BOLETIN OAC SEPTIEMBRE 2018

"El ciberespacio, no es pasible de soberanía, es un ambiente que más allá de las definiciones radica en la mente del ser humano, de allá que su infinitud supere largamente la del espacio exterior, por ende el pensar en soberanía del ciberespacio es una entelequia , como la de creer que se puede manejar la voluntad de la humanidad "

Alejandro Moresi

Contenidos

CIBERDEFENSA

- Inteligencia Artificial y Seguridad Nacional Golpes a Infraestructuras Críticas en los EE.UU

CIBERGUERRA

- Coerción y ciberespacio

CIBERSEGURIDAD

- Ciberseguridad, una cuestión de Estados
- Una nueva versión de malware Backswap ataca ahora a la banca española Google rastrea secretamente lo que compra con la conexión con los datos de Mastercard
- Cómo verificar si su cuenta de Twitter ha sido pirateada

CIBERCONFIANZA

- Buenas Prácticas en Redes Sociales

CIBERCRIMEN

- Internet Crime Report (IC3) 2107

PUBLICACIÓN DE TRABAJO FINAL DE MAESTRÍA

- La defensa nacional y la estrategia militar de seguridad cibernética (Baretto, Juan Fernando)

CIBERDEFENSA

Documento de Interés

Inteligencia Artificial y Seguridad Nacional

Sistemas parcialmente autónomos e inteligentes han sido utilizados en el ejército desde la Segunda Guerra Mundial, pero los avances en el aprendizaje de los sistemas digitales (learning machine) e Inteligencia Artificial (AI) representan un punto de inflexión en el uso de la automatización aplicada a la guerra.

Las FFAA de los EE.UU. y las comunidades de inteligencia están planeando expandir el uso de la IA, muchas de las aplicaciones más transformadoras de la IA todavía no han llegado a su madurez.
En este documento los autores, Gregory C. Allen (MPP/MBA graduado en el Harvard Kennedy School of Government y el Harvard Business School - Investigador de política de IA, robótica, cohetería y tecnología y becario en el programa de Tecnología y Seguridad Nacional del Centro para una Nueva Seguridad Estadounidense) y Taniel Chan (MPP/MBA graduado en el Harvard Kennedy School of Government y el Harvard Business School), proponen tres objetivos para desarrollar una política futura sobre la IA y la Seguridad Nacional:

1. Preservar el liderazgo tecnológico de los EE. UU.,
2. Uso pacífico y comercial,
3. Mitigación del riesgo catastrófico.

Han tomado como base de lecciones aprendidas y producir recomendaciones para la política de seguridad nacional hacia la IA, cuatro casos anteriores de tecnología militar transformadora: la nuclear, la aeroespacial, la cibernética y la biotecnológica.

https://www belfercenter org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

– – –

Golpes a Infraestructuras Críticas en los EE.UU

El Departamento de Transporte de los Estados Unidos comenzó con una campaña de búsqueda de errores que descubrió vulnerabilidades inesperadas en los sistemas informáticos de la sede central. Los ataques fueron de bajo grado y no estaban enfocados, lo suficiente como para interrumpir el trabajo de algunos miembros del personal, pero no para interrumpir la red en general

https://www.nextgov.com/cybersecurity/2018/09/ransomware-strikes-launched-cyber-cleansing-program-transportation/151092/

CIBERGUERRA

Coerción y ciberespacio

Compartimos un artículo, del "CIBER Elcano" No.36 del Real Instituto Elcano. Septiembre de 2018, donde el Sr. Miguel Alberto Gomez se proporciona una visión general de los factores cruciales en nuestra comprensión de las operaciones cibernéticas coercitivas como el ejercicio del poder a través del ciberespacio con el fin de coaccionar a un adversario en un curso de acción particular. Está enfocado en las acciones compelentes de los actores estatales, aunque ellos y los actores no estatales también pueden llevar a cabo acciones disuasivas. La primera sección presenta los fundamentos de la coacción. El segundo encuadra la coacción en el contexto del ciberespacio y muestra las características del dominio que lo habilita. Finalmente, el tercero establece las causas del fracaso coercitivo e, inversamente, el éxito.

