OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya

ISSN: en trámite

AÑO 2 N° 13

http://www.esgcffaa.edu.ar/obsciber/

Junio 2019

OAC Boletín de Junio 2019

La Inteligencia Artificial (IA) no es una tecnología más o una actividad que afecte sólo al ámbito académico y científico. Es una tecnología crítica para la transformación y la economía digital, por lo que su disponibilidad o carencia afecta al bienestar, prosperidad e igualdad de la sociedad

Félix Arteaga y Andrés Ortega

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,** que administra el **Centro Tecnológico y Prospectiva 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

Operaciones de Desinformación y Guerra Psicológica

Un interesante aspecto de las estrategias hoy presentes en el ciberespacio es el artículo de Ariel Corbat en el diario La Prensa, el citado nos muestra las acciones de la llamada "Guerra Psicológica" muy empelada en la "Guerra Fría".

El ciberespacio da a estos conceptos plena vigencia hoy donde, a través de la información y las "fake news", se trata de ganar la mente de las personas y mantenerlas en un estado de duda permanente, porque la realidad ha mutado de ser lo que es a ser lo que la sociedad "cree que es".

El artículo cita: "*Hubo un intento de imponer como verdad -y contra toda evidencia- la fantasía morbosa de la desaparición forzada en el caso Maldonado*"

http://www.laprensa.com.ar/477212-Operaciones-de-accion-psicologica.note.aspx

Inteligencia Artificial un desafío ético para la defensa

Un punto de vista que no se puede desconocer sobre la Inteligencia Artificial y su empleo en armas de decisión autónoma y la posibilidad de afectar la vida humana

http://visionnacional.com/2019/05/inteligencia-artificial-y-defensa-si-o-no-el-planteo-moral/

Facebook dentro de la contienda electoral europea

En una entrevista exclusiva con RTÉ News, el CEO de Facebook Mark Zuckerberg dijo que "no podía garantizar que Facebook no se utilizaría por malos actores para interferencia electoral durante las elecciones europeas" a llevarse a cabo el 26 de mayo de 2019.

En su sede internacional cerca de Grand Canal Square, la compañía ha establecido un centro de operaciones de elecciones donde está monitoreando lo que está sucediendo en Facebook, Instagram y WhatsApp en relación con la elección. Este centro funcionó por primera vez el año pasado para las elecciones de Brasil y luego en las de medio término de los Estados Unidos. Pero esta es la primera vez que se ha establecido en Europa.

https://www.rte.ie/news/politics/2019/0505/1047320-inside-facebook-election-centre/

Facebook prohibió a una compañía israelí que realizó una campaña de influencia dirigida a interrumpir las elecciones en varios países y que canceló docenas de cuentas involucradas en difundir la desinformación. Nathaniel Gleicher, jefe de la política de seguridad cibernética de Facebook, dijo a los periodistas que el gigante de la tecnología había eliminado 65 cuentas israelíes, 161 páginas, docenas de grupos y cuatro cuentas de Instagram.

https://www.cbc.ca/news/technology/facebook-elections-1.5138796

La IA en la toma de decisiones

El Captain George Galdorisi, U.S. Navy (Retired), analiza en esta publicación la evolución en la velocidad de la toma de decisiones en el ambiente naval y en consecuencia el empleo de la IA para su apoyo

https://www.usni.or/magazinsroceedings/2019/nay/navy-needs-its-ejust-note-sertain-whi

Desarrollo y mantenimiento de software, un cambio de concepto en el ejército de los EE.UU.

Un aspecto crítico de los sistemas actuales es que gran parte de sus capacidades dependen del software que contienen, en la Argentina algunas instituciones ya tienen dentro de sus estrategias esenciales de obtención la de incorporar los códigos fuentes y la capacidad de mantenimiento del software como parte del proceso.

