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 2 N° 16
Septiembre 2019

OAC Boletín de Septiembre 2019

"La primer etapa en el proceso de protección de los datos personales es la protección que el usuario debe tener para evitar que sus datos sean objeto de robo o mal uso"

CM (R) Dr. Ricardo Mato

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, Tecnología e Innovación Productiva de la Nación, administrada 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

INVITACIÓN IMPORTANTE

Informamos e invitamos a nuestros lectores a inscribirse en este importante seminario por web (Webinar) a desarrollarse entre el 03 y 24 de octubre del presente año. El tema tratado será "Ciberdefensa. ¿Cómo enfrentar este nuevo dominio militar?".

Pueden inscribirse activando el siguiente link.

https://www.tecnowebinars.com/webinar/26920/ciberdefensa-como-enfrentar-este-nuevo-dominio-militar-4-sesiones-y-1/alejandro-corletti

Ver detalles del programa al final del boletín

ESTRATEGIA

Informe

Las Operaciones en el ambiente de la Información.

En contraste con los sitios Web no interactivos en los que los usuarios se limitan a la visualización pasiva de la información que se les proporciona, un sitio Web 2.0 permite interactuar con otros usuarios o cambiar contenidos del sitio Web.

En la Web 2.0 se utilizan una serie de herramientas, entre las que se pueden destacar: los blogs, las redes sociales (*Facebook, Twitter, Hi5, Myspace, Instagram*, entre otras) donde cada usuario tiene una página en la cual publica contenidos y se comunica con otros. También existen redes sociales profesionales, dirigidas a establecer contactos dentro del mundo empresarial (*LinkedIn, Xing*...) y a su vez, entornos para almacenar en Internet, documentos (*Google Drive* y *OneDrive*), videos (Youtube), fotos (*Instagram*) presentaciones (*Slideshare*), etc. y compartirlos y visualizarlos cuando convenga.

Allí, cada individuo se convierte en un medio de comunicación en sí mismo que solo comparte lo que quiere y aquello con lo que está de acuerdo, las más de las veces sin detenerse a pensar, e incluso puede decidir aceptar, de manera consciente, determinadas informaciones para reafirmar sus propias opiniones y aceptar también con ello un lenguaje manipulado, ligado a las emociones, que crea, en consecuencia, una nueva realidad.

Gracias a Internet las noticias transitan sin filtro por la Web 2.0 y en forma casi potencial a su vez son transmitidas por más personas muchas de las cuales reenvían los artículos sin leerlos. Si bien la mayoría de las veces constituyen una herramienta útil también dentro de ese entorno de mensajes compartidos es donde aparecen historias inverosímiles y algo fantásticas - las denominadas "*fake news*" (noticias falsas) - promovidas generalmente desde una red de sitios de noticias inauténticas en las cuales puede haber mucho más que simples artículos con títulos exagerados que alimentan a los medios de comunicación social.

Muchos de esos sitios de noticias intencionalmente tratan de hacerlas pasar como reales, ya sea sin revelar su naturaleza satírica u ocultando detalles dentro de su sitio Web

Resulta entonces cada vez más arduo conocer qué es verdadero, falso o en qué medida algo es verdadero o falso. Los hechos objetivos verificables son menos relevantes, en la formación de la opinión pública, que la apelación a las emociones o las creencias personales (posverdad). La verdad - entendida como coincidencia entre una proposición y los hechos - solo tiene, a diferencia de la posverdad, una única presentación. El problema, ahora, no radica en que la verdad sea lo opuesto a la mentira, sino en que la opinión es elevada a la categoría de verdad.

Y es ese ambiente de la información, donde las redes sociales se unen con el ciberespacio, donde los seres humanos y los sistemas automatizados observan, orientan, deciden y actúan, el principal escenario de toma de decisiones.

Es allí, tanto en la paz, como en una crisis o en la guerra donde las Operaciones Cibernéticas y las Operaciones de Información se complementan, para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios mientras se protegen las propias.