http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari102-2018-gomez-coercion-cyberspace?utm_source=CIBERelcano&utm_medium=email&utm_campaign=36-september2018&_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-c72ddabb9af8e711812870106fa6f4a1-f2e3abd9583f42738b003cee751f3c8d&esid=19c2bf1c-c0b5-e811-a966-000d3a233b72&urlid=11

CIBERSEGURIDAD

Ciberseguridad, una cuestión de Estados-Una forma de Guerra Híbrida

Centramos nuestra actividad digital en dispositivos, plataformas o aplicaciones cuya seguridad es casi nula, bien por negligencia o bien por presiones de los Estados para que las vulnerabilidades se mantengan hasta que el debate sobre las campañas de desinformación se constituyó en una forma de guerra híbrida (acciones combinadas de robo de información, filtración interesada y ciberpropaganda), y saltó a las primeras páginas de los medios de comunicación, el principal riesgo en el ciberespacio parecían ser los delincuentes informáticos. A esta conclusión era fácil llegar teniendo en cuenta que la primera fuente de información en este ámbito, para el público en general, la constituyen las noticias sobre incidentes recogidas por los medios, que tienden a poner el foco en hechos relacionados con el cibercrimen.

https://www.politicaexterior.com/articulos/politica-exterior/ciberseguridad-una-cuestion-estados/

– – –

Una nueva versión de malware Backswap ataca ahora a la banca española

BackSwap, una variante de Tinba, un pequeño (10-50kB) pero sofisticado troyano bancario que implementa algoritmos de generación de dominios (para la comunicación con el C&C), captura de credenciales de usuario desde formularios o la inyección en diferentes procesos.

https://unaaldia.hispasec.com/search?q=Backswap+ataca+ahora+a+la+banca+espa%C3%B1ola

– – –

Google rastrea secretamente lo que compra sin conexión con los datos de Mastercard

Más de una semana después de que Google admitiera que la compañía rastrea la ubicación de los usuarios incluso después de que deshabiliten el historial de ubicaciones, ahora se ha revelado que el gigante tecnológico firmó un acuerdo secreto con Mastercard que le permite rastrear lo que los usuarios compran fuera de línea.

https://thehackernews.com/2018/09/google-mastercard-advertising.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1823.po0ao0di5a.148i

– – –

Cómo verificar si su cuenta de Twitter ha sido pirateada

¿Te has preguntado alguna vez si tu cuenta de Twitter ha sido pirateada, quién ha logrado acceder y cuándo sucedió? Twitter ahora te permite saber esto. Después de Google y Facebook, ahora, Twitter te permite ver todos los dispositivos (computadora portátil, teléfono, tableta y demás) conectados a tu cuenta de Twitter. Twitter lanzó recientemente una nueva característica de seguridad para sus usuarios, denominada Aplicaciones y Sesiones, que le permite saber qué aplicaciones y dispositivos acceden a su cuenta de Twitter, junto con la ubicación de esos dispositivos.

https://thehackernews.com/2018/09/twitter-account-hacked.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1829.po0ao0di5a.14do

---

CIBERCONFIANZA

Documento de Interés

Buenas Prácticas en Redes Sociales

Con todo, no es solo a nivel cuantitativo que los seres humanos han pasado a “habitar” el ciberespacio, sino que el ciberespacio es un territorio virtual donde los humanos “hacen vida”: interactúan, se comunican, realizan intercambios sociales, comerciales, políticos o religiosos y, en definitiva, acaban “siendo y estando”.
El ciberespacio es un dominio de intercambios sociales que está creciendo exponencialmente cada año y que se ha establecido como un territorio propio en el que individuos, colectivos, empresas e instituciones llevan a cabo actividades, se estima que habrá 50 mil millones de objetos conectados a Internet de las Cosas (IoT), interactuando con las personas a través de sus identidades digitales.

