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 5 N° 43
Abril 2022

OAC Boletín de abril 2022

""En la lucha contra las amenazas, no podemos mirar para otro lado, ser un superhéroe o actuar a lo bruto: La realidad es que es necesaria la colaboración".

Javier Berciano Alonso (6to encuentro de seguridad de la información)

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

Las operaciones de la Información y la creciente demanda

Las operaciones de información (IO) son el centro de atención del escenario mundial, la Fuerza Aérea de EE. UU. ve una creciente necesidad de expertos en ese campo y está tomando medidas para ampliar las oportunidades de capacitación en Operaciones de Información (IOS). La capacitación incluye el Curso de Integración de IO, que proporciona una calificación inicial para los aviadores que servirán principalmente en los Centros de Operaciones Aéreas; el Curso de gestión de firmas, que brinda capacitación en engaño militar y seguridad operativa a oficiales y suboficiales que se desempeñan como administradores de firmas en el nivel de Brigada Aérea; y el curso de Engaño Militar Operativo, que brinda capacitación para el comando principal de la Fuerza Aérea y los planificadores de la Fuerza Aérea.

https://www.afcea.org/content/air-force-expanding-information-operations-classes

China es un arma poderosa en la guerra de la información Rusa

La propaganda rusa sobre la guerra en Ucrania fracasó el mes pasado después de que los canales de noticias estatales rusos fueran bloqueados en Europa y restringidos a nivel mundial. Pero en las últimas semanas, China se ha convertido en una potente salida para la desinformación del Kremlin, presentando a Ucrania y la OTAN como los agresores y compartiendo afirmaciones falsas sobre el control neonazi del gobierno ucraniano.

"Con los gobiernos y las plataformas tecnológicas moviéndose para censurar o limitar la difusión de la propaganda rusa, los puntos de comunicación a favor del Kremlin ahora están siendo lavados a través de personas influyentes representantes, incluidos funcionarios chinos y medios de comunicación estatales que no enfrentan las mismas restricciones que se han impuesto a los medios de comunicación estatales rusos", dijo Bret Schafer, investigador principal y jefe del equipo de manipulación de información de la Alianza para Asegurar la Democracia, una iniciativa del Fondo Marshall Alemán de EE. UU. que rastrea los medios estatales chinos y rusos. "Esto ha

permitido al Kremlin eludir efectivamente las prohibiciones destinadas a limitar la difusión de la propaganda rusa".

https://www.msn.com/en-us/news/world/china-is-russias-most-powerful-weapon-for-information-warfare/ar-AAW03nc?ocid=sw

Interesante aporte del Profesor Invitado de la Escuela Superior de Guerra Conjunta de las FFAA de la República Argentina, Coronel del Ejército del Brasil Márcio Saldanha Walker a una nota publicada en nuestro Boletín

Sobre el artículo publicado en el Boletín de marzo de 2022 del Observatorio Argentino de Ciberespacio, **"La inteligencia en las Operaciones de Información", donde el Analista Manu Robledo define: "las actividades de información afectan al carácter o al comportamiento de las personas, mediante el uso de la información, para influir en sus percepciones y su comprensión, y abarcan un amplio espectro de actividades diseñadas para afectar a una audiencia objetivo en tres aspectos: sus capacidades, su comprensión y su voluntad… Para ello, estas actividades intervienen en el plano psicológico."** Vale la pena aclarar que el concepto militar doctrinario de Operaciones de Información no se restringe a las actividades de Operaciones Psicológicas, como lo está orientando la comprensión del artículo. Las Operaciones Psicológicas son metodologías y procedimientos técnico-especializados que añaden la capacidad de actuar sobre la voluntad de los blancos militares durante situaciones de combate. Por otro lado, las Operaciones de Información, según la doctrina de la OTAN, se definen como: **"una función militar para proporcionar asesoramiento y coordinación de actividades de información militar con el fin de crear los efectos deseados en la voluntad, la comprensión y la capacidad de los adversarios, adversarios potenciales y otras partes."** El término capacidad engloba otras capacidades militares de las Fuerzas Armadas, no solo las capacidades cognitivas individuales. Las acciones militares son cinéticas y no cinéticas. Las Operaciones de Información tratan de coordinar los efectos generados por las acciones para contribuir al estado final deseado del nivel Estratégico Militar. En otras palabras, las "Operaciones de Información" incluyen la coordinación de las capacidades relacionadas con la información, tal como la Comunicación Estratégica, la Guerra Cibernética, la Guerra Electrónica, entre otras, ello según la doctrina de cada país.

CIBERSEGURIDAD

Australia apuesta por la Ciberseguridad

En Australia, ha sido aprobado por votación un fondo de 9.9 millones de dólares dirigido completamente al campo de la ciberseguridad en un proyecto que abarca 10 años de duración. El programa REDSPICE **contará con 1900 técnicos** y que, además, pretende **ampliar hasta en 3 veces la capacidad ofensiva del país.** Estas medidas, según el ministro de defensa Peter Dutton, se debe a los recientes incidentes que afectan a dicha región y a la rápida expansión militar en el campo de la ciberseguridad por parte de los países rivales.

https://unaaldia.hispasec.com/2022/04/australia-apuesta-fuerte-por-la-ciberseguridad.html

https://theconversation.com/budget-2022-9-9-billion-towards-cyber-security-aims-to-make-australia-a-key-offensive-cyber-player-180321

CIBERDEFENSA

La problemática de la velocidad de respuesta en la Ciberdefensa

En el entorno cibernético actual, el ámbito de los ataques crece exponencialmente día tras día sin signos de desaceleración. La búsqueda de un contexto adecuado y significativo en la telemetría de sistemas y redes es como tratar de encontrar una aguja en un pajar. El "tiempo de permanencia" de los ataques entre la penetración inicial y el punto de detección/erradicación en 2020 era de 56 días, eso significa que un atacante estuvo en promedio casi dos meses dentro de una red antes de ser descubierto.

