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 3 N° 30
Diciembre 2020

OAC Boletín de Diciembre 2020

"*Los servicios de seguridad e inteligencia [spetssluzhby] de los estados árabes no fueron capaces de impedir la distribución de mensajes [de redes sociales] porque no tenían acceso a los servidores controlando las redes sociales, los cuales están ubicados en el territorio de los servicios de seguridad e inteligencia de los Estados Unidos.*"

Yu. Kuleshov y otros,
"Информационно-психологическое противоборство в современных условиях: теория и практика"
(Guerra de Información-Psicológica en Condiciones Modernas), pág. 107
Extraído del Manual de Guerra de Información Rusa (Keir Giles)

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

Lecturas de verano

Estimados Lectores, despidiendo un nuevo año de observación del ciberespacio, los que componemos este esfuerzo por crear un aporte a la cultura ciberespacial, creímos oportuno aprovechar la oportunidad para sugerir algunas lecturas que posean 2 vertientes, que los entrega en su periodo de descanso anual y que por otro lado aporte ideas, posturas y conocimientos sobre el quinto dominio.

Es por ello que rompemos el protocolo habitual de seguir por temas diferentes notas de información, o científicas para dejarles un conjunto de posibles lecturas que desde nuestra perspectiva pueden resultarles de interés:

Desde ya muchas gracias por seguir acompañándonos y nos encontramos de nuevo en febrero con nuestro primer boletín conteniendo aspectos y acontecimientos de actualidad del ciberespacio de los meses de enero y febrero.

Muchas gracias y aquí van nuestras sugerencias, para bajar en la Tablet, el Teléfono o la Portátil:

Manual de la Resiliencia (Alejandro Corletti Estrada)

La resiliencia, se ha convertido en una de las claves de éxito en la guerra por el 5to Dominio, resistir sin doblegarse y poder continuar operando y reconstituyendo esfuerzos de los sistemas atacados, mientras la pelea continua, podría ser la clave para disuadir en el ciberespacio, en este libro de agradable lectura Alejandro Corletti nos ilustra acerca del gran esfuerzo que significa tener resiliencia en las infraestructuras críticas y en los sistemas de información.

Disponible en: https://blog.segu-info.com.ar/2020/11/libro-gratuito-manual-de-la-resiliencia.html?m=0

Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (OEA-BID)

La Organización de Estado Americanos (OEA), nos ofrece junto con el Banco Interamericano de Desarrollo (BID), un trabajo del Observatorio de Ciberseguridad, ofrecen un reporte acerca de los riesgos, y avances en el área y un posible camino a seguir en Latinoamérica y el Caribe, el documento permite ver la evolución de los países en diferentes aspectos del ciberespacio, de manera gráfica y sencilla, a nuestro país lo pueden encontrar a partir de la página 50

https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

El Informe Global de Amenazas 2020 (Crowdstrike)

Los pedidos de rescate por la información propietaria, han escalado fuertemente llegando a millones, causando interrupciones sin precedentes, los cibercriminales están utilizando datos confidenciales como armas para incrementar la presión sobre víctimas de ransomware. La evolución del "**ecosistema eCrimen**", continúa, madurando y evolucionando de estos y otros temas podremos actualizarnos con este interesante libro de 68 páginas disponible en idioma inglés,

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

La Guerra informativa china: mucho más que APT y propaganda (Guillermo Colom)

Un artículo presentado por THIBER, teh security Think Tank, acerca de la guerra de información China y sus diferencias con otras naciones.

De acuerdo con el artículo para el país oriental este aspecto constituye una de las competencias claves a dominar por parte de su Ejército Popular de Liberación. Es una efímera muestra que podemos encontrar muy desarrollada en una lectura del libro de Liang Xiangsui "La Guerra Irrestricta"

https://www.thiber.org/wp-content/uploads/2020/01/Numero_16_Enero_AnalisisActualidad.pdf

Artificial Intelligence and National Security (Allen y Chan) (Inteligencia Artificial y Seguridad Nacional)

Los avances en el aprendizaje de las máquinas a través de la Inteligencia Artificial (IA) (Machine Learning) representan un punto de inflexión en la automatización de la guerra.

Aunque el ejército de los Estados Unidos y las comunidades de inteligencia están planeando un uso ampliado de la IA, muchas de las aplicaciones más transformadoras aún no han sido abordadas.

El documento, propone tres objetivos para el desarrollo de políticas futuras sobre IA y seguridad nacional: (1) preservar el liderazgo tecnológico de EE. UU. (2) uso pacífico y comercial, y (3) mitigación del riesgo catastrófico.

Los objetivos se desarrollan considerando cuatro casos de tecnología militar transformadora: la nuclear, la aeroespacial, la cibernética y la biotecnológica. Desarrollamos lecciones aprendidas y recomendaciones para la política de seguridad nacional hacia la IA.

https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Ciberespacio: 666 días de observación. Proyecto Observatorio Argentino del Ciberespacio (OAC)

Alejandro A. Moresi, Carlos Amaya, Alejandra Castillo

El artículo presenta una síntesis de la actividad llevada a cabo por el Observatorio Argentino del Ciberespacio (OAC) desde su creación. La propuesta, más allá de tratar la evolución del OAC, intenta mostrar cómo ha sido la interacción y articulación con la sociedad y el medio, comentar las lecciones aprendidas y las estrategias observadas por quienes operan allí, analizando el impacto de las tecnologías que lo componen y, finalmente, dar pautas para su continuidad.

https://www.undef.edu.ar/wp-content/uploads/2020/10/04_REVISTA-DEFENSA-NACIONAL.pdf (Paginas 121 a 152)

http://www.cefadigital.edu.ar/bitstream/1847939/1554/1/MORESI%2c%20AMAYA%2c%20CASTILLO.%20Defensa%20Nacional%20Nro.%204%2c%20arti%cc%81culo%204.pdf

Irán una potencia cibernética en construcción (Enrique Fojón Chamorro)

En este caso también es un artículo presentado por THIBER, teh security Think Tank, generado como consecuencia del ataque con drones que terminó con la muerte del General Inarní Qasem Soleimani.

https://www.thiber.org/wp-content/uploads/2020/01/Numero_16_Enero_Comentario.pdf

Cuadro de políticas de ciberseguridad del Departamento de Defensa

El Departamento de Defensa de los EE.UU., muestra aquí una matriz de políticas de ciberseguridad. La misma presenta diferentes aspectos del problema y para cada ítem da la posibilidad de acceder a un sinnúmero de documentos solo haciendo "click" en cada punto de la misma, ofreciendo una visión integral y completa de las políticas, estrategia, planes acciones etc… que realiza el país del norte en el ámbito de la de ciberseguridad.

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiugIOu88rtAhUOJLkGHclcAowQFjAAegQIAhAC&url=https%3A%2F%2Fdodiac.dtic.mil%2Fwp-content%2Fuploads%2F2019%2F01%2Fia-policychart-7-Jan-19-DoDIN.pdf&usg=AOvVaw2wGVh_spDx0arRHcno0GM4