Es en ese ambiente donde la información puede estar dirigida a informar o a desinformar[1]. Cuando es encaminada a desinformar y responde a una estrategia, la información es manipulada maliciosamente y utilizada como elemento competitivo y arma de guerra, para quebrar la cohesión del adversario e influir en su proceso de toma de decisiones. Aunque el objetivo final de la desinformación siempre es el mismo, sus instrumentos varían, así como el contenido de los mensajes emitidos, según sean los blancos elegidos.

Para Guillem Colom[2], "*cualquier actividad que pueda poseer una dimensión informativa, desde una declaración oficial o una noticia en un medio de comunicación de masas a un blog personal o un mensaje de Twitter, podrá ser utilizada para apoyar unas operaciones de información que buscarán influir en las percepciones culturales, ideológicas, históricas, científicas o filosóficas de los potenciales adversarios, neutrales y aliados*"[3].

Para MacFarquhar[4] "*Las características comunes de los mensajes de la desinformación son la dificultad de averiguar la exactitud de los hechos que tratan, la falta de equilibrio en la presentación de la información (se insiste más en las debilidades del oponente que en la información de los hechos) y la ausencia de credibilidad de las fuentes elegidas (se introducen con un "muchos dicen" o "se habla de", o se inventa un acontecimiento falso)*".

Como ejemplo de esa conjunción de lo cognitivo y lo automatizado, podría decirse que, en los momentos críticos de un país, como pueden ser las elecciones o los anuncios de un gobierno de grandes decisiones, se podría liberar gran cantidad de noticias falsas para afectar la opinión pública.

---

[1] Desinformar según el diccionario de la RAE, significa "*Dar información intencionadamente manipulada al servicio de ciertos fines*" o "*Dar información insuficiente u omitirla*".

[2] Colom, Guillem; Rusia y las operaciones de información; Disponible en: http://www.seguridadinternacional.es/?q=es/content/rusia-y-las-operaciones-de-informaci%C3%B3n

[3] Ibidem.

[4] MacFarquhar, Neil (2016), "A Powerful Russian Weapon: The Spread of False Stories", *New York Times*, 28/VIII/2016. Citado por: Mira Milosevich-Juaristi. El poder de la influencia rusa: la desinformación http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari7-2017-milosevichjuaristi-poder-influencia-rusa-desinformacion

Complementariamente, en el momento oportuno, también podrían lanzarse ataques distribuidos de denegación de servicio (DDoS) contra sitios web del gobierno para impedir que el público en general tenga acceso a la información correcta. Las personas podrían dejarse engañar por rumores y crear una turbulencia interna o incluso tomar acciones violentas.

La propaganda no es algo nuevo solo que hoy en día, Internet es un medio de comunicación que puede ser utilizado de manera abusiva para difundir mentiras y desinformación. Es por ello que las fuerzas armadas de muchos países también se han subido al carro de las redes sociales, especialmente para utilizarlas como herramienta de inteligencia y comunicación estratégica.

Las Operaciones de Información tampoco lo son, solo que en la actualidad han tomado un nuevo énfasis debido al uso de la energía electromagnética y operaciones cibernéticas y el uso de operaciones para manipular las percepciones de un adversario.

Esa mezcla de lo humano y lo automatizado, no sólo comprende a las operaciones cibernéticas, sino que también abarca a la guerra electrónica, al engaño militar, a las operaciones de seguridad y a las operaciones de apoyo a la información (ex operaciones psicológicas), al ataque físico y al ataque por red informática

Por todo ello, es necesario comprender que las Operaciones Cibernéticas y las Operaciones de Información son una realidad. La renovación o habilitación de esos conceptos es importante porque por mucho que se apliquen los avances tecnológicos a las capacidades militares existentes, su eficacia no mejora si se emplean según conceptos doctrinales obsoletos.

