ISSN: 2718-6245

# OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Editora: Bib Alejandra Castillo

ISSN: 2718-6245
http://www.esgcffaa.edu.ar/esp/oac-boletines.php

AÑO 3 N° 27
Septiembre 2020

## OAC Boletín de Septiembre 2020

"El hardware es fácil de proteger: encerrarlo en una habitación, encadenarlo a un escritorio o comprar uno de repuesto. La información plantea más un problema: puede existir en más de un lugar; ser transportada a la mitad del planeta en segundos; y ser robada sin su conocimiento".

***Bruce Schneier***

**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

### Construyendo la Gran Estrategia para la Ciberseguridad

La Comisión *Cyber Solarium*, un panel de legisladores expertos constituido por el Congreso, fue creado para abordar el conflicto cibernético de la misma manera que su predecesor de la era Truman abordó la confrontación de la Guerra Fría entre Estados Unidos y la Unión Soviética. Un artículo en la edición de agosto de la revista *SIGNAL* ("Los líderes buscan una gran estrategia para la ciberseguridad") exploró la teoría de la comisión de la disuasión por negación y cómo adoptó el concepto de resiliencia.

https://www.afcea.org/content/building-grand-strategy-cybersecurity?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=0OG47#

## CIBERDEFENSA

### El departamento de Defensa de los Estados Unidos publica el "*Military and Security Developments Involving the Peoples Republic of China* 2020"

China busca liderar el cambio hacia la "guerra inteligente" a través de su Fusión Civil-Militar (MCF), estrategia de desarrollo reforzando su investigación y desarrollo (I + D). En 2015, presentó una estrategia nacional, estableciendo nuevas organizaciones y promulgando políticas para impulsar el desarrollo de tecnologías de doble uso e integrar aún más la administración civil y militar.

Con una fuerza que totaliza aproximadamente dos millones de efectivos en las fuerzas regulares, el Ejército Popular de Liberación busca modernizar sus capacidades y mejorar sus competencias en todos los dominios de la guerra para que, como fuerza conjunta, pueda realizar toda la gama de operaciones terrestres, aéreas y marítimas, así como en el espacio, contraespacio, guerra electrónica (EW) y operaciones cibernéticas.

Además de mejorar las capacidades de ataque, defensa aérea, antimisiles, antisuperficie y antisubmarina, China se centra en la información, el ciberespacio y las operaciones espaciales y contraespaciales.

Obtiene tecnología extranjera a través de inversión extranjera directa, adquisiciones en el extranjero, importaciones de tecnología, el establecimiento de centros extranjeros de investigación y desarrollo (I + D), empresas, investigación y asociaciones académicas, reclutamiento de talentos y espionaje industrial y cibernético.

Cuenta con una Fuerzas de Apoyo Estratégico (SSF) que es una organización de nivel de comando del ambiente de operaciones, creada para centralizar las misiones estratégicas de guerra espacial, cibernética, electrónica y psicológica del EPL.

El Departamento de Sistemas de Red de la SSF es responsable de la guerra de información con una misión conjunta que incluye la guerra cibernética, reconocimiento técnico, guerra electrónica y guerra psicológica.

Es opinión de los líderes de China, lograr el dominio de la información y negar a los adversarios el uso del espectro electromagnético como hecho necesario para tomar y mantener la iniciativa estratégica en un conflicto, desarrollando capacidades de guerra electrónica como bloqueadores de satélites; capacidades cibernéticas ofensivas; y armas de energía dirigida todo asistido por tecnología de Inteligencia Artificial (IA), computación en la nube, análisis de big data, informática cuántica y sistemas no tripulados, de aplicación para el ejército.
https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

## CIBERGUERRA

### La resiliencia como arma

La resiliencia cibernética es especialmente importante para el Ejército de los Estados Unidos, ya que el servicio depende de las operaciones cibernéticas en un grado cada vez mayor. El Departamento de Defensa describe la resiliencia cibernética como la capacidad de los sistemas para resistir, absorber y recuperarse o adaptarse a una ocurrencia adversa durante la operación, por lo que, en consecuencia, el Ejército debe poder continuar llevando a cabo su misión cuando sus sistemas cibernéticos están comprometidos o bajo ataque.

https://www.afcea.org/content/army-gears-battle-cyber-resilience?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=L7J07#

### Cooperar para derrotar amenazas híbridas

Así como las amenazas híbridas explotan la sinergia de diversos actores y actividades, también deberían hacerlo nuestras defensas híbridas. Desde 2016, la OTAN y la Unión Europea han identificado la lucha contra las amenazas híbridas como una prioridad para la cooperación. El nuevo Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas *( Hybrid COE* ) en la capital de Finlandia, Helsinki, juega un papel único en facilitar esta cooperación.