El Ejército de los EEUU está cambiando la forma de celebrar nuevos contratos con la industria para adquirir los derechos de propiedad intelectual del software, ya que los contratistas que desarrollan sistemas para el ellos, al poseer el código fuente y ante la necesidad de ejecutar una actualización urgente, el Ejército tiene que volver al contratista y a menudo pagar las mismas porque no tienen los derechos a la programación.

https://www.c4isrnet.com/it-networks/2019/05/24/3-big-changes-in-how-the-army-thinks-about-software/

Documento de Interés

Paper "Hacia un ecosistema español de Inteligencia Artificial: una propuesta·

En este informe sus autores, Félix Arteaga y Andrés Ortega pretenden contribuir a un debate verdaderamente "español", transversal, con propuestas para la construcción de un ecosistema español de IA en el que participen las administraciones públicas, las empresas, el mundo académico y la sociedad. También, se trata de engarzar ese ecosistema español con el ecosistema europeo y con el resto de los actores o ecosistemas internacionales.

http://www.realinstitutoelcano.org/wps/wcm/connect/abb7c1e1-8f16-46bf-adcf-554c42b2fb6e/Policy-Paper-2019-Hacia-ecosistema-espanol-Inteligencia-Artificial-una-propuesta.pdf?MOD=AJPERES&CACHEID=abb7c1e1-8f16-46bf-adcf-554c42b2fb6e

CIBERSEGURIDAD

Documento de Interés

Estrategia Nacional de Ciberseguridad de la República Argentina

La recientemente difundida Estrategia Nacional de Ciberseguridad de la República Argentina, es un documento acorde a su denominación, presenta una clara definición de la situación, donde entre otras cosas define el ciberespacio y establece las posturas nacionales respecto a la conducta a mantener por parte de nuestro país en el ciberespacio.

> Define al ciberespacio como: "*dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones"*
>
> Establece "*Internet representa un dominio global e intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía, poniendo a prueba el concepto antes mencionado e instaurando un nuevo paradigma que es necesario entender*"
>
> Presenta como Objetivos:
>
> - "*REPÚBLICA ARGENTINA promoverá en todos los foros en los que participe, el uso pacífico del Ciberespacio y apoyará toda iniciativa que tenga por fin la instauración de valores como la Justicia, el respeto al Derecho Internacional, el equilibrio y la disminución de la brecha digital entre las naciones, impulsando el diálogo y la cooperación. El Ciberespacio debe constituirse en un dominio en el que impere la paz, sustrayéndolo de posibles conflictos armados*".
> - *"Enfrentar los desafíos que se presentan requiere articular adecuadas capacidades de prevención, detección, análisis, investigación, recuperación, defensa y respuesta, que constituyen elementos esenciales para alcanzar todos los beneficios que el uso seguro del Ciberespacio ofrece a nuestra Nación"*

Determina los "principios rectores de la ciberseguridad": (1) respeto por los derechos y libertades individuales, (2) liderazgo, construcción de capacidades y fortalecimiento federal (3) integración internacional, (4) cultura de ciberseguridad y responsabilidad compartida, (5) fortalecimiento del desarrollo socioeconómico. Todos aspectos completamente afines con los principios y cuestiones que la Unión Internacional de Telecomunicaciones (ITU), plantea como esenciales para la creación de la "*Ciberconfianza*"

Establece los objetivos de la Estrategia Nacional de Ciberseguridad: (1) "Concientización del uso seguro del Ciberespacio", (2) "Capacitación y educación en el uso seguro del Ciberespacio", (3) "Desarrollo del marco normativo". (4) "Fortalecimiento de capacidades de prevención, detección y respuesta", (5) "Protección y recuperación de los sistemas de información del Sector Público", (6) "Fomento de la industria de la ciberseguridad". (7) "Cooperación Internacional", (8) "Protección de las Infraestructuras Críticas Nacionales de Información", determinando que es necesario para cada uno de ellos.

En síntesis, un documento conciso con conceptos concretos, que abarca casi todos los aspectos que el ciberespacio reclama desde la cultura y la integración, hasta los relativo a defensa y seguridad de la información.