En la última década, varias capacidades relacionadas con la información han crecido en el mundo, lo cual revela el valor que se les asigna. Los cambios tecnológicos generalmente tardan en trasladarse a conceptos operativos. No resulta fácil ni rápido comprender el impacto de las nuevas tecnologías en la manera de hacer la guerra y, además, siempre existirá una resistencia al cambio de las personas e instituciones.

Estas operaciones no están definidas en la doctrina argentina, y es una necesidad hacerlo con premura.

El arma perfecta: guerra, sabotaje y miedo en la era cibernética

Un libro de David E. Sanger que seguramente va a despertar interés en el mundo de la cibernética

https://www.infobae.com/america/tecno/2019/09/11/el-arma-perfecta-que-vladimir-putin-ya-uso-contra-ucrania-y-amenaza-con-expandir-a-otros-paises/

CIBERSEGURIDAD

La Ciberseguridad en América Latina

El sitio web del espectador presenta los comentarios de Fabio Assolini, analista senior de seguridad en Kaspersky, la compañía global de seguridad informática, reveló los resultados de sus recientes investigaciones en la novena Cumbre de Ciberseguridad. Latinoamérica y comenta acerca de las malas prácticas.

https://www.elespectador.com/tecnologia/asi-esta-la-ciberseguridad-en-america-latina-articulo-878632

https://www.youtube.com/watch?v=VDoOTMHe32Y

https://www.ciberseguridadlatam.com/2019/08/29/kaspersky-registra-45-ataques-por-segundo-en-america-latina/

CIBERDEFENSA

Documento de Interés

La Internet de la Cosas y la Protección de Datos

Presentamos un informe preparado por el Dr. Oscar Ricardo Mato donde analiza ciertos aspectos a considerar con los nuevos dispositivos inteligentes que emplean Internet de la Cosas y como proteger los datos personales

http://www.cefadigital.edu.ar/handle/123456789/1248

Perú dio a conocer su Ley de Ciberdefensa

En sus Títulos contempla legislación referente a: (1) Las capacidades de ciberdefensa y las operaciones en y mediante el ciberespacio, (2) del uso de la fuerza en y mediante el ciberespacio, (3) de la seguridad de los activos críticos nacionales y recursos claves, y cuestiones orden general
https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

CIBERGUERRA

Gobierno y compañías privadas en conflicto por la seguridad de los usuarios

En un movimiento para proteger a sus usuarios con sede en Kazajstán de la vigilancia del gobierno, Google, Apple y Mozilla finalmente se presentaron y bloquearon el certificado raíz de CA (Certification Authority) emitido por el mismo dentro de sus respectivos softwares de navegación web.
https://thehackernews.com/2019/08/kazakhstan-root-certificate.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2053.po0ao0di5a.19ye

CIBERCONFIANZA

Informe

Google Zero y el hackeo de iPhone

Según confirma un informe de los investigadores del Proyecto Cero de Google, han descubrieron a principios de este año que su iPhone puede ser pirateado simplemente visitando un sitio web de aspecto inocente, al menos cinco cadenas de explotación de iPhone son capaces de liberar remotamente un iPhone e implantar spyware en él.

https://thehackernews.com/2019/08/hacking-iphone-ios-exploits.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2059.po0ao0di5a.1a3w

CIBERFORENSIA

iPhone bajo ataque

Una nueva carga útil de spyware altamente capaz puede monitorear todo en la vida digital de una persona. Catorce vulnerabilidades en iPhone han sido el objetivo de cinco cadenas de *exploits* (herramientas que unifican vulnerabilidades de seguridad, permitiendo al atacante penetrar en cada capa de las protecciones digitales de iOS). Estas cadenas forman parte de un ataque que ha durado años; dos de estas vulnerabilidades se trataban de *Zero Days*.

https://threatpost.com/iphone-zero-days-watering-hole-attacks/147891/

Windows corrige sus fallos de seguridad

Como suele ser frecuente ya en Microsoft, el segundo martes de cada mes se publica su paquete mensual de actualizaciones de seguridad, conocido por su nombre en inglés *«Patch Tuesday»*. Este mes Microsoft ha parcheado 93 fallos de seguridad y ha publicado dos avisos incluyendo mitigaciones para problemas relacionados con la seguridad que afectan a productos y servicios de su compañía

https://unaaldia.hispasec.com/2019/08/microsoft-en-su-martes-de-parches-de-agosto-corrige-93-fallos-de-seguridad.html

Nuevo ataque contra CPUs Intel

Investigadores de la universidad de *Vrije* de Amsterdan descubren una nueva vulnerabilidad en las CPUs de Intel, que puede ser explotada remotamente sin necesidad de acceso físico o malware instalado en la máquina objetivo.

