://www.rtve.es/noticias/20170207/5-consejos-para-luchar-contra-ciberdelincuencia-10-para-proteger-adolescentes-internet/1486820.shtml

Europa y una nueva ley de cibernética

La Unión Europea (UE) está redactando una directiva innovadora para abordar la ciberseguridad y la privacidad de los datos, así como la Internet de las cosas (IoT).

Este borrador es una respuesta directa a los riesgos, como aclara el texto en su oración inicial: "Los productos de hardware y software están cada vez más sujetos a ciberataques exitosos".

https://www.afcea.org/signal-media/cyber-edge/europe-tackle-cyber-new-law?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=cHfn8

TECNOLOGÍA

Aspectos a considerar sobre la Inteligencia Artificial

La inteligencia artificial reúne un conjunto de tecnologías como muestra el gráfico, y se está convirtiendo en un tema controvertido entre las tecnologías de la cuarta revolución industrial, los aspectos más positivos, las oportunidades de progreso y los avances revolucionarios que promete el evento de la singularidad revolucionarán el mundo que viene, los presenta la Universidad de la singularidad (https://www.su.org/), en la otra mano, encontramos problemas éticos acerca de la capacidad de esta tecnología de manipular la decisión de la gente, aquí exponemos algunos artículos al respecto.

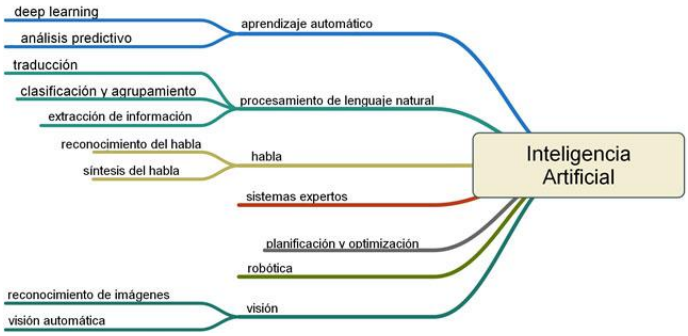

Ilustración 1: componentes de la IA
https://www.frbb.utn.edu.ar/utec/70/pasado_presente_futuro.html

- Pasado, presente y futuro de la Inteligencia Artificial: https://www.frbb.utn.edu.ar/utec/70/pasado_presente_futuro.html
- El futuro de la IA: hacia inteligencias artificiales realmente inteligentes: https://www.bbvaopenmind.com/articulos/el-futuro-de-la-ia-hacia-inteligencias-artificiales-realmente-inteligentes/

- La tecnología no tiene ética, pero la humanidad depende de ella: https://lab.elmundo.es/inteligencia-artificial/riesgos.html
- Google advierte: el verdadero peligro de la IA no son los robots asesinos sino los algoritmos sesgados: https://www.technologyreview.es//s/9610/google-advierte-el-verdadero-peligro-de-la-ia-no-son-los-robots-asesinos-sino-los-algoritmos
- El verdadero peligro inminente de la IA: https://elorientaldemonagas.com/el-verdadero-peligro-inminente-de-la-ia/
- Plataforma de inteligencia artificial de Microsoft: herramientas y servicios poderosos: https://www.microsoft.com/es-mx/ai/ai-platform
- Lea el eBook sobre la ética en la IA: https://news.microsoft.com/uploads/2018/02/The-Future-Computed_2.8.18.pdf

Los 15 mejores chatbots de inteligencia artificial en 2023:
https://blog.hubspot.es/service/chatbot-inteligencia-artificial

Inteligencia artificial. Aprendizaje automático profundo frente a redes neuronales: ¿cuál es la diferencia?

La tecnología se está integrando cada vez más en nuestra vida diaria y, para seguir el ritmo de las expectativas de los consumidores, las empresas confían más en los algoritmos de aprendizaje para facilitar las cosas. Puedes ver su aplicación en las redes sociales (a través del reconocimiento de objetos en fotos) o al hablar directamente con dispositivos (como Alexa o Siri).

https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks

¿Doctor ChatGPT? AI-bot casi pasa el examen de licencia médica de EE. UU.

