OAC Boletín de Mayo

"No comprender la importancia futura de los guerreros del ciberespacio (técnicos, especialistas, neurocientíficos, psiquiatras, psicólogos, pero por sobre todo estrategas), condenará a las fuerzas militares, que no se preparen para la guerra en las mentes de la sociedad. Lo que la infantería fue a Napoleón ("Reina de las Batallas") en el futuro serán los ciberguerreros a la conciencia del conflicto ("reyes de la guerra")

Alejandro Moresi
Observatorio Argentino del Ciberespacio

Contenidos Página

CIBERCONFIANZA

CIBERFORENSIA

NOTICIAS

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 es 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,** que administra el **Centro Tecnológico y Perspectiva 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

CIBERDEFENSA

Un reporte muy interesante de la segunda edición Internacional del Manual Tallin 2.0

El Tallin Manual 2.0 es la segunda edición del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN sobre el análisis y la aplicación del derecho internacional sobre el ciberespacio. El análisis se basa en la idea que las operaciones cibernéticas no se producen en un vacío legal, y las obligaciones preexistentes según el derecho internacional se aplican igualmente al dominio cibernético. Como tal, el Tallin Manual 2.0 se divide en cuatro partes con un total de veinte capítulos, cada uno examina un área diferente del derecho internacional existente. La primera sección trata sobre los principios legales generales, mientras que las últimas tres secciones abordan regímenes legales especializados específicos. De acuerdo con su premisa, el Tallin Manual 2.0 cita más de un siglo de tratados y jurisprudencia, extendiendo las premisas de los principios y regímenes de derecho internacional a sus aplicaciones en el ciberespacio.

https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations

CIBERGUERRA

Desinformación: concepto y perspectivas

Julia Alicia Olmo y Romero del CIBER Elcano, nos presenta este informe acerca de cómo la desinformación, cuando responde a una estrategia y objetivos de desestabilización, pone en riesgo los valores e instituciones democráticos, como los de la Unión Europea, ya erosionadas por conceptos como la posverdad, las *fake news* y la manipulación de las redes sociales.

http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari41-2019-olmoromero-desinformacion-concepto-y-perspectivas?utm_source=CIBERelcano&utm_medium=email&utm_campaign=43-abril2019

El Mapa de la Cibeguerra

El Mapa de CyberWar es una muy interesante guía visual de algunos de los jugadores y eventos más destacados en el conflicto cibernético de estado a estado creado como parte del Proyecto Ciber Vault del Archivo de Seguridad Nacional. Este recurso se centra en el pirateo y los ciberataques patrocinados por el estado. Al hacer clic en los elementos del mapa se producirán enlaces y descripciones de documentos relevantes para cada tema. Los elementos, las conexiones y los documentos se agregarán regularmente a esta ayuda de investigación en constante evolución.

Esta aplicación conforma una muy útil herramienta para seguir el estado del arte en la materia a nivel mundial.

https://embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38#apt-index/russia

Nueva área de la Guardia Nacional de los EEUU los Guerreros de fin de semana

La Guardia Nacional de los EE.UU, espera ser un colaborador para el talento tecnológico del Departamento de Defensa, encontrando trabajadores de tecnología cibernética a tiempo completo , convirtiéndolos en guerreros cibernéticos, dijo George Battistelli jefe de operaciones cibernéticas de la Guardia Nacional: "Se trata de asegurar que tengamos a las personas correctas y las personas capacitadas adecuadas".

https://defensesystems.com/articles/2019/04/10/guard-cyber-weekend-warriors.aspx?s=ds_250419&m=1

La posverdad (fake news)

A pesar de toda la información disponible, cada vez es más arduo conocer qué es verdadero, falso o en qué medida algo es verdadero o falso. La irrupción política, mediática y social de conceptos como posverdad, fake news y desinformación ha alcanzado a todos los países. La posverdad es la forma de describir aquellas circunstancias en las cuales los hechos objetivos verificables son menos relevantes, en la formación de la opinión pública, que la apelación a las emociones o las creencias personales. 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.