https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3009-ccn-cert-bp-08-redes-sociales/file.html?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-c72ddabb9af8e711812870106fa6f4a1-f2e3abd9583f42738b003cee751f3c8d&esid=19c2bf1c-c0b5-e811-a966-000d3a233b72&urlid=15

CIBERCRIMEN

Documento de Interés

Internet Crime Report (IC3) 2107

El IC3 (Internet Crime Complaint Center) del FBI proporciona al público un mecanismo de información confiable y conveniente para enviar información sobre actividades sospechosas de actividades delictivas tramitadas por Internet.

Previene sobre los avances en ciberdelincuencia y cómo hacer frente a las ciberamenazas persistentes y cambiantes que enfrentamos.

El Informe sobre crímenes en Internet de 2017 enfatiza los esfuerzos del IC3 para monitorear estafas vía Business email compromise (BEC), Ransomware, Fraude de soporte técnico y Extorsión.

El informe presenta historias de éxito a partir de quejas de IC3 y la Iniciativa Operation Wellspring (OWS) investigación cibernética mediante la utilización una Cyber Task Force, fortaleciendo así la colaboración de las fuerzas del orden público a nivel estatal y local.

https://pdf.ic3.gov/2017_ic3report.pdf

PUBLICACIÓN DE TRABAJO FINAL DE MAESTRÍA EN ESTRATEGIA MILITAR
Escuela Superior de Guerra Conjunta

Título: La defensa nacional y la estrategia militar de seguridad cibernética Autor: Juan Fernando Baretto
Director de Tesis: Evergisto de Vergara
Palabras clave: Ciberdefensa, Ciberseguridad, Estrategia
Fecha de publicación: sep-2018

Citación :
Baretto, J. F. (2018). La defensa nacional y la estrategia militar de seguridad cibernética. (Trabajo Final de Maestría). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Ciudad Autónoma de Buenos Aires, Argentina.

Resumen:
La digitalización de las estructuras públicas y privadas de un estado y su integración en red, potencian y facilitan su operación y desarrollo eficiente. Este proceso y sus características generan un nuevo ámbito con naturaleza, propósito y conducta únicos

Sin embargo, existen vulnerabilidades de seguridad que pueden afectar su operación. Las estrategias de seguridad nacional de los EEUU, del Reino Unido, de Francia, España, Brasil y otros estados, han abordado los desafíos planteados, destacando la importancia del problema. Producto de ellas, muchos estados han creado agencias de ciberseguridad y ciberdefensa para proteger sus redes y datos. Otros han ido más allá y desarrollaron capacidades cibernéticas para atacar sistemas de computación en otros países. Existe un consenso general respecto a que la ciberguerra y todo lo asociado a ella, revolucionará el mundo del mismo modo en que lo hizo el advenimiento de la aviación, a comienzos del siglo XX. Si bien el Estado Argentino conoce los riesgos existentes, ha abordado lentamente sus implicaciones legales y técnicas. La falta de políticas y estrategias específicas y de una integración plena entre las agencias especializadas en el tema, limitan un avance real. Este trabajo se centrará en estudios de casos específicos de los países que se encuentran a la vanguardia del tema, el análisis de los marcos jurídicos nacionales e internacionales existentes, la opinión de los expertos en la materia y la explotación de encuestas entre usuarios y administradores de redes militares nacionales. El objetivo principal de este trabajo es sensibilizar al lector sobre este problema, al mismo tiempo que contribuye a identificar las vulnerabilidades de los sistemas informáticos militares argentinos y propone los conceptos básicos para desarrollar una estrategia militar de ciberdefensa, que puede servir como base para llevar a cabo acciones a corto y mediano plazo.
Descripción: Trabajo Final de Maestría
Aparece en las colecciones: Trabajos Finales de Maestría (TM)

http://www.cefadigital.edu.ar/bitstream/123456789/1061/1/TFM%2004-2018%20BARETTO.pdf