https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

### Documento de Interés

#### *La guerra secreta de la influencia cibernética*

David *Tayouri Ben-Gurion University of the Negev | bgu · Department of Information Systems Engineering* Subdirector, Gerente de I + D en cibernética, Dirección de Ingeniería, *Cyber Division en Defense de Ashdod*, distrito de HaDarom (sur), Israel. Es además profesional con un Master en Ciencias con Honores, enfocado en Ciencias de la Computación de la Universidad Bar-Ilan, desarrolla en este interesante artículo una descripción de las operaciones de ciberinfluencia, posibles daños en los que pudieran incurrir y cómo se llevan a cabo. Además, el artículo analizará los desafíos de identificar tales operaciones y detallará varios parámetros indicativos con qué operaciones de ciberinfluencia se pueden identificar.

https://www.researchgate.net/publication/340136185_The_Secret_War_of_Cyber_Influence_Operations_and_How_to_Identify_Them

## CIBERCONFIANZA

### China combina el poder económico y político para la primacía de las telecomunicaciones

Un nuevo dominio de Internet y 5G tiene como objetivo impulsar la fortaleza del gobierno. Según expertos en Internet los movimientos globales de China para ganar hegemonía tecnológica sobre 5G y remodelar Internet para que se adapte a sus propias necesidades ofrecen el potencial de darle el control del mercado de telecomunicaciones y la información en sí. Como mínimo, lograría el dominio del mercado. Pero a lo sumo, controlaría tanto la naturaleza de Internet como la información que fluye a través de ella.

https://www.afcea.org/content/china-blends-economic-and-political-might-telecom-primacy?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=wNG47#

## CIBERSEGURIDAD

### La pandemia de COVID-19 plantea la necesidad de ampliar la identificación digital.

La gestión de identidad actual está fragmentada y descentralizada, y se basa en muchos sistemas diferentes para autenticar a las personas y gestionar las identidades. Las organizaciones utilizan una variedad de herramientas inconexas, desde contraseñas y tarjetas inteligentes hasta datos biométricos. En cambio, las organizaciones deberían adoptar un enfoque más holístico. Cada vez más, la gestión integral de identidades debe tener un componente digital, especialmente durante la pandemia de COVID-19, según Combiz Abdolrahimi, líder global de innovación y tecnología emergente de Deloitte .

https://www.afcea.org/content/re-imagining-identity-management?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=1OG47#

### Estrategia Nacional de Ciberseguridad aún hace falta en México

De acuerdo con la firma de ciberseguridad Kaspersky, a nivel internacional México ocupa el lugar 9 de las naciones que más sufren ataques por malware, según lo publicado por XTREMSECURE el 14 de agosto de 2020.

El citado artículo concluye mencionando la necesidad de integrar un plan nacional para formar a las nuevas generaciones de expertos en el tema de ciberseguridad mediante una coordinación profunda con el sector educativo del país.

http://www.xtremsecure.com.mx/estrategia-nacional-de-ciberseguridad-aun-hace-falta/

## CIBERFORENSIA

### Informes de la Agencia de Ciberseguridad e Infraestructuras de los EE.UU

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EE.UU., estos boletines proporciona 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 03 de agosto | https://us-cert.cisa.gov/ncas/bulletins/sb20-223 |
| Semana de 10 de agosto: | https://us-cert.cisa.gov/ncas/bulletins/sb20-230 |
| Semana de 17 de agosto: | https://us-cert.cisa.gov/ncas/bulletins/sb20-237 |
| Semana de 24 de agosto: | https://us-cert.cisa.gov/ncas/bulletins/sb20-244 |
| Semana de 31 de agodto: | https://us-cert.cisa.gov/ncas/bulletins/sb20-251 |

## AGENDA de INTERÉS

### Cursos y Seminarios en Línea

#### *Agencia de Seguridad de Infraestructura y Ciberseguridad*

La 3ra Cumbre Nacional Anual de Ciberseguridad de CISA se llevará a cabo virtualmente como una serie de seminarios web todos los miércoles durante cuatro semanas a partir del 16 de septiembre y hasta el 7 de octubre. Cada evento se desarrollará desde el mediodía hasta las 2:00 p.m.EDT, La agenda prevista incluye:

- Miércoles 16 de septiembre: Key Cyber Insights
- Miércoles 23 de septiembre: Liderando la transformación digital
- Miércoles 30 de septiembre: Diversidad en ciberseguridad
- Miércoles 7 de octubre: Defender nuestra democracia

https://www.eventbrite.com/e/3rd-annual-national-cybersecurity-summit-tickets-114443214736

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 | *