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 5 N° 42
Marzo 2022

OAC Boletín de Marzo 2022

"El impacto de largo alcance de las redes sociales, la expansión de la tecnología de la información, la extendida disponibilidad de comunicaciones inalámbricas, y las campañas de influencia de la competencia han afectado y cambiado considerablemente el carácter de la guerra moderna".

Patrick M. Shanahan, Subsecretario de Defensa de los EEUU

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), **es un micro-sitio de la Escuela Superior de Guerra Conjunta de la Facultad Militar Conjunta, editado y publicado por el Instituto de Ciberdefensa de las Fuerzas Armadas**
URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php.
Esta publicación mensual se encuentra inserta en el **Nodo 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 ambiente operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

ESTRATEGIA

La inteligencia en las Operaciones de Información

En el Analista, Manu Robledo dice a cerca de "las actividades de información afectan al carácter o al comportamiento de las personas, mediante el uso de la información, para influir en sus percepciones y su comprensión, y abarcan un amplio espectro de actividades diseñadas para afectar a una audiencia objetivo en tres aspectos: sus capacidades, su comprensión y su voluntad. Se trata pues de promover percepciones, actitudes y comportamientos favorables a las operaciones propias de determinadas audiencias e influir en la toma de decisiones humanas o automatizadas. Esta función proporciona la posibilidad de integrar la generación y preservación de información favorable junto con el aprovechamiento de aspectos informativos inherentes a las actividades, su finalidad es promover actitudes favorables a las operaciones propias."

https://elanalista.com.ar/la-inteligencia-en-las-operaciones-de-informacion/

El esfuerzo del pentágono para suministrar capacidades de la nube en todo el departamento se retrasa nuevamente

El Departamento de Defensa está retrasando la adjudicación de su último programa multimillonario para proporcionar servicios comerciales en la nube.

Amazon Web Services, Google, Microsoft y Oracle fueron nombrados por el Pentágono como oferentes para el contrato.

https://www.nextgov.com/it-modernization/2022/03/pentagons-effort-supply-departmentwide-cloud-capabilities-delayed-again/363787/

https://fcw.com/it-modernization/2021/11/dod-names-cloud-contenders-in-jedi-replacement/259177/

CIBERSEGURIDAD

Documento de Interés

Operaciones electromagnéticas: deshaciendo el nudo gordiano del multidominio

Desde que en 2016 el Ejército de los Estados Unidos empezara el desarrollo del concepto operativo de las Operaciones en el Multidominio (MDO), este está siendo adoptado por la OTAN y por las Fuerzas Armadas de países occidentales, entre las que se encuentran las españolas. Las MDO guiarán la modernización y el desarrollo de capacidades, buscando derrotar múltiples desafíos en todos los dominios, incluyendo el espacio y el ciberespacio, de forma que se mantenga la coherencia en las operaciones. La sinergia, operando simultáneamente en los 5 dominios actuales, se anticipa un problema de difícil solución. Entender el entorno operativo como un «conjunto de dominios» reconocería al espectro electromagnético (EMS) como dominio, siendo el nexo común a los anteriores, lo colocaría por encima de ellos. La superioridad en el EMS debe alcanzarse y mantenerse, siendo condición indispensable para el planeamiento y ejecución de las MDO.

https://www.ieee.es/publicaciones-new/documentos-de-opinion/2022/DIEEEO22_2022_JUAMAR_Operaciones.html

CIBERDEFENSA

Las tropas cibernéticas frente a la crisis en Ucrania

La guerra en Ucrania ha proporcionado una llamada de atención para los ciberdefensores militares de EE UU, que enfrentan decisiones difíciles sobre cómo desplegar recursos limitados, dijo el general Chad D. Raduege, director de información del Comando Europeo de EEUU.

Pero frente a una crisis que exige implementaciones ágiles en EEUU junto con una amplia variedad de aliados, lo que significa el empleo de pequeños equipos que operan desde ubicaciones desconocidas, no había suficiente equipamiento de defensa cibernética para todos, dijo Raduege, respondiendo una pregunta de la audiencia por parte del Mayor retirado. Burke Wilson, ex subsecretario adjunto de defensa para política cibernética, quien anteriormente estuvo al mando de Air Forces Cyber.

https://www.airforcemag.com/cyber-troops-stretched-thin-ukraine-response-nato-common-air-picture/ .

Comando y control de todos los dominios conjuntos (JADC2)

En su sesión del 21 de enero del presente año, el Servicio de Investigación del Congreso de los Estados Unidos, trató el concepto del sistema de Comando y Control de dominio conjunto (JADC2), que es para el Departamento de Defensa de los EEUU (DoD's), conectar a los sensores de todos los servicios militares (Fuerza Aérea, Ejército, Cuerpo de Marina, Marina y Fuerza Espacial), en una sola red. Tradicionalmente, cada uno de los servicios militares desarrolló su propia red táctica que era incompatible con los de otros servicios (es decir, las redes del ejército no pudieron interactuar con las redes de la Fuerza de la Marina o la Fuerza Aérea). Los funcionarios del DoD han argumentado que los futuros conflictos pueden requerir

que se tomen decisiones en cuestión de horas, minutos o potencialmente segundos en comparación con el proceso actual para analizar el entorno operativo de los comandos. También han declarado que la arquitectura de control existente en el departamento es insuficiente para satisfacer las demandas de la Estrategia de Defensa Nacional (NDS). El Congreso puede estar interesado en el concepto porque se está utilizando para desarrollar gran cantidad de programas de adquisiciones de alto perfil.

