



**OBSERVATORIO ARGENTINO
DEL
CIBERESPACIO**

Director del Proyecto: TC (R) Mg. Ing. Antonio Castro Lechtaler
Codirector: BM (R) Mg. Alejandro Moresi

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

AÑO 2 N° 10
Marzo 2019

OAC Boletín de Marzo

"Cuando vas a la guerra, sabes las consecuencias... para eso te unes ... solo tienes miedo cuando empieza a suceder y cualquiera que diga que no está asustado en la batalla es estúpido".

Jon Gaunt

Excombatiente Inglés en Malvinas

<https://sputniknews.com/radio-shooting-from-the-lip/201903081073067990-our-politicians-are-the-problem/>

Contenidos

CIBERDEFENSA.....	2
Documento de Interés.....	2
Operaciones Ciberespaciales.....	2
Las Operaciones Especiales y su aplicaciones en campo cibernético	2
CIBERGUERRA.....	2
Submarinos Rusos merodean los cables de conexión globales	2
La carrera de armas cuánticas que puede transformar el orden mundial.....	3
El papel de la web oscura en las futuras guerras cibernéticas.....	3
El Debate Alemán Sobre La Tecnología 5 G China	3
CIBERSEGURIDAD	3
El despliegue de las redes 5G, o la geopolítica digital.....	3
Documento de Interés.....	3
Guía Española de notificación y Gestión de Ciberincidentes	3
Una Revisión Estrategia de Ciberseguridad desde la perspectiva Privada.....	4
CIBERFORENSIA	4
Facebook permite ver fotos privadas videos y archivos de otros usuarios	4
Google revela un error en el núcleo de Apple macOS	4



**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>.

Este esfuerzo es posible por el financiamiento que el observatorio recibe de la Universidad de la Defensa Nacional, a través de los programas UNDEFI y en conjunto con el Centro de Estudios de Prospectiva Tecnológica Militar "Gral. Mosconi".

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

CIBERDEFENSA

Documento de Interés

Operaciones Ciberespaciales

El JP 3-12, es el reglamento conjunto de los Estados Unidos de Norteamérica para la Operaciones Ciberespaciales. La versión presentada es una publicación no clasificada, que trata aspectos como la descripción general de las Operaciones Ciberespaciales, principales actividades en las operaciones ciberespaciales, roles y responsabilidades de los diferentes niveles de autoridad en la cuestión ciberespacial, planeamiento, ejecución y evaluación de operaciones ciberespaciales

https://fas.org/irp/doddir/dod/jp3_12.pdf

Las Operaciones Especiales y sus aplicaciones en campo cibernético

Un equipo de oficiales de diferente extracción de las Fuerzas Armadas de los EE.UU., presentan una interesante apreciación acerca de como las operaciones especiales guardan una relación intrínseca con la operaciones ciberespaciales que permiten una explotación de su doctrina

<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1737001/applying-irregular-warfare-principles-to-cyber-warfare/>

CIBERGUERRA

Submarinos Rusos merodean los cables de conexión globales

Submarinos rusos han aumentado su actividad en torno a datos submarinos en los cables en el Atlántico norte, que proporcionan conexión a Internet y otras conexiones de comunicaciones entre América del Norte y Europa, esto podría darle al Kremlin el poder de aprovechar datos vitales o cortar la conectividad de los cables una vez que hayan asegurado su capacidad de aislarse de internet.

https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?utm_term=.26dd1be31437



La carrera de armas cuánticas que puede transformar el orden mundial

La carrera entre EE.UU y China por la creación de un computador cuántico , tomado tintes de los años 60 en la competencia por llevar al hombre a la Luna. El problema está en que la creación de una computadora cuántica funcional incrementa de manera dramática la posibilidad de un ataque contra los sistemas militares e infraestructura de un potencial enemigo. La clave de este potencial entre otras cosas permitiría detectar movimientos que los sistemas de radar tradicionales no pueden por ejemplo aviones furtivos.

