ISSN: 2718-6245

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 4 N° 39
Octubre 2021

OAC Boletín de Octubre 2021

"Un nuevo medio artificial, bots sociales, ha sido introducido al constantemente cambiante IE, para moldear e influenciar las percepciones y cognitivamente desencadenar cambios en el comportamiento, en una escala mundial exponencialmente masiva"

Del Libro Percepciones son realidad capítulo 10
(Galeano & otros, 2018)

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

La Inteligencia Artificial en la defensa de la Red

Kimberly Underwood
Senior Editor de Signal

A medida que avanza la automatización de procesos robóticos, la Agencia de Sistemas de Información de Defensa (DISA) está ampliando sus esfuerzos de inteligencia artificial a través de un acuerdo de investigación y un nuevo programa piloto. La agencia está volcando estos esfuerzos para examinar la aplicación de las capacidades de inteligencia artificial a la defensa de la red**,** ello mientras lleva a cabo su misión diaria de proteger la red de información del Departamento de Defensa de los EEUU las 24 horas del día.

La DISA está trabajando con Viena, compañía de software con sede en Virginia NT a través de un acuerdo de investigación y desarrollo cooperativo, para aplicar el aprendizaje de la máquina a las operaciones cibernéticas defensivas.

https://www.afcea.org/content/node/23820?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=Lq4v7

https://www.afcea.org/content/node/23806

https://www.afcea.org/content/node/23821?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=Mq4v7

Inteligencia Artificial y Recursos Humanos

La IA en RRHH ha avanzado mucho más allá de los algoritmos que rastrean los CV. Puede hacer **recomendaciones** sobre aumentos salariales y ascensos. En el caso de los empleados que buscan desarrollar su carrera, la IA puede evaluar sus habilidades, recomendar oportunidades de crecimiento y ofrecer contenido de aprendizaje en el camino. Para las empresas, puede ayudar a identificar y cerrar las brechas de habilidades. Y en todas estas aplicaciones, puede ayudar a eliminar los prejuicios e impulsar la inclusión.

https://revistabyte.es/actualidad-it/ia-etica-deib/

CIBERDEFENSA

Escuadrones de Comunicaciones convertidos a Escuadrones de Ciberdefensa

WASHINGTON - En septiembre, la Fuerza Aérea anunció que el 55 ° Escuadrón de Comunicaciones había cumplido con todos los objetivos para ser redesignado como el 55 ° Escuadrón Cibernético, lo que significa que el servicio agregaría un nuevo equipo de defensa de la misión a sus capacidades, un equipo cibernético especializado.

En tal sentido, la fuerza Aérea de los EEUU, ha implementado un plan por el cual habiendo cumplido ciertos objetivos un escuadrón de comunicaciones puede ser concebido como Escuadrón Cibernético, lo que significa que el servicio agregaría un nuevo equipo de defensa de la misión a sus capacidades. Estos equipos cibernéticos especializados están enfocados a permitir a la Fuerza Aérea el cumplimiento de misiones y defender instalaciones e infraestructuras críticas o computadoras asociadas con aeronaves y sistemas piloteados a distancia. El logro de estas capacidades se concretó mediante la subcontratación de sistemas de TI a la industria privada, lo que le permite preparar a sus RRHH para llevar a cabo la defensa en el ambiente del ciberespacio.

https://www.c4isrnet.com/cyber/2021/10/01/air-force-squeezes-new-cyber-defense-teams-out-of-its-communications-squadrons/

CIBERSEGURIDAD

Nuevos Empleos: “El socio tecnológico”

Un socio o *partner* tecnológico actúa como la persona u organización que ayuda en los procesos digitales y a los empleados para tener una constante actualización tecnológica, a no sufrir ningún problema técnico o al menos, solucionarlo lo más rápido posible.

En un entorno en el que la tecnología cobra cada vez más importancia, es primordial contar con un proveedor tecnológico que ayude a las empresas a no perder el ritmo y a conocer las oportunidades que ofrece la digitalización, pero, sobre todo, la tecnología.

https://revistabyte.es/actualidad-it/partners-tecnologicos/

TECNOLOGÍA

La contienda en el desarrollo de Inteligencia Artificial

La presente es una traducción libre de una nota del “Financial Times” del 10 de octubre de 2021 con acceso por suscripción.

El primer director de software del Pentágono dijo que renunció en protesta por la lentitud de la transformación tecnológica en el ejército de Estados Unidos y porque no podía soportar ver a China superar a Estados Unidos.

"En su primera entrevista desde que dejó el puesto en el Departamento de Defensa hace una semana, Nicolas Chaillan le dijo al Financial Times que el hecho de que Estados Unidos no respondiera a las amenazas cibernéticas chinas y otras amenazas estaba poniendo en riesgo el futuro de sus hijos.

“No tenemos ninguna posibilidad de competir contra China en 15 a 20 años. En este momento, ya es un trato hecho; en mi opinión ya se acabó, dijo, y agregó que había “buenas razones para estar enojado”.

