



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 3 N° 23
Mayo 2020

OAC Boletín de Mayo 2020

“Si reconocemos que los ‘nuevos’ principios de la guerra, ya no están ‘empelando la fuerza armada para obligar al enemigo a someterse a la voluntad de uno’, sino que están utilizando todos los medios, incluyendo la fuerza armada o no armada, militar y no militar y medios letales y no letales para obligar al adversario a aceptar los intereses de uno.”

La Guerra Irrestricada
Cnel Qiao Liang y Cnel Wang Xiangsui

Tabla de Contenidos

ESTRATEGIA.....	2
<i>Documento de Interés</i>	2
La Estrategia Nacional de Seguridad de los EEUU para la tecnología 5 G	2
<i>Feudalismo Digital una visión Filosófica desde Oriente</i>	2
<i>El progreso tecnológico exponencial, especialmente en el dominio digital, está afectando a todos los ámbitos de la vida</i>	2
CIBERDEFENSA	3
<i>La herramienta un Arma secreta de la Inteligencia Israelí</i>	3
DOCUMENTO DE INTERÉS	3
La Ciberseguridad Militar y el empleo de Fuerzas de Reserva	3
CIBER-ESCUDO DIGITAL.....	3
CIBERTERRORISMO	4
<i>El Terrorismo Cibernético</i>	4
CIBERCONFIANZA.....	4
<i>La Crisis del COVID 19 y la Inteligencia Artificial</i>	4
CIBERSEGURIDAD.....	4
<i>Documento de Interés</i>	4
Seguridad Cibernética 2020 las brechas	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>.

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

La Estrategia Nacional de Seguridad de los EEUU para la tecnología 5 G

El gobierno de los EEUU, ha publicado en Marzo del 2020 su Estrategia de Nacional de Seguridad para la tecnología 5G, la que entiende es un elemento esencial para su seguridad y prosperidad, tanto para el gobierno, como empresas y consumidores en el siglo XXI, debido a sus capacidades de conectividad que permitirán que decenas de miles de millones de dispositivos nuevos aprovechen el poder de Internet, transformando la forma en que vivimos, trabajamos, aprendemos y nos comunicamos.

<https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf?cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-7f85b85c378c424d9f93bc3be0dfe7bc&esid=96e47e8d-a479-ea11-a811-000d3a210cf2>

<https://share.america.gov/es/paises-en-praga-acuerdan-en-materia-de-seguridad-de-las-redes-5g/>

Feudalismo Digital una visión Filosófica desde Oriente

En el diario Clarín el filósofo coreano y ensayista Byung-Chul Han, alerta que el coronavirus podría llevarnos a una sociedad de vigilancia total: el régimen chino podría imponer el control digital y jaquear las libertades occidentales.

https://www.clarin.com/cultura/byung-chul-vamos-feudalismo-digital-modelo-chino-podria-imponerse_0_QqOkCraxD.html

El progreso tecnológico exponencial, especialmente en el dominio digital, está afectando a todos los ámbitos de la vida

Tanto a nivel nacional como multilateral, las tecnologías nuevas y potencialmente disruptivas desafían drásticamente la forma en que se conciben y aplican políticas de disuasión y defensa en términos generales.



https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.nato.int%2Fdocu%2Freview%2Farticles%2F2020%2F05%2F05%2Fgame-of-drones-how-new-technologies-affect-deterrence-defence-and-security%2Findex.html%3Futm_medium%3Demail%26utm_campaign%3DNATO%2520Review%2520Emerging%2520and%2520disruptive%2520technologies%26utm_content%3DNATO%2520Review%2520Emerging%2520and%2520disruptive%2520technologies%2BCID_6c863933a90444666cd033e5a33e4225%26utm_source%3DEmail%2520marketing%2520software%26utm_term%3DGame%2520of%2520drones%2520How%2520new%2520technologies%2520affect%2520deterrence%2520defence%2520and%2520security&data=02%7C01%7C%7CEcb7371232844c8b9df408d7f144f132%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637243150713547671&sdata=X3pdPGolpuxwO1RC41dkHC3q2rQG4HPi88iqjLkiQrE%3D&reserved=0

CIBERDEFENSA

La herramienta un Arma secreta de la Inteligencia Israelí

El sistema de Inteligencia interior de Israel, conocido como “Shin Bet” o el Shabak, denomina “la herramienta” a una impresionante base de datos, que recoge y guarda información sobre todos los ciudadanos y habitantes de Israel. Se creó en su momento para contar con información sobre terroristas, pero ahora se está utilizando para rastrear y hacer el seguimiento de enfermos de coronavirus. Fuentes del Shabak dicen: “Manejamos la información con muchísimo cuidado y de acuerdo con la ley”.