Dos enfoques excelentes para estos desafíos son la detección y respuesta extendidas (XDR) impulsadas por inteligencia artificial (IA) y la detección y respuesta administradas (MDR). Ambos acortan el tiempo de permanencia al detectar y responder rápidamente a las penetraciones.

Este artículo describe a grandes rasgos el funcionamiento del motor XDR AI.

https://www.afcea.org/content/automated-cyber-defense-speed-manageable?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=8VHH8

CIBERGUERRA

Guerra en Ucrania Ciberataques, no son detectados ni neutralizados

El articulo presenta una tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas. Del mismo modo, otra de las acciones que son muy efectivas y que, sin embargo, más de la mitad de las empresas encuestadas no disponen es la lista blanca. Gracias a este sistema se eligen los programas que pueden funcionar en el ordenador para evitar que el software malicioso se active

https://revistabyte.es/actualidad-it/ucrania-ciberataques-guerra/

CIBERCONFIANZA

CIBER-EMPAREJAMIENTO

El Dr. en Ingeniería Alejandro Corletti, Mayor retirado de nuestro Ejército Argentino, comenta esta nueva forma de ciberdelicuencia, por el momento inocua pero de potencial destructivo

https://www.youtube.com/watch?v=JJdk8UWexI4

Metaverso: claves para entender su impacto a nivel económico, consumo y social

¿Ha evolucionado El concepto de Metaverso hasta convertirse en el siguiente paso en la transformación de Internet?

El concepto de Metaverso ha evolucionado hasta convertirse en el siguiente paso en la transformación de Internet, donde emerge una proyección de un universo paralelo a la vida real a través de una combinación de realidad virtual, aumentada y mixta. Desde Softtek, empresa que proporciona servicios y

soluciones de transformación digital de próxima generación a nivel global, analizan las claves para entender el impacto que su llegada puede generar en términos de economía, consumo y sociedad.

https://revistabyte.es/tendencias-tic/metaverso-claves-para-entender/

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 28 de Marzo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-094

Semana del 04 de Abril: https://www.cisa.gov/uscert/ncas/bulletins/sb22-101

Informes de interés:

1. Google ha lanzado la versión 100.0.4896.75 de Chrome para Windows, Mac y Linux. Esta versión aborda las vulnerabilidades que un atacante podría aprovechar para tomar el control de un sistema afectado. CISA alienta a los usuarios y administradores a revisar: https://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop.html
2. Mozilla ha publicado actualizaciones de seguridad para solucionar vulnerabilidades en Firefox, Firefox ESR y Thunderbird. Un atacante podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado. CISA alienta a los usuarios y administradores a revisar los avisos de seguridad de Mozilla para https://www.mozilla.org/en-US/security/advisories/mfsa2022-13/ ; https://www.mozilla.org/en-US/security/advisories/mfsa2022-14/ y https://www.mozilla.org/en-US/security/advisories/mfsa2022-15/
3. Nuevas Vulnerabilidades agregadas al catálogo de CIS (https://www.cisa.gov/known-exploited-vulnerabilities-catalog), https://www.cisa.gov/uscert/ncas/current-activity/2022/04/06/cisa-adds-three-known-exploited-vulnerabilities-catalog

TECNOLOGÍA

La guerra en Ucrania impulsa mejoras en Internet usando el espacio

Es probable que las capacidades perfeccionadas por las empresas espaciales comerciales para documentar la destrucción infligida por Rusia en Ucrania tengan efectos duraderos en la industria.

Los satélites han brindado al mundo visiones sin precedentes de la brutal guerra, ya sea a través de imágenes comerciales que muestran la destrucción rusa de un refugio claramente etiquetado como con niños adentro, videos de redes sociales compartidos a través de los satélites Starlink de SpaceX o imágenes de un fotoperiodista de Mariupol archivadas a través de teléfonos satelitales . Es probable que estos despachos gráficos desde la zona de guerra hayan jugado al menos algún papel en la efusión

mundial de apoyo y ayuda, incluidos los 4 de cada 10 estadounidenses que dijeron en una encuesta de marzo que EE. UU. debería hacer más para ayudar a Ucrania.

"Creemos que actualmente, la inteligencia geoespacial está teniendo su momento en Internet", dijo Bill Rozier, vicepresidente de marketing de BlackSky, que está utilizando inteligencia artificial para analizar las imágenes satelitales que recopila sobre Ucrania.

https://www.defenseone.com/technology/2022/04/ukraine-war-giving-commercial-space-internet-moment/364101/

NOVEDADES

TALLER VIRTUAL EN VIGILANCIA TECNOLÓGICA E INTELIGENCIA ESTRATÉGICA

DESTINADO A OFICIALES CURSANTES DE AÑOS SUPERIORES DE LA

ESGA, ESGN, ESG, ESGCFFAA, IIFFAA y FIE. (link será publicado en la página del Instituto de Ciberdefensa de las Fuerzas Armadas)

02 y 09 de mayo de 2022 a las 18:00

Modalidad virtual: Campus Virtual FIE

Actividad con inscripción previa:

Contacto: ceptm@fie.undef.edu.ar

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 | *