OAC Boletín de Agosto/Septiembre 2022

"La seguridad no es posible sin el poder, porque una nación despreciable por su debilidad, sacrificará hasta el privilegio de ser neutral"

Alexander Hamilton
Pg, 7 del Libro "Estrategia: el Camino" GD Evergisto de Vergara

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 estrategia de Inteligencia Artificial (IA) del Reino Unido

Esta estrategia establece cómo el RUGB explotará la IA a ritmo y escala, transformando la Defensa en una organización preparada para IA, brindando capacidad de vanguardia; construyendo alianzas más sólidas con la industria de IA del Reino Unido; colaborar internacionalmente para dar forma a los desarrollos globales de IA promoviendo la seguridad, la estabilidad. Lo considera un elemento clave de la Estrategia para obtener una ventaja estratégica a través de la ciencia y la tecnología. Sus objetivos son:

1. Transformar Defensa en una organización 'preparada para IA
2. Adoptar y explotar la IA a ritmo y escala para la ventaja de Defensa
3. Fortalecer el ecosistema de IA de defensa y seguridad del Reino Unido
4. Dar forma a los desarrollos globales de IA para promover la seguridad, la estabilidad y los valores democráticos.

https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy#:~:text=The%20Integrated%20Review%20(2021)%20highlights,transform%20all%20areas%20of%20life.

La guerra invisible

El 24 de febrero, el día de la invasión rusa de Ucrania, se pudo observar cuán cerca están la guerra visible y la invisible. De repente, una gran cantidad de clientes del proveedor de telecomunicaciones estadounidense Viasat perdieron sus conexiones a Internet satelital. Al mismo tiempo, 5.800 aerogeneradores en Alemania de repente ya no pudieron comunicarse con su centro de red.

"Con la guerra Ruso/ Ucraniana, la amenaza del espionaje ruso, las campañas de desinformación y los ataques cibernéticos han adquirido otra dimensión", dice la ministra del Interior alemana, Nancy Faeser.

https://www.spiegel.de/international/germany/hackers-spies-and-contract-killers-how-putin-s-agents-are-infiltrating-germany-a-2cc6c24c-16ac-43d4-97fa-103081414acc

CIBERSEGURIDAD

Informe de amenazas 2022 de BlackBerry

Su organización requiere de una ciberseguridad sólida, como lo demuestran los ataques contra la infraestructura crítica, el software de la cadena de suministro, los gobiernos, grandes compañías y pequeñas a medianas empresas. El Informe de amenazas 2022 de BlackBerry® lo pone al día sobre las últimas técnicas, tácticas y procedimientos (TTP) empleados por los delincuentes cibernéticos, incluso los grupos de amenazas avanzadas persistentes (APT). Use esta información para ayudar a su organización a asignar los recursos de seguridad con inteligencia y protéjase de los ataques cibernéticos.

Nota: la bajada del documento requiere la entrega de datos personales

https://www.blackberry.com/la/es/forms/enterprise/report-bb-2022-threat-report?utm_source=google&utm_medium=cpc&utm_campaign=smb_enterprise_es-ar&_bt=605278076526&_bk=ataques%20ransomware&_bm=b&_bn=g&_bg=138767644955&gclid=Cj0KCQjwuaiXBhCCARIsAKZLt3mRbhVoOBactAW_k8JWrYgarHWPhXQXtkSq0h7CAjcUsDB3-4kyhO0aAu2AEALw_wcB

Ataques empleando los Led de las computadoras y la clave Morse

La implementación de sistemas aislados tiene como objetivo evitar la filtración de información confidencial y de carácter sensible en ámbitos como, por ejemplo, el militar. ETHERLED, ataca sistemas aislados y permite el envío de información sensible mediante señales en código morse a través de los LED de las tarjetas de red (NIC), al igual que otro tipo de ataques dirigidos contra sistemas aislados, cuenta con el requisito de que antes de poder filtrar la información hacia el exterior, se debe instalar malware en el sistema. Además, por la naturaleza de esta técnica basada en el uso de los LED para la transmisión de información, los usuarios que estén lo suficientemente alerta podrían detectar el ataque.