Distintos hechos ocurridos en las últimas elecciones en distintas partes del mundo deben alertarnos respecto de lo que podría llegar a ocurrir en las elecciones presidenciales de Argentina de 2019 que tendrán lugar el 27 de octubre de 2019 cuyos candidatos surgirán de elecciones primarias abiertas, simultáneas y obligatorias (PASO) a realizarse el domingo 11 de agosto 2019.

Seguramente a lo largo de la campaña los encuestadores, los partidos políticos, las organizaciones no gubernamentales y empresas de tecnología estarán vigilando las redes sociales, Facebook, Twitter, buscando indicios de manipulación maliciosa por distintos actores, nacionales e internacionales, que tienen un interés directo en el resultado del proceso electoral.

Esta manipulación, difícilmente trate de cambiar lo que la gente cree, sino que buscará modificar su forma de sentir. La ira y el miedo no son cosas que puedan corregirse con mejores hechos.

Cómo Whatsapps influyó en las elecciones brasileñas y ayudó a ganar a Jair Bolsonaro.

Según las encuestas realizadas unos días antes de la primera ronda de las elecciones presidenciales de Brasil de 2018, el 81 por ciento de los partidarios de Bolsonaro dijeron haber utilizado los medios de comunicación social, mientras que el 61 por ciento reportó el uso de WhatsApp para acceder a la información y el 40% afirmó que usó la plataforma para compartir información. Una encuesta realizada entre las dos rondas, mostró que el 47 por ciento de los encuestados afirmó utilizar WhatsApp para obtener noticias, información y un asombroso 87% de ellos afirmó haber recibido noticias falsas a través de la plataforma.

https://www.cfr.org/blog/whatsapps-influence-brazilian-election-and-how-it-helped-jair-bolsonaro-win

CIBERSEGURIDAD

Oferta de curso para hackers éticos

El sitio "the hackersnews.com" presenta un *paquete de Master Class de Ethical Hacker 2019* que ofrece preparación para los aspirantes a profesionales, con 10 cursos y más de 180 horas de video tutoriales.

https://thehackernews.com/2019/02/ethical-hacker-training.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.1975.po0ao0di5a.181q

Los piratas informáticos chinos usaron herramientas de piratería de la NSA

Según un nuevo informe publicado por la firma de ciberseguridad Symantec, un grupo vinculado a los chinos, al que llama Buckeye, estaba usando las herramientas de piratería vinculadas a la NSA desde marzo de 2016.
https://thehackernews.com/2019/05/buckeye-nsa-hacking-tools.html

La Inteligencia Artificial y la ética

Actualmente, las redes sociales se enfrentan a una grave crisis de confianza y la UE quiere asegurarse que la Inteligencia Articial (AI) no vaya en la misma dirección. Recientemente, la organización dio a conocer sus pautas de ética que están diseñadas para impactar el desarrollo de los sistemas de inteligencia artificial antes que estén integrados en la sociedad.

https://itmunch.com/eu-reveals-ethical-guidelines-for-artificial-intelligence/

CIBERCONFIANZA

Glosario Cibernético

Es un documento en línea, preparado por la National Security Archive de los EE.UU que contiene un glosario de términos empleados en las cuestiones cibernéticas.

https://nsarchive.gwu.edu/cyber-glossary-a

CIBERFORENSIA

Herramientas para análisis de dispositivos que emplean Internet de las Cosas (IoT)

Los dispositivos inteligentes son cada vez más comunes, pudiendo controlar desde un celular las luces de alguna habitación o cualquier otro objeto, para ello el mercado presenta una gran cantidad de opciones disponibles de este tipo de dispositivos que interactúan con tu teléfono móvil y/o la red de tu hogar.

Para ello deben estar bien configurados o bien el fabricante debe tener en consideración aspectos de seguridad suficientes, de lo contrario podrían ser vulnerables y exponer información personal o sensible. Esta publicación plantea un camino por donde comenzar el análisis de dispositivos IoT, explicando cuales son las vulnerabilidades más comunes y cómo encontrarlas.

https://www.welivesecurity.com/la-es/2019/03/14/herramientas-analizar-dispositivos-iot/