Bautizada como *NetCAT* (*Network Cache ATtack*), esta vulnerabilidad permite a un atacante remoto averiguar información sensible a través de la cache de las CPUs de Intel.

La vulnerabilidad con identificador *CVE-2019-11184* se encuentra en una capacidad de estas CPUs llamada *DDIO* (*Data Direct I/O*), que por diseño permite a dispositivos y periféricos de una red acceder a la cache de dichas CPUs.

Esta capacidad está activada por defecto en todas las CPUs de Intel usadas en servidores, como son los procesadores de la familia Xeon E5, E7 y SP.

Según los investigadores, el ataque *NetCAT* funciona de forma similar a *Throwhammer*, en el sentido de que se envían paquetes de red especialmente diseñados a una máquina destino que tiene activado *RDMA* (*Remote Direct Memory Access*).

RDMA permite a un usuario malicioso espiar las acciones de aquellos dispositivos que hagan uso de esta tecnología, como puede ser una tarjeta de red. Esta técnica se consigue mediante la observación de las diferencias de tiempo entre un paquete de red que es ofrecido desde la cache de procesador y otro que es ofrecido desde la memoria.

La idea es llevar a cabo un análisis del tiempo de las pulsaciones realizadas por la víctima usando un algoritmo de inteligencia artificial. El equipo de *Vrije* logró una tasa de acierto del 85% en sus pruebas, en las que se recuperó una credencial SSH a través de la red.

Intel por su parte ha reconocido el problema y recomienda a los usuarios afectados desactivar *DDIO* o al menos *RDMA* para hacer este tipo de ataques más complicados. También se sugiere limitar el contacto de los servidores vulnerables con redes de poca confianza.

Más Información:

https://www.cs.vu.nl/~herbertb/download/papers/netcat_sp20.pdf

CIBERCRIMEN

Silence APT, un grupo cibercriminal de habla rusa, conocido por atacar organizaciones financieras principalmente en los antiguos estados soviéticos y países vecinos, ahora está atacando agresivamente a bancos en más de 30 países de América, Europa, África y Asia.

https://thehackernews.com/2019/08/silence-apt-russian-hackers.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2053.po0ao0di5a.19yk

Documentó de Interés

Acerca de Silence APT

Hace tres años, un joven y motivado grupo ciberdelincuente de habla rusa comenzó a atacar el sector financiero. Al principio, el Silence mostró signos de inmadurez en su TTP (siglas en ingles de proceso de Confianza) al cometer errores y prácticas copia de otros grupos. Ahora, Silence es uno de los actores de amenazas más activos, dirigido al sector financiero. Desde que lanzamos nuestro informe original, Silence: Moving into the lado oscuro, el daño confirmado de las operaciones de Silence se ha multiplicado por cinco en comparación con las cifras del informe inicial del Grupo IB.

https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf

NOVEDADES

Federalizar la vigilancia tecnológica

Entrevista a Nancy Pérez, la especialista estuvo a cargo de la capacitación en vigilancia tecnológica e inteligencia estratégica en el taller sobre *"Vigilancia Tecnológica e inteligencia estratégica",* la jornada fue organizada en el marco de las actividades que se desarrollan en pos del proyecto "Distrito de innovación tecnológica Paraná -Oro Verde-".