Chaillan, de 37 años, quien pasó tres años en un esfuerzo en todo el Pentágono para impulsar la seguridad cibernética y como primer director de software de la Fuerza Aérea de los EE. UU., dijo que Beijing se dirige hacia el dominio global debido a sus avances en inteligencia artificial, aprendizaje automático y capacidades cibernéticas. Argumentó que estas tecnologías emergentes eran mucho más críticas para el futuro de Estados Unidos que el hardware como los aviones de combate de quinta generación de gran presupuesto, como el F-35.

Nicolás Chaillan: “Si se necesita una guerra o no, es algo anecdótico", dijo, argumentando que China estaba destinada a dominar el futuro del mundo, controlando todo, desde las narrativas de los medios hasta la geopolítica. Agregó que las ciberdefensas de Estados Unidos en algunos departamentos gubernamentales estaban a "nivel de jardín de infantes".

También culpó a la renuencia de Google a trabajar con el departamento de defensa de EE. UU. En IA y a los extensos debates sobre la ética de la IA para frenar a EE. UU. Por el contrario, dijo que las empresas chinas están obligadas a trabajar con Beijing y están haciendo una "inversión masiva" en IA sin tener en cuenta la ética.

Chaillan dijo que planea testificar ante el Congreso sobre la ciberamenaza china a la supremacía estadounidense, incluso en sesiones informativas clasificadas, durante las próximas semanas.

Reconoció que EE. UU. Aún gasta tres veces más que China en defensa, pero dijo que el dinero extra era irrelevante porque los costos de adquisiciones de EE.UU. eran muy altos y se gastaban en las áreas equivocadas, mientras que la burocracia y la regulación excesiva se interpusieron en el camino del cambio tan necesario en el Pentágono. .

Los comentarios de Chaillan se produjeron después de que una comisión de seguridad nacional de EE. UU. ordenada por el Congreso advirtiera a principios de este año que China podría superar a EE. UU. Como la superpotencia mundial de inteligencia artificial en la próxima década.

Los altos funcionarios de defensa han reconocido que "deben hacerlo mejor" para atraer, capacitar y retener a los jóvenes talentos cibernéticos, pero han defendido lo que, según ellos, es su enfoque responsable para la adopción de la IA.

Michael Groen, teniente general de la Infantería de Marina y director del Centro Conjunto de Inteligencia Artificial del departamento de defensa, dijo en una conferencia la semana pasada que quería desplegar IA en las fuerzas armadas de manera incremental, diciendo que su adopción requeriría un cambio de cultura dentro de las fuerzas armadas.

Sus comentarios se producen después de que el secretario de defensa de Estados Unidos, Lloyd Austin, dijera en julio que su departamento "necesita urgentemente" desarrollar inteligencia artificial responsable como una prioridad, y que agregar una nueva inversión de $ 1.5 mil millones aceleraría la adopción de la IA por parte del Pentágono en los próximos cinco años.

Pero se comprometió a que su departamento no "escatimaría en seguridad, protección o ética".

Un portavoz del Departamento de la Fuerza Aérea dijo que Frank Kendall, secretario de la Fuerza Aérea de los Estados Unidos, había discutido con Chaillan sus recomendaciones para el futuro desarrollo de software del Departamento luego de su renuncia y le agradeció sus contribuciones.

Chaillan anunció su renuncia en una carta crítica a principios de septiembre, diciendo que los oficiales militares fueron puestos repetidamente a cargo de iniciativas cibernéticas para las que carecían de experiencia, denunciando los "rezagados" del Pentágono y la falta de financiación.

“Estamos configurando infraestructura crítica para fallar”, dijo en su carta, que solo hacía una referencia superficial a los avances de China. “No pondríamos un piloto en la cabina sin un entrenamiento de vuelo extenso; ¿Por qué esperaríamos que alguien sin experiencia en TI esté cerca del éxito? [. . .] Mientras perdíamos el tiempo en la burocracia, nuestros adversarios avanzaron más”.

Robert Spalding, un general de brigada de la Fuerza Aérea retirado que se desempeñó como agregado de defensa en Beijing, dijo que Chaillan se había quejado "legítimamente" y agregó que él también había renunciado temprano para crear sus propias soluciones de tecnología de defensa encriptadas después de verse frustrado por sistemas "arcaicos".

Chaillan, quien se naturalizó como ciudadano estadounidense en 2016 y dirigió los esfuerzos para instalar medidas de seguridad cibernética de "confianza cero" en el Departamento de Seguridad Nacional antes de unirse al Pentágono, dijo que era una fuerza polarizadora en el Departamento de Defensa y que alarmó a algunos funcionarios de alto nivel que pensaban que debía mantener sus denuncias “en la familia”.

El emprendedor tecnológico en serie, que comenzó su primer negocio a los 15 años en Francia, dijo que también comenzó a sentirse obsoleto porque pasó sus tres años “arreglando cosas básicas en la nube y computadoras portátiles” en lugar de innovar.

https://www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0

CIBERCONFIANZA

Cómo enseñar a combatir la desinformación

2021 con acceso por suscripción.