https://thehackernews.com/2022/08/air-gapped-devices-can-send-covert.html

https://arxiv.org/abs/2208.09975

https://hispasec.us16.list-manage.com/track/click?u=dd62599a9195e52f2dca2ab9a&id=04746928b5&e=c0522112d9

CIBERDEFENSA

Argentina Comando Conjunto de Ciberdefensa

Zoma Militar público en el mes de Julio, una interesante entrevista al Comandante Conjunto de Ciberdefensa que nos acerca una idea de las actividades que este organismo realiza en el marco de la Defensa Nacional

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

El mayor ataque de denegación de servicios registrado

Un cliente de Google Cloud Armor sufrió un ataque de denegación de servicio distribuido (DDoS) a través del protocolo HTTPS que alcanzó los 46 millones de solicitudes por segundo (RPS), lo que lo convierte en el más grande jamás registrado de este tipo. En solo dos minutos, el ataque escaló de 100 000 RPS a un récord de 46 millones de RPS, casi un 80 % más que el récord anterior, un HTTPS DDoS de 26 millones de RPS que Cloudflare mitigó en junio

https://www.bleepingcomputer.com/news/security/google-blocks-largest-https-ddos-attack-reported-to-date/

https://www.bleepingcomputer.com/news/security/akamai-blocked-largest-ddos-in-europe-against-one-of-its-customers/

TECNOLOGÍA

Interfaces cerebro-computadora

La accesibilidad, la adaptabilidad y la transparencia de las herramientas de interfaz cerebro-computadora (BCI) y los datos que recopilan probablemente afectarán la forma en que navegamos colectivamente en una nueva era digital. Esta discusión revisa algunas de las aplicaciones diversas y transdisciplinarias de la tecnología BCI y extrae inferencias especulativas sobre las formas en que las herramientas BCI, combinadas con los algoritmos de aprendizaje automático (ML), pueden dar forma al futuro. Las BCI vienen con consideraciones éticas y de riesgo sustanciales, y se argumenta que los principios de código abierto pueden ayudarnos a navegar dilemas complejos al alentar la experimentación y hacer públicos los desarrollos a medida que construimos salvaguardas en este nuevo paradigma. Llevar los principios de adaptabilidad y transparencia de código abierto a las herramientas de BCI puede ayudar a democratizar la tecnología, permitiendo que más voces contribuyan a la conversación sobre cómo debería ser un futuro impulsado por BCI. Las herramientas BCI de código abierto y el acceso a los datos sin procesar, en contraste con los algoritmos de caja negra y el acceso limitado a los datos resumidos, son facetas fundamentales que permiten a los artistas, aficionados al bricolaje, investigadores y otros expertos en el dominio participar en la conversación sobre cómo estudiar y mejorar la capacidad humana. conciencia. Mirando hacia un futuro en el que la realidad virtual y aumentada se conviertan en partes integrales de la vida diaria, es probable que las BCI desempeñen un papel cada vez más importante en la creación de comentarios de circuito cerrado para el contenido generativo. Las interfaces cerebro-computadora están situadas de manera única para proporcionar a los algoritmos de inteligencia artificial (IA) los datos necesarios para determinar la decodificación y el tiempo de entrega de contenido.

https://www.media.mit.edu/publications/brain-computer-interfaces-open-source-and-democratizing-the-future-of-augmented-consciousness/

https://www.brainaccess.ai/?gclid=Cj0KCQjwuaiXBhCCARIsAKZLt3n2gwURfyDnKA5hGn051A-apkEbw43JpE4e8LseVHJf0huvZGfNRocaAnn4EALw_wcB

https://wearablesensing.com/applications/bci-and-neurogaming/?gclid=Cj0KCQjwuaiXBhCCARIsAKZLt3lFzrvnUzp8OiJ9tqfu9TgkVumht0yQZYvmGsBFmLmKzOYMq0uIiZwaAlbNEALw_wcB

Los ciber-delincuentes ya pueden atacar tu cerebro

Antiguamente lo habrían llamado brujería o posesión demoníaca. Sin embargo, a día de hoy podemos hablar de Brain Hacking cuando nos referimos a la aplicación simultánea de técnicas y tecnologías para alterar el estado mental de las personas, así como sus procesos cognitivos o el nivel del funcionamiento de la mente, a nivel psicológico, de un individuo.