<https://www.ynetespanol.com/global/israel/article/ryLBM0aK8>

Documento de Interés

La Ciberseguridad Militar y el empleo de Fuerzas de Reserva

El proyecto de Ciberdefensa del Centro de Estudios para la Seguridad de Zúrich, ha realizado un trabajo con conclusiones acerca de la importancia del desarrollo de fuerzas de reserva cibernética, concluyendo que no existe una solución única que se adapte a todos los estados. Las fuerzas de reserva, al ser un servicio militar entre el servicio militar en servicio activo y la vida civil, parecen particularmente adecuadas para las tareas militares de seguridad cibernética y parecen ser una solución para atraer personal calificado. El adecuado desarrollo de una Fuerza Cibernética de reserva es un proceso de prueba y error. El estudio se basó en la experiencia de: Estonia, Francia, Israel, Suiza, EE.UU. y Finlandia

[https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-03-military-cybersecurity.pdf?_cldee=YW1vcMvZaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-b7b0f5b701ef4f87b6adc69b759447b3&esid=9488c3d7-9580-
ea11-a811-000d3a44afcc](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-03-military-cybersecurity.pdf?_cldee=YW1vcMvZaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-b7b0f5b701ef4f87b6adc69b759447b3&esid=9488c3d7-9580-
ea11-a811-000d3a44afcc)

Ciber-escudo Digital

Israel creará un ciber-escudo para proteger a los hospitales de ese país contra ataques hackers , los que se han incrementado de manera sensible durante la pandemia

<https://www.israeleconomico.com/tecnologia-y-ciencia/coronavirus-israel-creara-un-ciber-escudo-para-proteger-hospitales-contr-hackers/>



CIBERTERRORISMO

El Terrorismo Cibernético

Un interesante artículo que introduce acerca de la disyuntiva del tratamiento del terrorismo cibernético, a partir del concepto que no importa el objetivo sino el sujeto y el ataque si es terrorismo o no es un tema posterior desde la perspectiva cibernética se debe tratar el problema de intromisión u obstrucción de los sistemas protegidos.

http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari47-2020-soesanto-cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will?utm_source=CIBERelcano&utm_medium=email&utm_campaign=54-abril2020&cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-b7b0f5b701ef4f87b6adc69b759447b3&esid=9488c3d7-9580-ea11-a811-000d3a44afcc

CIBERCONFIANZA

La Crisis del COVID 19 y la Inteligencia Artificial

La situación de la pandemia global, ha mostrado una metodología de control poblacional intrusiva y exhaustiva a través de la Inteligencia Artificial (IA), si bien las capacidades de control poblacional a través de la IA era conocida en algunos ámbitos, hoy es pública y preocupa acerca de los niveles de intromisión en la libertad de las personas, al respecto el IEEE, ha realizado un estudio sobre la directiva europea para evitar este tipo de situaciones.

http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEE036_2020LORCOT_CovidDigital.pdf

CIBERSEGURIDAD

Documento de Interés

Seguridad Cibernética 2020 las brechas

El Analista Emma Johns, presenta un documento que encuesta acerca de los incumplimientos cuantitativo y cualitativo basado en un estudio de empresas del Reino Unido y organizaciones benéficas. Su objetivo es ayudar a entender la naturaleza y el significado de las amenazas de seguridad cibernética que enfrentan. La encuesta cuantitativa fue realizada en invierno 2019 y análisis cualitativo a principios de 2020.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875573/Main_report_-_Cyber_Security_Breaches_Survey_2020.pdf?cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-b7b0f5b701ef4f87b6adc69b759447b3&esid=9488c3d7-9580-ea11-a811-000d3a44afcc