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° 33
Abril 2021

OAC Boletín de Abril 2021

"Hay un conflicto directo entre el concepto occidental de internet, insistiendo en el flujo libre, irrestricto y sin gobierno y el consenso adoptado por Rusia y estados de ideas afines, que coloca importantes salvedades sobre el flujo de información e insiste en el principios de soberanía nacional en el ciberespacio"

Keir Giles
Manual de Guerra de la Información Rusa (Pag 47)

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), micro-sitio de la **Facultad Militar Conjunta de las Fuerzas Armadas**
URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php.
Es un esfuerzo posible por el financiamiento que el observatorio recibe de la **Universidad de la Defensa Nacional**, a través de los programas UNDEFI y se encuentra inserto en la **Antena 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

5G ¿el final de la Privacidad?

Un documento audiovisual de interés para el público en general, que le permitirá de manera sencilla entender la tecnología 5G y comprender algunas de las razones de su discusión en el marco global, donde de alguna manera se plantea si esta es una nueva tecnología o realmente una estrategia de control poblacional.

https://youtu.be/iRfxRLdPdN8

CIBERSEGURIDAD

Los problemas de la seguridad cibernética afectan a los EE.UU

El jefe del Comando Cibernético, el general Paul Nakasone, dijo al Congreso hoy que los adversarios de Estados Unidos están descaradamente "explotando una brecha" en la estructura de las autoridades civiles y militares estadounidenses para atacar a la nación. Operar dentro de los EE. UU. pone a los actores de amenazas más allá del alcance de CYBERCOM y la Agencia de Seguridad Nacional.

https://breakingdefense.com/2021/03/nakasone-warns-adversaries-hack-unseen-in-us/?utm_campaign=Breaking%20News&utm_medium=email&_hsmi=117965923&_hsenc=p2ANqtz-9ZrcyW4DV1VO-H9w2tGf1FF3cKH87TmttTyxXljBFE8cMvcXnHUpWqAz6DBnn9FaCa546soUGqSDWytf-y6UvswmktrQ&utm_content=117965923&utm_source=hs_email

CIBERDEFENSA

Documento de Interés

China, el Ciberespacio y el poder estatal híbrido

El ascenso de China como un competidor por el estatus de superpotencia se ha convertido en un desafío importante para Estados Unidos. El Comité Cibernético de la AFCEA abre la discusión sobre el enfoque híbrido de China para el uso del poder, particularmente en el ciberespacio, como competidor de Estados Unidos. La gobernanza interna y externa y su aplicación en el campo de batalla son dos facetas del enfoque de China.

Para acceder al documento haga click

https://www.afcea.org/signal/resources/linkreq.cfm?id=302&utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=vu4U7

Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman

En los sistemas industriales SCADA (Supervisory Control And Data Acquisition), conocer el estado de cada dispositivo permite obtener información de su comportamiento. De esta forma se pueden deducir acciones y conformar estrategias diferentes que ayuden a reducir el riesgo cibernético. En este artículo de investigación aplicada, se presenta un modelo de predicción de posibles ciberataques en un sistema SCADA.

Quiroz Tascón, Stephen; Zapata Jiménez, Julián; Vargas Montoya, Héctor Fernando Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman TecnoLógicas, vol. 23, núm. 48, 2020 Instituto Tecnológico Metropolitano, Colombia Disponible en:

http://www.redalyc.org/articulo.oa?id=344263272013

CIBERGUERRA

Desinformación antes y ahora

Una modalidad de comunicación multimedia (Voz, letra) nos trae este artículo de Camile François acerca de como los investigadores de la desinformación han estado librando dos batallas durante la última década: una para combatir y contener información dañina, y otra para convencer al mundo de que estas manipulaciones tienen un impacto fuera de línea que requiere soluciones complejas y matizadas

https://www.humanetech.com/podcast/31-disinformation-then-and-now?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-

a5e4c470e59de911a97d000d3a233b72-724e9e6379f94998b816e27a10e4d891&esid=93c111f0-a38c-eb11-b1ac-000d3abdd313

Comando y Control Conjunto de todos los Dominios (JADC2)

Northern Command está creando un prototipo y probando un conjunto de herramientas de inteligencia artificial para respaldar la implementación de Comando y Control Conjunto de Todos los Dominios (JADC2), la nueva inteligencia artificial reunirá instantáneamente todo tipo de datos para brindar a los comandantes una imagen clara del campo de batalla, lo que permitirá tomar buenas y rápidas decisiones.

https://breakingdefense.com/2021/03/exclusive-northcom-developing-testing-ai-tools-to-implement-jadc2/?utm_campaign=Breaking%20News&utm_medium=email&_hsmi=114440486&_hsenc=p2ANqtz-_mIe4jGH8PZvJZZhldHcNw8qyW5SbzVFOV251gM5tAVYBtiIA_t7pSzrZFu1cCKgB5NVE8RaFTlTg8-P1GraWgb9Ot7Q&utm_content=114440486&utm_source=hs_email

Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista

Es indudable que la creciente accesibilidad a internet, así como la rápida evolución de las tecnologías de la información y comunicación (TIC) han propiciado importantes progresos y ventajas para la sociedad. Sin embargo, este mundo virtual (ciberespacio) está repleto de nuevas amenazas que no sólo pueden perjudicarnos individualmente, también pueden llegar a ser capaces de poner en peligro la paz y seguridad internacionales.