Los analistas también preguntan: "¿quién tendría autoridad de toma de decisiones a través de los dominios?"

https://sgp.fas.org/crs/natsec/IF11493.pdf

CIBERGUERRA

La inteligencia potencia capacidades cibernéticas

La comunidad de inteligencia (IC) ha enfatizado que la segunda época tecnológica de la información se definirá, en parte, por la creación de un ecosistema de nube integrado, flexible, interoperable y seguro. Este entorno deberá proporcionar a los recopiladores de datos y analistas de todo el IC acceso a las últimas herramientas y tecnologías, como inteligencia artificial (IA) y aprendizaje automático (ML), y debe admitir flujos de trabajo dentro y entre múltiples dominios de seguridad.

https://info.breakingdefense.com/hubfs/Booz_Allen_Hamilton_multi_cloud_Pathfinder_PDF.pdf

Interesante análisis sobre la situación ciber en el conflicto Rusia-Ucrania

(Autor: el equipo del sitio CIBER PRISMA liderado por la Mg. Susana García sobre la base del artículo publicado por Paulo Sergio Pagliusi "Guerra cibernética Ruso-Ucraniana-Lecciones para Brasil y el mundo". Reproducción autorizada en castellano del artículo publicado por DCiber de Brasil.-)

La trayectoria de los ciberataques llevados a cabo por Rusia contra Ucrania, y viceversa, demuestran que, aunque realizada de forma encubierta, esta ciberguerra fría entre ambas naciones se ha venido intensificando desde hace casi una década, siendo un componente precursor de la guerra posterior.

Las siguientes secciones revelan los ataques cibernéticos que se originan en ambos lados, organizados en una línea de tiempo. En estas batallas libradas en el ciberespacio se puede notar el predominio de victorias más significativas por parte de Rusia, en vista de su posible mejor preparación en relación a Ucrania.

https://ciberprisma.org/2022/03/28/guerra-cibernetica-ruso-ucraniana-lecciones-para-brasil-y-el-mundo-paulo-sergio-pagliusi/

CIBERCONFIANZA

Consideraciones de seguridad ocultas al pasar a 5G

Las ventajas de la tecnología inalámbrica 5G en el gobierno también serán transformadoras, y los militares verán muchas ganancias potenciales. Los militares podrán, por ejemplo, colocar miles de sensores, drones, vehículos autónomos, combatientes, dispositivos IoT y casi todo lo demás en una red 5G, sin preocuparse demasiado por las limitaciones de ancho de banda. Esa es una de las razones por las que los militares han asumido un papel de liderazgo en la adopción de 5G.

https://www.nextgov.com/emerging-tech/2022/03/hidden-security-considerations-when-moving-5g/363456/

CIBERFORENSIA

Informes Semanales

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EEUU, estos boletines proporcionan 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 del 28 de febrero: https://www.cisa.gov/uscert/ncas/bulletins/sb22-066

Semana del 7 de febrero: https://www.cisa.gov/uscert/ncas/bulletins/sb22-045

Semana del 14 de febrero: https://www.cisa.gov/uscert/ncas/bulletins/sb22-052

Semana del 21 de febrero: https://www.cisa.gov/uscert/ncas/bulletins/sb22-059

Semana del 28 de febrero: https://www.cisa.gov/uscert/ncas/bulletins/sb22-066

Semana del 7 de marzo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-073

Semana del 14 de marzo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-080

Semana del 21 de marzo: https://www.cisa.gov/uscert/ncas/bulletins/sb22-087

CISA tiene conocimiento de una vulnerabilidad de escalada de privilegios en las versiones 5.8 y posteriores del kernel de Linux conocida como "Dirty Pipe" (CVE-2022-0847). Un atacante local podría aprovechar esta vulnerabilidad para tomar el control de un sistema afectado.

https://www.cisa.gov/uscert/ncas/current-activity/2022/03/10/dirty-pipe-privilege-escalation-vulnerability-linux

https://www.nextgov.com/?oref=ng-nav

CIBERDELITO

Chema Alonso entrevista a César Cerrudo el hacker "retranquilo"

Cesar Cerrudo, al que solemos llamar el hacker «retranquilo» por la calma y serenidad que transmite y por su forma calmada de expresarse, es, probablemente por mérito propio, uno de los hackers argentinos más famosos del mundo. Sus investigaciones le han labrado un impacto mundial.

https://unaaldia.hispasec.com/2022/03/chema-alonso-entrevista-a-cesar-cerrudo-el-hacker-retranquilo.html

NOVEDADES

- Con este número retomamos nuestras ediciones luego de dos meses de haberlas suspendido por razones de reorganización de la estructura académica de este Instituto, siendo este el primer número publicado desde el **INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS**.