IA-bot casi aprueba el examen de licencia médica de EE. UU.: Para probar, los científicos eliminaron las preguntas basadas en imágenes y procedieron a hacerle a ChatGPT 350 de las 376 preguntas . La herramienta de IA obtuvo una puntuación de entre el 52,4 % y el 75,0 % en los tres exámenes. El umbral de aprobación cada año es de aproximadamente el 60 por ciento.

https://interestingengineering.com/innovation/chatgpt-medical-licensing-exam?utm_source=newsletter&utm_content=newsletter-10-02-2023&utm_medium=greetings&utm_campaign=article

¿Qué es el Machine Learning?

El aprendizaje automático es una rama de la inteligencia artificial (IA) y la informática que se centra en el uso de datos y algoritmos para imitar la forma en que los humanos aprenden, mejorando gradualmente su precisión.

https://arxiv.org/pdf/1808.02342.pdf

https://www.ibm.com/topics/machine-learning

¿Qué es la robótica?

La robótica es una disciplina que se ocupa del diseño, operación, manufacturación, estudio y aplicación de autómatas o robots. Para ello, combina la ingeniería mecánica, ingeniería eléctrica, ingeniería electrónica, ingeniería biomédica y las ciencias de la computación, así como otras disciplinas.

https://concepto.de/robotica/#ixzz80scHZeAJ

https://concepto.de/robotica/

Automatización en la WEB Semántica Marco de Descripción de Recursos (RDF)

RDF es un método general para descomponer cualquier tipo de conocimiento en trozos pequeños, con algunas reglas acerca de la semántica o significado, de esas piezas. El punto es tener un método tan simple que puede expresar cualquier hecho, y a la vez tan estructurada que las aplicaciones informáticas pueden hacer cosas útiles con él.

Los miembros del Consorcio WWW (W3C) y otras partes interesadas han revisado este documento y el director lo ha aprobado como Recomendación W3C. Es un documento estable que se utilizará como material de referencia o se citará como referencia normativa en otros documentos. El papel del W3C al elaborar la Recomendación es llamar la atención sobre la especificación y promover un desarrollo generalizado de la misma. Esto enriquece la operatividad e interoperabilidad del Web.

http://www.sidar.org/recur/desdi/traduc/es/rdf/rdfesp.htm

http://www.w3.org/TR/1999/REC-rdf-syntax-19990222/errata

Para las finanzas, los riesgos de la cadena de bloques superan con creces sus recompensas

Por Hilary Allen (abril 5, 2023)

Las criptomonedas modernas surgieron en 2009 con el lanzamiento de Bitcoin, la primera moneda virtual consecuente que se basa en la tecnología blockchain. Las cadenas de bloques son esencialmente bases de datos; su característica distintiva es que, en lugar de depender de una autoridad centralizada para actualizarlos, utilizan algún tipo de mecanismo de consenso para decidir quién puede agregar transacciones a la base de datos. El mecanismo de consenso varía, pero los dos más comunes son la prueba de trabajo (como la usa Bitcoin) y la prueba de participación (como la usa Ethereum). La prueba de trabajo se basa en personas conocidas como "mineros", que validan las transacciones. La prueba de participación selecciona validadores de un grupo de personas que poseen la criptomoneda relevante. En ambos casos, los validadores elegidos son compensados por su trabajo, y aunque teóricamente el validador podría ser cualquiera, en realidad.

https://www.foreignaffairs.com/united-states/crypto-currency-finance-blockchain-case-banning-rewards?utm_medium=newsletters&utm_source=fatoday&utm_campaign=Confronting%20the%20New%20Nuclear%20Peril&utm_content=20230405&utm_term=FA%20Today%20-%20112017

Cómo funciona el aprendizaje profundo

El aprendizaje profundo es un subconjunto del aprendizaje automático, que es esencialmente una red neuronal con tres o más capas. Estas redes neuronales intentan simular el comportamiento del cerebro humano, aunque lejos de igualar su capacidad, lo que le permite "aprender" de grandes cantidades de datos. Si bien una red neuronal con una sola capa aún puede hacer predicciones aproximadas, las capas ocultas adicionales pueden ayudar a optimizar y refinar la precisión.