El profesor Michael Caulfield ha diseñado un método en cuatro pasos para ayudar a los jóvenes a mejorar sus recursos contra la desinformación. En el primer año de estudio en muchas universidades de Estados Unidos, los bibliotecarios suelen dar unas clases de cómo buscar información y comprobar fuentes. Hace una década, con la explosión de internet, se dieron cuenta de que algo fallaba. La confusión crecía. Los estudiantes creían dar con fuentes fiables que en realidad eran basura.

https://elpais.com/tecnologia/2021-04-04/como-ensenar-a-combatir-la-desinformacion-menos-pensamiento-critico-y-mas-saber-que-miras.html

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 Septiembre: https://us-cert.cisa.gov/ncas/bulletins/sb21-270

Semana del 27 de Septiembre: https://us-cert.cisa.gov/ncas/bulletins/sb21-277

Semana del 4 de Octubre: https://us-cert.cisa.gov/ncas/bulletins/sb21-284

Semana del 11 de Octubre: https://us-cert.cisa.gov/ncas/bulletins/sb21-291

Semana del 18 de Octubre: https://us-cert.cisa.gov/ncas/bulletins/sb21-298

CIBERFORENSIA

Google lanza un parche de emergencia para un zero-day de Google Chrome

La semana pasada se lanzaba la versión de Chrome 94, sin embargo, varios días después Google actualizaba el popular navegador con una nueva versión más actualizada de Chrome 94, ya que fue detectada una vulnerabilidad de alto riesgo**.** Es de resaltar, además, que esta nueva versión resolvía problemas de esta índole, según las notas del parche 19.

https://thehackernews.com/2019/11/chrome-zero-day-update.html

Crean señales inalámbricas con un cable Ethernet para robar datos

Este método emplea cables Ethernet como una "antena de transmisión" para desviar sigilosamente datos altamente sensibles de sistemas *air-gap*, según las últimas investigaciones. *Air-gap* es el nombre de una medida de seguridad de red empleada en una o más computadoras o dispositivos para garantizar que una red segura esté físicamente aislada de las redes potencialmente no seguras, como el internet público o una red de área local no segura.

https://arxiv.org/abs/2012.06884

https://unaaldia.hispasec.com/2021/10/crean-senales-inalambricas-con-un-cable-ethernet-para-robar-datos.html

CIBERDELITO

Solo un 20% de desarrolladores comprende las políticas de seguridad que debe seguir

VMware ha publicado una investigación sobre el nivel de interacción entre los equipos de TI, su seguridad y desarrollo en la medida en que las organizaciones se mudan a un modelo de seguridad `confianza cero´.

La compañía afirma que solo uno de cada cinco desarrolladores comprende claramente las políticas de seguridad que debe seguir. Y es que, el 52% cree que mantendrá su estrategia de seguridad.

https://revistabyte.es/ciberseguridad/desarrolladores-seguridad/

NOVEDADES

PARA TENER EN CUENTA

Cyber Defense Webinars (Oct 27, 2021 2:00 PM - 3:00 PM EDT)

Ya sea motivada por evitar riesgos o impulsada por el cumplimiento, la seguridad de la identidad se ha convertido en una de las principales preocupaciones de los CISO, independientemente de su industria o tamaño. Gartner ahora presenta la seguridad en primer lugar como una de las 3 principales prioridades de CISO para 2021. Los CISO inteligentes están tomando medidas para proteger la continuidad de su negocio

y el bienestar de la empresa aumentando sus inversiones en soluciones de Detección y Respuesta de Identidad (IDR)

https://cyberdefensemagazine.tradepub.com/free/w_defa1653/prgm.cgi?a=1

Compromiso de Defensa y Seguridad de los Estados Unidos en la Región del Mar Negro

Únase al CSIS (Center for Strategic International Studies) para una conversación sobre las visitas del Secretario de Defensa Austin a Georgia, Ucrania y Rumania la semana pasada y la dinámica de seguridad regional en la región del Mar Negro.

¿Cómo puede Estados Unidos trabajar con sus aliados y socios en la región para garantizar mejor su seguridad y contrarrestar la influencia rusa?

https://www.csis.org/events/us-defense-and-security-engagement-black-sea-region

Mesa-debate: La tecnología, ¿ayuda o esclaviza?

Continuación del ciclo 2021 "Transitando un cambio de época", organizado por el Comité de Cultura del CARI

¿Estamos "Transitando hacia una nueva época?" Para contestar esa pregunta hemos convocado las mesas del Trabajo, de la Educación, del Ambiente y ahora la de tecnología. La Tecnología y sus múltiples aplicaciones, que aumentan día a día y parece imposible no usarlas. Sin embargo, el filósofo Alejandro Piscitelli dice: "Apostamos todo al software... y así nos fue". Mientras el Físico Vicente Campenni (INVAP) sostiene que: "Ser autónomo es poder elegir qué tecnología desarrollar". Tanto Piscitelli como Campenni estarán tratando de explicarnos lo que le debemos a la tecnología y hasta dónde debemos depender de ella.

https://docs.google.com/forms/d/1u41nV_fdCpx0vZnkV4E1IQ_-APb6vMtgzrJZPcuVDS8/viewform?edit_requested=true

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 | *