Facebook revela una falla de seguridad

A fines del mes pasado, Facebook reveló que almacenaba las contraseñas de multitud de usuarios de Facebook e Instagram en texto sin formato. No obstante, hace poco se actualizó el comunicado de prensa de marzo aumentando la cantidad de usuarios de Instagram afectados desde las decenas de miles iniciales hasta el orden de cientos de millones de usuarios. El almacenamiento de las contraseñas de estos usuarios de Facebook e Instagram en texto plano, son prácticamente de libre acceso para determinados ingenieros de la compañía.

https://thehackernews.com/2019/04/instagram-password-plaintext.html

NOTICIAS

Oportunidades Argentinas de frente al negocio de la Singularidad

El Dr. Uzal en dialogo con la Directora de Asuntos Globales de la Oficina de Gerenciamiento de la Tecnología Informática del Gobierno de Estonia, ofrece un breve reporte acerca de las posibilidades de nuestro país de cara a esta cuarta revolución industrial y la apertura de la era de la singularidad tecnológica

Singularidad Tecnológica – Tecnologías Exponenciales y Cuarta Revolución Industrial

Como actividad excursus, de la Maestría en Ciberdefensa y Ciberseguridad de la UBA, Singularidad Tecnológica, Tecnologías Exponenciales y Cuarta Revolución Industrial, fueron temas sobre los que intercambiaron opiniones, la semana pasada, alumnos graduados de la citada Maestría con Sandra Sarav, Directora de Asuntos Globales de la Oficina de Gerenciamiento de la Tecnología Informática del Gobierno de Estonia.

Se entiende por Singularidad Tecnológica al fenómeno que se verificará en el momento a partir del cual, los análisis más sensitivos y los procesos decisorios de mayor relevancia pasarán a ser incumbencia de la Inteligencia Artificial; los "decididores humanos", en el mejor de los casos, pasarán a cumplir roles complementarios o de "negociación" con la Inteligencia Artificial. Por otro lado, Tecnologías Exponenciales son aquellas a las que inversiones incrementales, según un esquema lineal, se corresponden con un retorno de la inversión exponencial (Inteligencia Artificial, Procesadores Cuánticos, Ingeniería Genética, Robótica, …). Estarán incluidos en la Cuarta Revolución Industrial aquellos países en los cuales, las mayores contribuciones a su Producto Bruto Interno provengan de las Tecnologías Exponenciales (las de mayor rentabilidad esperada).

El estilo de gobierno que posicionó a Estonia, en los temas citados, en una posición de privilegio global, constituye un verdadero desafío para nuestros líderes políticos, empresariales y sociales.

El liderazgo en Estonia de Toomas Henrik Ilves merece ser estudiado en detalle, Argentina puede y debe ingresar exitosamente en el contexto de la Cuarta Revolución Industrial en las próximas décadas. El mayor aporte esperado de nuestros líderes: Talento y creatividad. No lograrlo se corresponde con un retroceso relativo a una suerte de "Edad de Piedra Tecnológica" de nuestro país. El factor crítico de éxito esencial, disponibilidad de Recursos Humanos de alta calidad, es una precondición que se verifica en Argentina. La "toma de la batuta tecnológica" por parte de un Toomas Henrik Ilves argentino o de un Enrique Mosconi y/o un Manuel Nicolás Savio, pero de la Cuarta Revolución Industrial (no de la segunda) seguramente posicionarían a Argentina en las "ligas mayores", casualmente, en el medio ambiente de la Cuarta Revolución Industrial. Estonia lo logró en 20 años, con algo más de un millón de habitantes y sin contar con la estructura de enseñanza superior de Argentina.

El intercambio de opiniones con Sandra Sarav confirió un interesante sustento a las aseveraciones y propuestas de "Visión del Negocio de Argentina" contenidos en este breve aporte.

Ciudad Autónoma de Buenos Aires, 29 de abril de 2019 Dr. Roberto Uzal Director de la Maestría en Ciberdefensa y Ciberseguridad – UBA

La Escuela Nacional de Defensa Cibernética del Brasil, será base de formación para militares en el área de seguridad de datos

Con la misión de proteger las fronteras cibernéticas del Brasil, el Ejército Brasilero comenzó a instalar una Escuela Nacional de Defensa Cibernética (ENaDCiber)

https://www.defesa.tv.br/escola-nacional-de-defesa-cibernetica-sera-base-de-formacao-para-militares-na-area-de-seguranca-de-dados/#