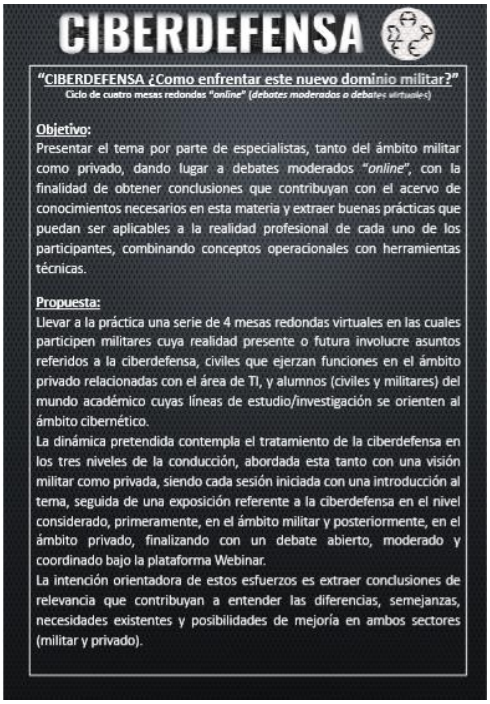
https://noticias.uner.edu.ar/entrevistas/7174/federalizar-el-conocimiento-mediante-el-trabajo-en-territorio

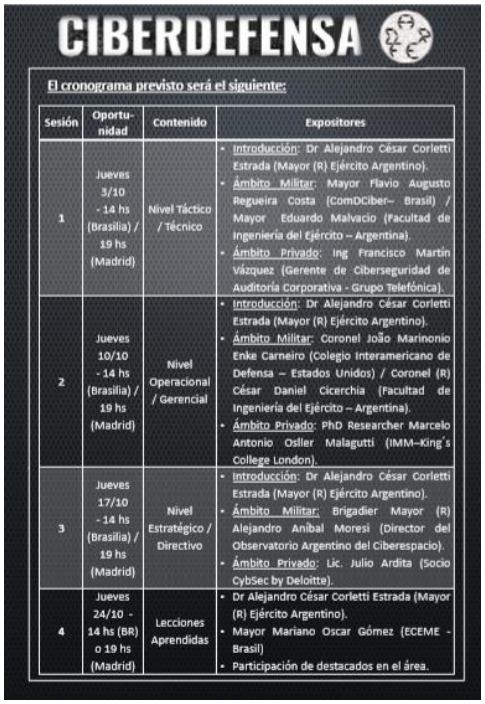
INVITACIÓN IMPORTANTE

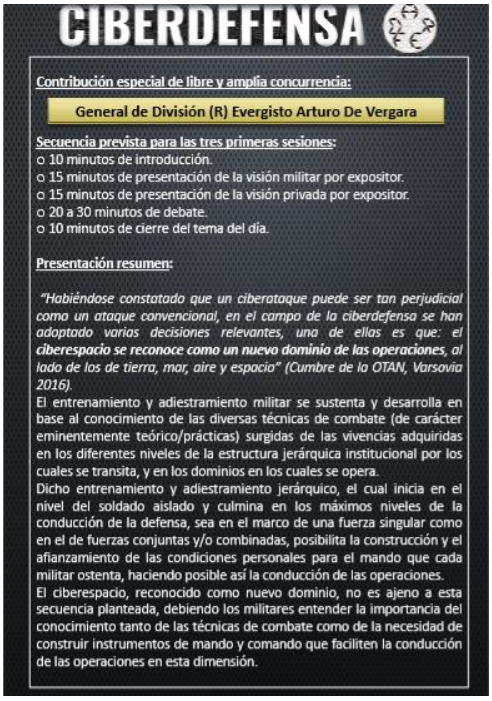
Informamos e invitamos a nuestros lectores a inscribirse en este importante seminario por web (Webinar) a desarrollarse entre el 03 y 24 de octubre del presente año. El tema tratado será “Ciberdefensa. ¿Cómo enfrentar este nuevo dominio militar?”.

Pueden inscribirse activando el siguiente link.