Artículo disponible en: *Poveda Criado, Miguel Ángel, Torrente Barredo, Begoña Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista. Opción [en linea]. 2016, 32(8), 509-518[fecha de Consulta 17 de Abril de 2021]. ISSN: 1012-1587.* Disponible en:

https://www.redalyc.org/pdf/310/31048481030.pdf

CIBERCONFIANZA

Retener los RRHH con experiencia en el Ciberespacio

Originado en AFCEA este documento de SixGen trata sobre la demanda de profesionales de seguridad cibernética. Los datos recientes confirman las tendencias de años anteriores de que el dominio de la guerra de la información es un riesgo que toda organización debe tener en cuenta.

Para acceder al documento se le requerirá una previa identificación

https://www.afcea.org/signal/resources/content/SixGen_White_Paper.pdf

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 de 1 de marzo: https://us-cert.cisa.gov/ncas/bulletins/sb21-067

Semana de 8 de marzo: https://us-cert.cisa.gov/ncas/bulletins/sb21-074

Semana de 15 de marzo: https://us-cert.cisa.gov/ncas/bulletins/sb21-081

Semana de 22 de marzo: https://us-cert.cisa.gov/ncas/bulletins/sb21-088

Semana de 29 de marzo: https://us-cert.cisa.gov/ncas/bulletins/sb21-095

Semana de 5 de abril: https://us-cert.cisa.gov/ncas/bulletins/sb21-102

Alerta (AA20-099A)

COVID-19 explotado por actores cibernéticos maliciosos: https://us-cert.cisa.gov/ncas/alerts/aa20-099a

Android cerrando una vulnerabilidad bajo ataque activo

Google ha actualizado su boletín de seguridad de enero de 2021 para informar de una vulnerabilidad que afecta a dispositivos con chipsets Qualcomm estaría siendo explotada activamente.

https://thehackernews.com/2021/03/warning-new-android-zero-day.html

CIBERDELITO

Dos casos relacionados con ciberataques

El Departamento de Justicia de EE.UU. anunció ayer las novedades de dos casos distintos relacionados con ciberataques: un hacktivista suizo y un pirata informático ruso que planeaban plantar malware en la empresa Tesla.

https://unaaldia.hispasec.com/2021/03/el-hacker-del-ransomware-de-tesla-se-declara-culpable-y-un-hacktivista-suizo-es-acusado-de-fraude.html

NOVEDADES

Documento de Interés

El petróleo del siglo 21

En “Comentarios” una publicación de Carrier y Asociados, un estudio profesional dedicado a la información y análisis de mercado, Enrique Carrier y Adriana Berro, publican una interesante investigación donde analizan cómo en pleno siglo XXI, controlar la provisión de chips equivale a haber controlado la producción de petróleo en el siglo XX

El crecimiento de la demanda fue tal que genera problemas de abastecimiento, impactando en múltiples industrias

Para dimensionar la magnitud de lo que está sucediendo, y ante la persistencia de una fuerte demanda, TSMC (Taiwan Semiconductor Manufacturing Company)acaba de anunciar que llevará sus inversiones en ampliar su capacidad productiva. También Samsung e Intel anunciaron fuertes inversiones para instalar

nuevas fábricas. Intel hará lo mismo y además anunció la creación de una unidad independiente llamada Foundry Services, con lo que comenzará a fabricar para terceros y desde los EE.UU.

Estas preocupaciones se ven agudizadas por la creciente importancia política de la industria, acentuada por la pérdida de relevancia en la fabricación en EE.UU y la concentración de la producción en Asia

https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmailchi.mp%2F002cfc413153%2Fsobre-la-escasez-de-chips%3Fe%3Dc469fd07b6&data=04%7C01%7C%7Cd7df8e1fa6984aa3417308d9010dad65%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637541980518275521%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=uk6yLAQXtbiAFINMkmjHWzTtDn9SsUv1T4fcy2AQWBQ%3D&reserved=0

Instituto de Ciberdefensa de las Fuerzas Armadas

El 18 de marzo, en Buenos Aires y en el marco de la 10ma Reunión del Consejo de Dirección de la Universidad de la Defensa Nacional (UNDEF), se concretó la creación del Instituto de Ciberdefensa de las Fuerzas Armadas.

En su exposición, el Ministro de Defensa Argentino, resaltó la real valía de incorporar dentro de la currícula de la formación del personal militar esta capacitación de vital importancia para la defensa nacional.

https://www.fuerzas-armadas.mil.ar/Noticias-actividad-operacional.aspx