https://www.ibm.com/topics/deep-learning

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 30 de enero 2023: https://us-cert.cisa.gov/ncas/bulletins/sb23-037
2. Vulnerabilidades semana del 6 de febrero 2023: https://us-cert.cisa.gov/ncas/bulletins/sb23-045
3. Vulnerabilidades semana del 13 de febrero 2023: https://us-cert.cisa.gov/ncas/bulletins/sb23-052
4. Vulnerabilidades semana del 20 de marzo 2023: https://www.cisa.gov/news-events/bulletins/sb23-058
5. Vulnerabilidades semana del 27 de febrero 2023: https://www.cisa.gov/news-events/bulletins/sb23-072
6. Vulnerabilidades semana del 6 de marzo 2023: https://www.cisa.gov/news-events/bulletins/sb23-065
7. Vulnerabilidades semana del 13 de marzo 2023: https://www.cisa.gov/news-events/bulletins/sb23-079
8. Vulnerabilidades semana del 20 de marzo 2023: https://www.cisa.gov/news-events/bulletins/sb23-086
9. Vulnerabilidades semana del 27 de marzo 2023: https://www.cisa.gov/news-events/bulletins/sb23-093

10. Vulnerabilidades semana del 3 de abril 2023: https://www.cisa.gov/news-events/bulletins/sb23-100

11. Vulnerabilidades semana del 10 de abril 2023: https://www.cisa.gov/news-events/bulletins/sb23-108

12. Vulnerabilidades semana del 17 de abril 2023: https://www.cisa.gov/news-events/bulletins/sb23-114

13. Vulnerabilidades semana del 24 de abril 2023: https://www.cisa.gov/news-events/bulletins/sb23-121

14. Vulnerabilidades semana del 1 de mayo 2023: https://www.cisa.gov/news-events/bulletins/sb23-128

15. Vulnerabilidades semana del 8 de mayo 2023: https://www.cisa.gov/news-events/bulletins/sb23-135

Microsoft febrero 2023, corrige 3 días cero, 77 fallas explotadas:

https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/

GoDaddy, una de las principales compañías de alojamiento web, ha informado de una brecha de seguridad en la que su entorno de alojamiento compartido *cPanel* fue vulnerado por atacantes desconocidos. Los atacantes obtuvieron acceso a la siguiente información: Direcciones de correo, electrónico. Contraseñas de administrador de WordPress.Acceso a sFTP, .credenciales de la base de datos.Claves privadas de clientes activos:

https://unaaldia.hispasec.com/2023/02/codigo-fuente-de-godaddy-filtrado.html

Inteligencia Artificial aplicada a la lucha contra malware

El pasado 24 de abril VirusTotal informaba a sus usuarios de la incorporación de Code Insight a su catálogo de funcionalidades. Basada en Sec-PaLM, Code Insight es capaz de generar resúmenes comprensibles para los usuarios desde el punto de vista de una IA especializada en ciberseguridad y malware.

https://unaaldia.hispasec.com/2023/04/virustotal-code-insight-analisis-de-amenazas-mediante-ia.html

Un libro de interés ChatGPT vs. GPT-4 ¿imperfecto por diseño? ¿Explorando los límites de la inteligencia artificial?:

Con prólogo de Vincenzo Aquaro, Director de Gobierno Digital de Naciones Unidas (United Nations) y junto a un gran equipo multidisciplinario e intergeneracional, se realizaron 600 pruebas para entender algo fundamental: la necesaria intervención humana frente a tareas o áreas críticas si consideramos el impacto en las personas y en las organizaciones. Vean estos resultados- ChatGPT resultados globales (excluyendo

sesgos) 55,9% respuestas correctas 9% respuestas plausibles 22% respuestas incorrectas o incoherentes ChatGPT resultados globales de sesgos 59,3% no sesgadas 4,30% parcialmente sesgadas 36,30% respuestas sesgadas Mejora de GPT-4 sobre ChatGPT Funcionalidades 30% Razonamiento 9,55% Lógica 9,9% Derecho argentino 15,11% Salud 10,81% Sesgos de género: 14,28% Otros sesgos: 7,29% Está claro que nos espera un enorme desafío en el corto plazo: cómo desarrollar capacidades para desaprender y aprender en ciclos cada vez más breves, mientras exploramos el coworking con la IA, y nos acostumbramos a convivir con tecnologías inteligentes que se vuelven omnipresentes y desafían nuestras habilidades cognitivas en cada área y tarea.