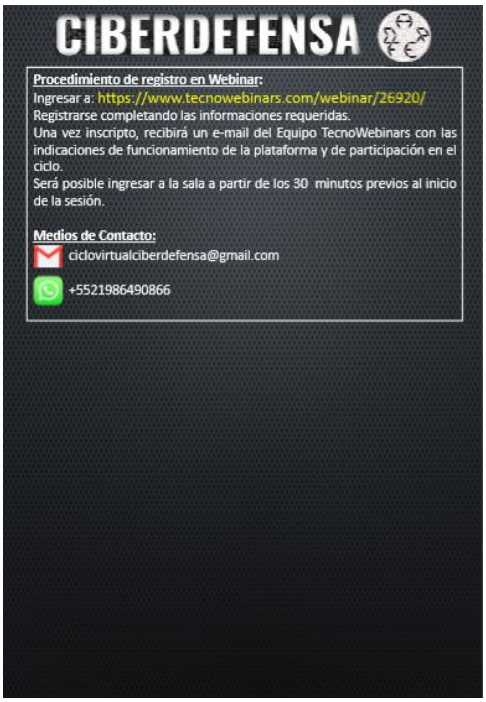
https://www.tecnowebinars.com/webinar/26920/ciberdefensa-como-enfrentar-este-nuevo-dominio-militar-4-sesiones-y-1/alejandro-corletti




CIBERDEFENSA
El cronograma previsto será el siguiente:
Sesión | Oportunidad | Contenido | Expositores
1 | Jueves 3/10 - 14 hs (Brasilia) / 19 hs (Madrid) | Nivel Táctico / Técnico | • Introducción: Dr Alejandro César Corletti Estrada (Mayor (R) Ejército Argentino). • Ámbito Militar: Mayor Flavio Augusto Regueira Costa (ComDCiber– Brasil) / Mayor Eduardo Malvacio (Facultad de Ingeniería del Ejército – Argentina). • Ámbito Privado: Ing Francisco Martín Vázquez (Gerente de Ciberseguridad de Auditoría Corporativa - Grupo Telefónica).
2 | Jueves 10/10 - 14 hs (Brasilia) / 19 hs (Madrid) | Nivel Operacional / Gerencial | • Introducción: Dr Alejandro César Corletti Estrada (Mayor (R) Ejército Argentino). • Ámbito Militar: Coronel João Marinonio Enke Carneiro (Colegio Interamericano de Defensa – Estados Unidos) / Coronel (R) César Daniel Cicerchia (Facultad de Ingeniería del Ejército – Argentina). • Ámbito Privado: PhD Researcher Marcelo Antonio Osller Malagutti (IMM–King´s College London).
3 | Jueves 17/10 - 14 hs (Brasilia) / 19 hs (Madrid) | Nivel Estratégico / Directivo | • Introducción: Dr Alejandro César Corletti Estrada (Mayor (R) Ejército Argentino). • Ámbito Militar: Brigadier Mayor (R) Alejandro Aníbal Moresi (Director del Observatorio Argentino del Ciberespacio). • Ámbito Privado: Lic. Julio Ardita (Socio CybSec by Deloitte).
4 | Jueves 24/10 - 14 hs (BR) o 19 hs (Madrid) | Lecciones Aprendidas | • Dr Alejandro César Corletti Estrada (Mayor (R) Ejército Argentino). • Mayor Mariano Oscar Gómez (ECEME - Brasil) • Participación de destacados en el área.