Es opinión de esta publicación que quizás hubiere sido deseable que este documento planteara de alguna forma de estrategia de la información con las temáticas propias de la guerra de la información y la desinformación, una batalla que se desenvuelve en la mente de la gente y que es propia de este ambiente y este siglo.

https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528

Código de Derecho de la Ciberseguridad de España

El vínculo siguiente se refiere a la versión actualizada al 12 de junio de 2019
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiP8_CYnIXjAhUCJrkGHYKRCOgQFjAAegQIABAB&url=https%3A%2F%2Fwww.boe.es%2Flegislacion%2Fcodigos%2Fcodigo.php%3Fid%3D173_Codigo_de_Derecho_de_la_Ciberseguridad%26modo%3D1&usg=AOvVaw2bQ0TWBnA2OF7KHI0XKunq

CIBERDEFENSA

Geopolítica de la Información

La información es una de las fuentes de poder del siglo XXI y la desinformación es la forma de desarticular ese poder, las cuatro facetas clave del poder de la información:

1) Influir en el entorno político y económico de otros actores;
2) Crear crecimiento económico y riqueza;
3) Permitir una ventaja en la toma de decisiones sobre los competidores
4) Comunicarse de forma rápida y segura,

Son estos los campos de batalla en los cuales la geopolítica de la información se va a debatir para ganar o confundir las mentes de las personas, ello bajo la creencia por parte de algunos estados que la competencia estratégica en el siglo XXI se caracteriza por un concurso de suma cero para el control de datos, así como la tecnología y el talento necesarios para convertir los datos en información útil

https://www.belfercenter.org/publication/geopolitics-information

La sociedad de la desinformación: propaganda, «fake news» y la nueva geopolítica de la información

Ángel Badillo Matos, para Ciberelcano presenta, a la desinformación como un asunto de relevancia pública debido al empleo de información y desinformación en función de los intereses geoestratégicos de ciertos países y los efectos que producen en los ciudadanos.

Presenta un debate acerca de la naturaleza de las redes digitales empleada para difundir información y para atacar robando, desvirtuando o modificación de los datos; el uso de las redes sociales y la personalización de la información suponen nuevas formas de ruptura de la esfera pública, donde el ciudadano desprevenido o no preparado consume información digital sin conocimiento claro de esta nueva forma de comunicación poco tradicional. El artículo presenta iniciativas europeas sobre

desinformación, un modelo de análisis de la situación y el refuerzo de la acción coordinada europea desde España

http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion?utm_source=CIBERelcano&utm_medium=email&utm_campaign=44-mayo2019

CIBERGUERRA

La cultura en la Guerra Cibernética

Brandi Vincent de NexGov, explica las iniciativas del Gobierno de los EE.UU., para incrementar la fuerza laboral en cibernética, echando mano a la academia y las agencias federales con el objeto de disminuir la brecha entre los requerimientos de RR.HH. y la falta de los mismos, un tema también tratado en nuestra estrategia de ciberseguridad.

https://www.defenseone.com/ideas/2019/05/trump-signs-executive-order-boost-federal-cyber-workforce/156740/?oref=d1-related-article

CIBERCONFIANZA

Tecnología 5G la línea de Tiempo de Huawei en la Unión Europea

La preocupación por la seguridad cibernética y la participación de la compañía china Huawei en el despliegue de 5G en todo el mundo, son discusiones muy fuertes no sólo en el aspecto económico sino también en el campo de la seguridad.

Una línea de tiempo preparada por Carnegie Endowment, muestra los últimos cinco años con más de 100 eventos relacionados con Huawei y 5G en los estados miembros de la UE y la OTAN, así como en Australia, Japón, Nueva Zelanda, Filipinas y Corea del Sur, en el período comprendido entre febrero de 2015 y mayo de 2019.

https://carnegieendowment.org/publications/interactive/huawei-timeline

CIBERFORENSIA

Como bloquear cookies en Firefox

Las cookies se almacenan en su computadora por los sitios web que visita y contienen información como las preferencias del sitio o su estado de inicio de sesión. Este artículo describe cómo habilitar y deshabilitar las cookies en Firefox.