Espionaje mental es la aplicación de técnicas y/o tecnologías para conocer e intervenir en el estado mental, los procesos cognitivos o funcionamiento a nivel psicológico de un individuo Conociendo y manipulando los procesos psicológicos de los individuos se pueden realizar adoctrinamientos e incluso las radicalizaciones violentas.

https://www.lisanews.org/ciberseguridad/brain-hacking-o-espionaje-mental/

https://www.pandasecurity.com/es/mediacenter/seguridad/brain-hacking/#:~:text=Sin%20embargo%2C%20a%20d%C3%ADa%20de,nivel%20psicol%C3%B3gico%2C%20de%20un%20individuo.

¿Qué es Internet 3.0 o la WEB Semántica?

La idea de web 3.0, está relacionada a lo que se conoce como web semántica. Los usuarios y los equipos, en este marco, pueden interactuar con la red mediante un lenguaje natural, interpretado por el software. De esta manera, acceder a la información resulta más sencillo. Dicho de otro modo, todos los datos alojados en la web 3.0 deberían ser “entendidos” por las máquinas, que podrían procesarlos con rapidez. La web 3.0, en definitiva, está relacionada con la inteligencia artificial. Los sitios web incluso tendrían la capacidad de conectarse entre sí de acuerdo a los intereses del usuario.

https://definicion.de/web-3-0/

https://www.plainconcepts.com/es/que-es-web-3/

https://academy.binance.com/es/articles/the-evolution-of-the-internet-web-3-0-explained

CIBERCONFIANZA

Confrontando la Realidad en el Ciberespacio: Política Exterior para una Internet Fragmentada

La visión utópica de una red global abierta, confiable y segura no se ha logrado y es poco probable que alguna vez se realice. Hoy, Internet es menos libre, más fragmentado y menos seguro. Internet global, una vasta matriz de telecomunicaciones, fibra óptica y redes satelitales, es en gran parte una creación de los

Estados Unidos. Las tecnologías que sustentan Internet surgieron de proyectos de investigación federales y las empresas estadounidenses innovaron, comercializaron y globalizaron la tecnología. La estructura básica de Internet —una dependencia del sector privado y la comunidad técnica, una supervisión regulatoria relativamente ligera y la protección de la expresión y la promoción del libre flujo de información— reflejaba los valores estadounidenses.

Además, los intereses estratégicos, económicos, políticos y de política exterior de EE. UU. fueron atendidos por la Internet global y abierta. Washington creyó durante mucho tiempo que su visión de Internet finalmente prevalecería y que otros países se verían obligados a adaptarse o perderían los beneficios de una Internet global y abierta.

Durante la última década, la mayoría de las operaciones cibernéticas han sido ataques que violan la soberanía, pero se mantienen por debajo del umbral para el uso de la fuerza o ataque armado. Estas infracciones se utilizan para obtener ventajas políticas, espionaje y el arte de gobernar a nivel internacional, y los ataques más dañinos socavan la confianza en las instituciones sociales, políticas y económicas

https://www.cfr.org/report/confronting-reality-in-cyberspace

La Inteligencia Artificial y una mirada diferente sobre el impacto en el consumo

La socióloga Shoshana Zuboff explica que los usuarios de la tecnología ya no son meros clientes, sino la materia prima de un nuevo sistema industrial; de los que se extrae datos para hacer predicciones sobre su conducta y vender productos. Este es el hilo conductor que recorre"*La era del capitalismo de vigilancia*"(Paidós), considerado como uno de los libros más influyentes de este siglo. Zuboff es comparada con el economista Thomas Piketty, que alertó de que la creciente concentración de la riqueza es inevitable si no se modifica el sistema, pero, a diferencia de Piketty, Zuboff concita el aplauso del *Financial Times* y *The Wall Street Journal*.

https://www.abc.es/xlsemanal/personajes/capitalismo-de-vigilancia-shoshana-zuboff-seguridad-datos-internet-redes-sociales.html#vca=modulos&vso=abc-es&vmc=noticias-rel-1-cmp&vli=personajes

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).