<https://mundo.sputniknews.com/tecnologia/201705191069295765-ordenador-cuatico-carrera-militar/>

El papel de la web oscura en las futuras guerras cibernéticas

La guerra evoluciona y se está centrando en "WEB oscura" o "WEB profunda", la Internet ha afectado a la seguridad en la última década y su influencia será mayor en los próximos años. El artículo busca establecer un marco conceptual de la Red Oscura como una especie de paisaje caracterizado por una serie de problemas de amenazas y actores que los profesionales del ciberespacio deberían conocer.

https://www.realcleardefense.com/2019/02/25/the_role_of_the_dark_web_in_future_cyber_wars_to_come_306775.html#

El Debate Alemán Sobre La Tecnología 5 G China

Estados Unidos, Australia y Nueva Zelanda han prohibido la tecnología de las empresas de Tecnología de la Información relacionadas con sistema 5G, provenientes de China, Huawei y ZTE. Varios países europeos, entre ellos Francia, Gran Bretaña, España, Polonia y la República Checa están reconsiderando su estrategia basada en preocupaciones de seguridad nacional. Alemania está aún indecisa y su papel es crítico en la UE.

<http://www.gmfus.org/blog/2019/02/15/why-german-debate-5g-and-huawei-critical>

CIBERSEGURIDAD

El despliegue de las redes 5G, o la geopolítica digital

Vicente Moret Millás | Letrado de las Cortes Generales, Letrado de la Comisión Mixta de Seguridad Nacional y profesor asociado IE Law School. Nos ilustra acerca de cómo el despliegue de las nuevas redes de comunicaciones 5G está poniendo de relieve la existencia de una competición geopolítica por el control e implantación de las nuevas tecnologías.

<http://www.realinstitutoelcano.org/wps/wcm/connect/1c87499a-f0df-4d11-bc4f-c40d30138fb3/ARI31-2019-Moret-despliegue-de-redes-5G-geopolitica-digital.pdf?MOD=AJPERES&CACHEID=1c87499a-f0df-4d11-bc4f-c40d30138fb3>

Documento de Interés

Guía Española de notificación y Gestión de Ciberincidentes

Esta guía confeccionada por el gobierno español, nos permite conocer la notificación y gestión de ciberincidentes, detectada por sus CERT, se define como la referencia estatal respecto a la notificación de ciberincidentes (bien sea la comunicación de carácter obligatoria o potestativa), así como en lo relativo a la demanda de capacidad de respuesta a los incidentes de ciberseguridad.



<http://www.interior.gob.es/documents/10180/9814700/Gu%C3%ADa+Nacional+de+notificaci%C3%B3n+y+gesti%C3%B3n+de+ciberincidentes/f01d9ed6-2e14-4fb0-b585-9b0df20f2906>

Una Revisión Estrategia de Ciberseguridad desde la perspectiva Privada

Javier Alonzso Lecuit desde el Ciberelcano, comenta acerca de cómo se encuentra la revisión de la estrategia de ciberseguridad española desde la perspectiva del sector privado el cual posee una implicancia importante en la misma.

http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari18-2019-alonsolecuit-revision-estrategia-ciberseguridad-nacional-vision-sector-privado?utm_source=CIBERelcano&utm_medium=email&utm_campaign=41-febrero2019

CIBERFORENSIA

Facebook permite ver fotos privadas videos y archivos de otros usuarios

La privacidad esta en jaque, millones de usuarios que usan el chat de Facebook todos los días. Imagínese si él revela mensajes de audio, fotos o videos de personas muy VIP, etc., como ejemplo, es realmente peligroso

<https://medium.com/bugbountywriteup/disclose-private-attachments-in-facebook-messenger-infrastructure-15-000-ae13602aa486>

Google revela un error en el núcleo de Apple macOS

Mohit Kumar, investigador de seguridad cibernética en la división Project Zero de Google ha revelado públicamente detalles y una vulnerabilidad de prueba de concepto de una vulnerabilidad de seguridad de alta severidad en el sistema operativo macOS después de que Apple no lanzara un parche dentro de los 90 días de haber sido notificado.

<https://thehackernews.com/2019/03/cybersecurity-macos-hacking.html>

*Copyright © */2018/* */Escuela Superior de Guerra Conjunta/*, All rights reserved.*

/Observatorio Argentino del Ciberespacio /

Nuestra dirección postal es:

/Luis María Campos 480 - CABA - República Argentina /

Nuestro correo electrónico:

/observatorioargentinodelciberespacio@conjunta.undef.edu.ar /

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

