OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya

ISSN: en trámite
http://www.esgcffaa.edu.ar/obsciber/

AÑO 2 N° 17
Octubre 2019

OAC Boletín de Octubre 2019

"Los investigadores de RAND recomiendan que las democracias realicen urgentemente una investigación rigurosa sobre la manipulación social para obtener una mejor comprensión de su dinámica"

https://www.rand.org/news/press/2019/09/04.html

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), micro-sitio de la **Escuela Superior de Guerra Conjunta**
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

Documento de Interés

Ataques entre estados mediante Internet.
Estudio de casos orientados por el Esquema Nacional de Seguridad.

Julián Ignacio Alfonso Beltrán, presenta su trabajo final de carrera, en la Universidad Politécnica de Valencia, sobre un tema que hoy ocupa un aspecto importante del panorama estratégico en el Ciberespacio. El trabajo abarca el estudio y recopilación de casos y análisis de técnicas empleados por los estados contra otros estados o particulares y a la inversa, ataques DDOS, phishing, etc., al servicio de causas políticas o en conflictos bélicos o prebélicos y del terrorismo al espionaje.

https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1

CIBERSEGURIDAD

Documento de Interés

El impacto de la computación Cuántica en la Ciberseguridad

Las computadoras cuánticas son ampliamente vistas como una tecnología innovadora, especialmente cuando se emplean en disciplinas como inteligencia artificial, criptografía y análisis de big data. Sin embargo, con la expectativa innegable de la "computación cuántica", surge una gran cantidad de futuras aplicaciones que al momento pueden considerarse como una exageración y dar a confusión si no se comprenden adecuadamente los conceptos de SUPERPOSICIÓN, ENREDO y QuBITS que se describen en el presente artículo. Necesitamos estar preparados para esto en el futuro

https://hcss.nl/sites/default/files/files/reports/HSD-Rapport-Quantum.pdf

CIBERDEFENSA

La relación Público-Privada vista desde la perspectiva de la Reglamentación Europea

CiberElcano presenta un aspecto complejo de la relación público-privada se ha anunciado durante mucho tiempo como un escenario clave en la seguridad cibernética, donde los acuerdos de colaboración pueden garantizar una mayor resistencia a los ataques cibernéticos y respuestas más rápidas a dichos incidentes. Sin embargo, este artículo argumenta que la relación cambiará enormemente en un mundo posterior al Reglamento General de Protección de Datos (RGPD). La relación ahora debe considerarse como una en la que se aumenta la colaboración con medidas coercitivas para cambiar el comportamiento del sector privado en el ciberespacio.

http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari97-2019-steed-cyber-security-how-gdpr-is-already-impacting-public-private-relationship?utm_source=CIBERElcano&utm_medium=email&utm_campaign=48-octubre2019&_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-73e3ddacc0534efe86fd4d3d86ff83d1&esid=8eedbbbd-6dee-e911-a812-000d3a44afcc

CIBERGUERRA

RAND advierte sobre el papel de la guerra de la información

El papel de la guerra de información en la competencia estratégica global se ha vuelto mucho más evidente en los últimos años. Los autores de este informe llaman “manipulación social hostil” al empleo de campañas dirigidas a las redes sociales, falsificaciones sofisticadas, acoso cibernético y hostigamiento de personas, distribución de rumores y teorías de conspiración, entre otras herramientas, siendo su finalidad causar daños al ente que ha sido seleccionado como objetivo

https://www.rand.org/pubs/research_reports/RR2713.html?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-73e3ddacc0534efe86fd4d3d86ff83d1&esid=8eedbbbd-6dee-e911-a812-000d3a44afcc

CIBERCONFIANZA

Vulnerabilidades del Día O en TE Android

Los atacantes están explotando una vulnerabilidad de día cero en el sistema operativo móvil Android de Google que puede darles el control total de al menos 18 modelos de teléfonos diferentes (Pixel 1 y XL, Pixel 2 y XL Huawei P20, Xiaomi Redmi 5ª, Xiaomi Redmi Note 5, Xiaomi A1, Oppo A3, Moto Z3. Teléfonos Oreo LG, Samsung S7, Samsung S8. Samsung S9, dijo el jueves por la noche un miembro del grupo de investigación Proyecto Cero de Google.

https://arstechnica.com/information-technology/2019/10/attackers-exploit-0day-vulnerability-that-gives-full-control-of-android-phones/

CIBERFORENSIA

Acceda a la guía de actualización de Microsoft y actualice su Software

Aquí se presenta la guía de actualización de seguridad de Microsoft, con las soluciones a las últimas 59 vulnerabilidades en productos entre los principales afectados se encuentran Windows, Internet Explorer, Edge, Office, Office SharePoint, el motor de scripting Chakra y los componentes relacionados con el sistema de actualizaciones, el protocolo RDP o el servidor de bases de datos SQL Server.

https://portal.msrc.microsoft.com/en-us/security-guidance

Como Apple advierte a Ud. sobre sitios fraudulentos

Antes de visitar un sitio web, Safari puede enviar información calculada a partir de la dirección del sitio web a Google Safe Browsing y Tencent Safe Browsing para verificar si el sitio web es fraudulento. Estos proveedores de navegación segura también pueden registrar su dirección IP", señala Apple

https://thehackernews.com/2019/10/apple-safari-safebrowsing-tencent.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2090.po0ao0di5a.1ava

CIBERTERRORISMO

Documento de Interés

Ciberterrorismo ¿realidad o Mito?

Pía Martabit Tellechea, ha escrito este cuaderno publicado por el "*Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos*"

La llamada era de la "post-verdad" entrega a la academia de la seguridad internacional especial consideración a la teoría constructivista. Cuando este se utiliza para estudiar el fenómeno "ciberterrorismo", revela que, debido a una falta de evidencia empírica que sustenta la realidad del fenómeno y en contraposición con un elevado uso del concepto tanto en prensa como en la academia, el ciberterrorismo es una realidad discursiva en primer medida y una posiblemente profecía auto cumplida en segundo lugar.

Parte importante de la problemática recae en las dificultades descriptivas encontradas en el concepto terrorismo que emigraron con ellas en su camino al ciberespacio. Este trabajo busca esclarecer la problemática señalada por medio de un análisis de la discusión descriptiva del fenómeno terrorismo y ciberterrorismo en la academia.

https://www.anepe.cl/wp-content/uploads/Cuaderno-de-Trabajo-N°5-2018.pdf

NOVEDADES

WEBINAR ¿Cómo enfrentar este nuevo dominio militar?

Este webinar que continua el Jueves 17 y 24 de octubre a las 1400 hora local, ya completando las sesiones correspondientes a los niveles táctico y operacional, pero como producto interesante ha abierto un foro donde se pueden bajar los videos del mismo y una gran variedad de productos desde libros hasta direcciones para capacitación en Ciberseguridad, aquí adjuntamos su dirección.

http://ciberdefensa.online/index.php