Libro: https://lnkd.in/d72ZZ9dR Anexos de pruebas realizadas: https://lnkd.in/dcdqgtvv

Resumen de noticias cibernéticas del Blavatnik Interdisciplinary Cyber Research Center (ICRC), la Tel Aviv University y el Taller de Ciencia, Tecnología y Seguridad de Yuval Ne'eman – Abril 2023

Propuestas gubernamentales para regular ChatGPT

Este mes, varios estados occidentales presentaron algunas iniciativas para investigar las consecuencias del uso del chatbot de OpenAI, ChatGPT.

El ***28 de abril***, ChatGPT reanudó sus servicios en Italia ya que el desarrollador de chat, OpenAI, acordó cumplir con las demandas específicas de la Autoridad de Protección de Datos de Italia (IDPA) para fines de abril, por ejemplo, informar a los consumidores italianos sobre los procesos de recopilación de datos. Tras las acciones de la Italian Data Protection Authority (IDPA), los organismos de control de la privacidad en Francia y España declararon que comenzaron a examinar las consecuencias del uso de ChatGPT. Al mismo tiempo, Alemania e Irlanda revelaron que están considerando prohibir el uso del chatbot. Suecia también declaró planes para auditar los efectos del uso de ChatGPT, pero no tenía planes para limitar el uso del chatbot.

Finalmente, la Junta Europea de Protección de Datos (EDPB) anunció el 13 de abril que había establecido un grupo de trabajo para revisar la prohibición de ChatGPT. Además, promoverá la cooperación y los intercambios de información sobre posibles actividades de aplicación para aumentar la transparencia de los procesos de procesamiento de datos realizados por el chatbot.

La guerra cibernética Rusia-Ucrania

El 13 de abril, el Servicio Federal de Seguridad de la Federación Rusa (FSB) dio a conocer un comunicado según el cual, durante 2022, EE. UU. y otros miembros de la OTAN lanzaron más de 5000 ataques cibernéticos contra entidades de infraestructura crítica en Rusia. Según el comunicado, aunque muchos ataques se presentaron como actividades del ejército de TI voluntario de Ucrania, la mayoría fueron lanzados por grupos de hackers globales, como Anonymous.

Al mismo tiempo, la empresa de telecomunicaciones rusa Rostelecom publicó un informe que incluye datos sobre ciberataques dirigidos a Rusia entre marzo de 2022 y marzo de 2023. Según el informe, el 38% de los ataques fueron realizados por grupos hacktivistas, mientras que el 20% fueron atribuidos a los grupos APT, que se cree que son los grupos chinos APT10, APT27 y APT41 y el grupo Lazarus de Corea del Norte.

20 de abril: cuatro legisladores estadounidenses introdujeron una legislación bipartidista para fortalecer la cooperación en seguridad cibernética entre EE. UU. y Taiwán para contrarrestar las amenazas cibernéticas chinas. En medio de la creciente agresión china en el ciberespacio, cuatro senadores y representantes de EE. UU.

Como parte de la futura cooperación, los dos países lanzarán ejercicios mutuos de entrenamiento en ciberseguridad, centrándose en la defensa de las redes, la infraestructura y los sistemas militares de Taiwán. La ley también incluye aprovechar las tecnologías de seguridad cibernética de EE. UU. para ayudar a Taiwán a detener más ataques de China.

21 de abril: un documento estadounidense clasificado revela planes chinos para desarrollar capacidades avanzadas para interrumpir satélites extranjeros: según un informe de inteligencia de la CIA, que se emitió este año, China está desarrollando capacidades avanzadas de guerra cibernética para negar, explotar o secuestrar satélites extranjeros durante tiempos de guerra, simulando las señales que reciben de sus operadores. Esta técnica puede permitir que China se apodere de los satélites enemigos y evitar que brinden servicios esenciales, como guiar los sistemas de armas y brindar servicios de comunicación a los combatientes. La CIA estima que estas capacidades son fundamentales para el objetivo de China de obtener la supremacía en el campo de la información en futuras guerras. El documento es parte de un grupo de documentos clasificados del Pentágono, que fueron filtrados en línea recientemente por un miembro de la Guardia Aérea de EE. UU. de 21 años, Jack Teixeira.