https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

CIBERCRIMEN

Los restaurantes también son objeto de malware

La cadena de restaurantes «Checkers» y «Rally's» ha descubierto en los últimos días que han accedido a los datos de tarjetas de crédito de sus clientes que almacenaban en sus puntos de venta. Por el momento no se conoce la forma en la que los atacantes consiguieron instalar el software malicioso en los puntos de venta de los restaurantes. Uno de estos puntos de venta ha estado infectado por el malware desde diciembre de 2015, y ha estado capturando datos de tarjetas de crédito hasta marzo de 2018.

https://thehackernews.com/2019/05/credit-card-checkers-restaurants.html

NOVEDADES

Estados Unidos lanzó un ataque cibernético a los sistemas de armas de Irán

Estaba dirigido a los sistemas de armas utilizados por el Cuerpo de la Guardia Revolucionaria Islámica de Irán (IRGC), que derribó el avión no tripulado de EE. UU. El jueves pasado y que, según los Estados Unidos, también atacó a los petroleros.
Tanto el Washington Post como la agencia de noticias AP dijeron que el ataque cibernético había deshabilitado los sistemas. El New York Times dijo que tenía la intención de desconectar los sistemas por un período de tiempo.

Christopher Krebs, el director de la Agencia de Seguridad de la Ciberseguridad y la Infraestructura, dijo además que la "ciberactividad maliciosa" estaba dirigida a las industrias estadounidenses y a las agencias gubernamentales por "actores del régimen iraní y sus representantes".

https://www.bbc.com/news/world-us-canada-48735097

https:// www.rt.com/news/462486-us-cyber-attack-iran/

Se realizó el primer seminario sobre la Ciberdefensa en la República Argentina

El Jefe del Estado Mayor Conjunto de las Fuerzas Armadas Teniente General VGM Bari del Valle SOSA presidió la ceremonia del cierre del "Primer Seminario sobre la Ciberdefensa en la República Argentina", que tuvo lugar el 06 y 07 de junio en la Escuela Superior de Guerra Conjunta.

El evento fue organizado por el Comando Conjunto de Ciberdefensa y tuvo por finalidad conocer el estado en que se encuentra la Ciberdefensa en nuestro país, a partir de una

aproximación multidisciplinar con distintos ejes temáticos, expuestos por prestigiosas y reconocidas personalidades del ámbito científico, político, académico y jurídico.

"El Estado Mayor Conjunto, a través del Comando Conjunto de Ciberdefensa, se ha propuesto alcanzar sus objetivos de integración no solo en el ámbito nacional sino trabajando de manera intensa con los países de la región, desarrollando ejercicios de simulación e intercambiando valiosas experiencias, de manera de reducir la incertidumbre propia de la naturaleza de este conflicto", sostuvo el Teniente General SOSA.

El desarrollo de este Seminario contó con la participación de diversos profesionales del área como es el caso del Dr. Luis KUN, Profesor Distinguido Emérito del *Center for Hemispheric Defense Studies* (CHDS), de la *National Defense University* (NDU); del Doctor Mariano BARTOLOMÉ, reconocido académico que se especializa en temas de seguridad ciudadana e Internacional, de defensa, Inteligencia y Política Internacional Contemporánea y Geopolítica; del Doctor Horacio JAUNARENA, ex Ministro de Defensa; del Ingeniero Alfredo Raúl PARODI, actual Subsecretario de Ciberdefensa del Ministerio de Defensa y del Ingeniero Pablo LÁZARO, actual Director de Investigaciones del Ciberdelito de la Dirección Nacional de Investigaciones, del Ministerio de Seguridad de la Nación.

El evento tuvo una alta convocatoria que se reflejó con la asistencia de representantes de distintas carteras de gobierno como el Ministerio de Relaciones Exteriores y Culto, Ministerio de Seguridad, Secretaría de Modernización como así también miembros de las tres Fuerzas Armadas y de las Fuerzas de Seguridad.

El Ministerio de Defensa estuvo representado por el Secretario de Investigación, Política Industrial y Producción para la Defensa, Ingeniero Luis RIVA, de quien depende la Subsecretaría de Ciberdefensa.