1. Vulnerabilidades semana 11 de Julio: https://www.cisa.gov/uscert/ncas/bulletins/sb22-199
2. Vulnerabilidades semana 18 de Julio: https://www.cisa.gov/uscert/ncas/bulletins/sb22-206
3. Vulnerabilidades semana 25 de Julio: https://www.cisa.gov/uscert/ncas/bulletins/sb22-213
4. Vulnerabilidades semana 1 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-220
5. Vulnerabilidades semana 8 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-227

6. Vulnerabilidades semana 15 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-234
7. Vulnerabilidades semana 22 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-241
8. Vulnerabilidades semana 29 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-249
9. Vulnerabilidades semana 05 de septiembre https://www.cisa.gov/uscert/ncas/bulletins/sb22-255
10. Vulnerabilidades semana 12 de septiembre https://www.cisa.gov/uscert/ncas/bulletins/sb22-262
11. Vulnerabilidades semana 19 de septiembre https://www.cisa.gov/uscert/ncas/bulletins/sb22-269

Informes de interés:

1. Apple actualiza su seguridad en varios productos: https://support.apple.com/en-us/HT201222
2. Chrome actualiza su seguridad: https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html
3. **Parando taques de Ransomware**: el *aviso de seguridad cibernética (CSA) es parte de un esfuerzo continuo #StopRansomware para publicar avisos para los defensores de la red que detallan varias variantes de ransomware y actores los avisos incluyen tácticas, técnicas y procedimientos (TTP) observados recientemente e históricamente e indicadores de compromiso (IOC) para ayudar a las organizaciones a protegerse contra el ransomware.* https://www.cisa.gov/uscert/ncas/alerts/aa22-223a
4. **Actualización del catalogo de vulnerabilidades de CISA:** https://www.cisa.gov/known-exploited-vulnerabilities-catalog
5. **Mozilla lanza actualización de seguridad para Thunderbird:** https://www.mozilla.org/en-US/security/advisories/mfsa2022-38/

Alibaba comprometido por distribución de malware mediante esteganografía

El servicio de almacenamiento de objetos (OSS) de Alibaba Cloud (también conocido como Aliyun), podría servir para la distribución de malware y actividades ilícitas de minería de criptomonedas mediante el uso de esteganografía (es la práctica de ocultar un mensaje secreto dentro (o incluso encima) de algo que no es secreto)

https://unaaldia.hispasec.com/2022/07/oss-buckets-de-alibaba-comprometidos-para-distribuir-shell-scripts-maliciosos-mediante-esteganografia.html

https://www.trendmicro.com/en_us/research/22/g/alibaba-oss-buckets-compromised-to-distribute-malicious-shell-sc.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0722_Alibaba

La cortina de Hierro Digital

Las autoridades rusas bloquearon el acceso a todos los principales sitios de noticias de la oposición, así como a Facebook, Instagram y Twitter. Según las nuevas leyes, que pretenden combatir las noticias falsas sobre la guerra ruso-ucraniana, los usuarios de Internet se han enfrentado a cargos administrativos y penales por supuestamente difundir información falsa sobre las acciones de Rusia en Ucrania. La

mayoría de las empresas de tecnología occidentales, desde Airbnb hasta Apple, han detenido o limitado sus operaciones en Rusia como parte del éxodo corporativo más amplio del país.

https://theconversation.com/kremlin-tightens-control-over-russians-online-lives-threatening-domestic-freedoms-and-the-global-internet-182020?utm_medium=email&utm_campaign=Latest%20from%20The%20Conversation%20for%20June%2030%202022%20-%202335823273&utm_content=Latest%20from%20The%20Conversation%20for%20June%2030%202022%20-%202335823273+CID_ecdf8b5274c97f1992d3e2b40d6ad778&utm_source=campaign_monitor_us&utm_term=Kremlin%20tightens%20control%20over%20Russians%20online%20lives%20%20threatening%20domestic%20freedoms%20and%20the%20global%20internet

NOVEDADES

Inicio la Diplomatura en la Gestión de la Ciberdefensa

Con fecha 01 de septiembre ha dado comienzo la quinta edición de la Diplomatura Universitaria en Gestión de la Ciberdefensa (Resolución Rectoral UNDEF Nro 277/2021), este año por primera vez en el recientemente creado Instituto de Ciberdefensa de las Fuerzas Armadas.

Las ediciones anteriores se desarrollaron en el ámbito de la Escuela Superior de Guerra Conjunta.

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 | *