CIBERDEFENSA
Contribución especial de libre y amplia concurrencia:
General de División (R) Evergisto Arturo De Vergara
Secuencia prevista para las tres primeras sesiones:
o 10 minutos de introducción.
o 15 minutos de presentación de la visión militar por expositor.
o 15 minutos de presentación de la visión privada por expositor.
o 20 a 30 minutos de debate.
o 10 minutos de cierre del tema del día.
Presentación resumen:
"Habiéndose constatado que un ciberataque puede ser tan perjudicial como un ataque convencional, en el campo de la ciberdefensa se han adoptado varias decisiones relevantes, una de ellas es que: el ciberespacio se reconoce como un nuevo dominio de las operaciones, al lado de los de tierra, mar, aire y espacio" (Cumbre de la OTAN, Varsovia 2016).
El entrenamiento y adiestramiento militar se sustenta y desarrolla en base al conocimiento de las diversas técnicas de combate (de carácter eminentemente teórico/prácticas) surgidas de las vivencias adquiridas en los diferentes niveles de la estructura jerárquica institucional por los cuales se transita, y en los dominios en los cuales se opera.
Dicho entrenamiento y adiestramiento jerárquico, el cual inicia en el nivel del soldado aislado y culmina en los máximos niveles de la conducción de la defensa, sea en el marco de una fuerza singular como en el de fuerzas conjuntas y/o combinadas, posibilita la construcción y el afianzamiento de las condiciones personales para el mando que cada militar ostenta, haciendo posible así la conducción de las operaciones.
El ciberespacio, reconocido como nuevo dominio, no es ajeno a esta secuencia planteada, debiendo los militares entender la importancia del conocimiento tanto de las técnicas de combate como de la necesidad de construir instrumentos de mando y comando que faciliten la conducción de las operaciones en esta dimensión.


CIBERDEFENSA
Fechas y contenidos de los Webinar:
•Nivel Táctico / Técnico.
Jueves 03 de octubre – 14 horas (Brasilia) / 19 horas (Madrid)
Abordaje Militar | Abordaje Informático Privado
Ámbito (nivel) en el que se encuadra. Objetivo de la capacitación a este nivel. Metodología de formación/capacitación en este nivel. Técnicas principales empleadas. Diferentes escuelas o líneas de formación (referentes).
Ámbito (nivel) en el que se encuadra. Objetivo de la capacitación a este nivel. Técnicas principales empleadas. Herramientas y técnicas de hacking ético. Herramientas y técnicas de seguridad. Metodología de formación/capacitación, cursos, certificaciones.
•Nivel Operacional / Gerencial.
Jueves 10 de octubre – 14 horas (Brasilia) / 19 horas (Madrid)
Abordaje Militar | Abordaje Informático Privado
Inserción de la ciberdefensa en el proceso de planeamiento de nivel operacional. Influencia en el ciclo de reunión de información, inteligencia y contrainteligencia. Inserción de la ciberdefensa en el proceso de toma de decisiones.
Centros de supervisión y monitorización. Centros de respuesta a incidentes de seguridad (CSIRT). Centros de operación de seguridad (SOC). Plan de recuperación de desastres (DRP).
•Nivel Estratégico / Directivo.
Jueves 17 de octubre – 14 horas (Brasilia) / 19 horas (Madrid)
Abordaje Militar | Abordaje Informático Privado
Infraestructuras críticas como objetivos estratégicos. Análisis de escenarios / hipótesis de conflictos (genéricas). Articulación y conexión entre el área de ciberdefensa militar (defensa) y su equivalente en la estructura de seguridad interior del Estado.
Concepto de infraestructuras críticas. El CIO (Cheaf Information Officer) El CSO (Cheaf Security Officer) El DPO (Data Protection Officer)
•Lecciones Aprendidas.
Jueves 24 de octubre – 14 horas (Brasilia) / 19 horas (Madrid)
Conclusiones, evaluación de resultados y consideraciones finales. Experiencias adquiridas a lo largo del ciclo y desafíos futuros.


CIBERDEFENSA
Procedimiento de registro en Webinar:
Ingresar a: https://www.tecnowebinars.com/webinar/26920/
Registrarse completando las informaciones requeridas.
Una vez inscripto, recibirá un e-mail del Equipo TecnoWebinars con las indicaciones de funcionamiento de la plataforma y de participación en el ciclo.
Será posible ingresar a la sala a partir de los 30 minutos previos al inicio de la sesión.
Medios de Contacto:
ciclovirtualciberdefensa@gmail.com
+5521986490866