



# 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 4 N° 36

Julio 2021

## OAC Boletín de Julio 2021

*“La guerra tradicional se centra en la eliminación del enemigo, y la defensa nacional se centra en proteger al propio público”*

### Tabla de Contenidos

<b>ESTRATEGIA</b>	<b>2</b>
¿Dirigirán los niños en el ciberespacio?	2
La legítima defensa del Estado frente a ataques cibernéticos según el Derecho internacional	2
<b>CIBERSEGURIDAD</b>	<b>3</b>
¿QUÉ HARÁ REALMENTE LA NUEVA CIBERFUERZA BRITÁNICA?	3
<b>CIBERDEFENSA</b>	<b>3</b>
Un ciberataque golpea al Gobierno de Estados Unidos	3
<b>CIBERGUERRA</b>	<b>3</b>
Los Hackers Militares en EE.UU:	3
<b>CIBERCONFIANZA</b>	<b>4</b>
TikTok recopilará información biométrica en los EEUU	4
Informes Semanales	4
El malware Emotet se destruye en todas las computadoras infectadas del mundo	4
<b>CIBERFORENSIA</b>	<b>4</b>
Los dispositivos de Amazon compartirán WiFi con otros desconocidos	4
<b>CIBERDELITO</b>	<b>5</b>
NOVELA GRÁFICA DE LA SERIE RESILIENCE: BUG BYTES	5
<b>NOVEDADES</b>	<b>5</b>
PARA TENER EN CUENTA	5



**El Observatorio Argentino del Ciberespacio (OAC), micro-sitio de la Escuela Superior de Guerra Conjunta de la Facultad Militar 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 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 ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

**Hemos incluido en la sección NOTICIAS, una serie de posibilidades de participación en webinars y seminarios, especialmente destinados a la actualización sobre 5G.**

## **ESTRATEGIA**

### **¿Dirigirán los niños en el ciberespacio?**

La educación y la capacitación cibernéticas no deben comenzar en la universidad, ni en la escuela secundaria, ni en la escuela intermedia, ni en la escuela primaria, sino en casa tan pronto como los niños puedan ver o usar las redes sociales, dicen algunos expertos. Esta formación es importante no solo para sentar las bases para los futuros profesionales de la ciberseguridad en un campo hambriento de experiencia, sino también para inculcar buenos hábitos de higiene cibernética que puedan transmitirse a otros miembros de la familia.

[https://www.afcea.org/content/shall-children-lead-cyberspace?utm\\_source=Informz&utm\\_medium=Email&utm\\_campaign=Informz%20Email&\\_zs=plIVg1&\\_zl=cbVg7#](https://www.afcea.org/content/shall-children-lead-cyberspace?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=plIVg1&_zl=cbVg7#)

### **La legítima defensa del Estado frente a ataques cibernéticos según el Derecho internacional**

La posibilidad de legítima defensa por parte de los Estados frente a ciberataques es una cuestión de gran actualidad. En este artículo se trata de aclarar su marco jurídico dentro del derecho internacional público, realizando un análisis de los conceptos de uso de la fuerza y ataque armado concretados para el caso de los ciberataques, que son fundamentales para establecer cuando es lícita o no la reacción del Estado en legítima defensa. Se realiza también un análisis de las diferencias entre la legítima defensa anticipada y la legítima defensa preventiva, explicando por qué la defensa preventiva no es conforme a derecho, pese a que pudiera parecer útil dentro de la estrategia de ciberdefensa. Finalmente, se lleva a cabo una breve explicación del Manual de Tallin 2.0, documento que contiene una amplia recopilación de las normas que regulan este tema.



<https://global-strategy.org/la-legitima-defensa-del-estado-frente-a-ataques-ciberneticos-segun-el-derecho-internacional/>

---

## CIBERSEGURIDAD

### ¿QUÉ HARÁ REALMENTE LA NUEVA CIBERFUERZA BRITÁNICA?

¿Cómo resolverá el Reino Unido la tensión en el corazón de las operaciones cibernéticas?, caminando en la línea entre reconocer el ciberespacio como un dominio de conflicto y competencia y defender Internet como el lugar vibrante de gran parte de nuestra vida cotidiana? Para abordar esta tensión, el gobierno del Reino Unido ha invocado recientemente el concepto de un “poder cibernético democrático y responsable” para enmarcar sus aspiraciones cibernéticas, pero hasta ahora este concepto y cómo se ejecutará sólo se entienden en forma básica.

<https://warontherocks.com/2021/05/what-will-britains-new-cyber-force-actually-do>

[https://www.kaspersky.es/blog/hr-related-threats/24612/?mkt\\_tok=ODAyLUIkTi0yNDAAAF-EM23EFGZzuxd44ont84XoGDoL5Ld91cxKD-HPUuYCqlr4v-kFZvTTFT\\_i86wZkJibkgPR3u-hG2Pirb3QN3NJ9jzGwSwWuPRVCPHCwqtPw10Cu9OKv\\_I](https://www.kaspersky.es/blog/hr-related-threats/24612/?mkt_tok=ODAyLUIkTi0yNDAAAF-EM23EFGZzuxd44ont84XoGDoL5Ld91cxKD-HPUuYCqlr4v-kFZvTTFT_i86wZkJibkgPR3u-hG2Pirb3QN3NJ9jzGwSwWuPRVCPHCwqtPw10Cu9OKv_I)

---

## CIBERDEFENSA

### Un ciberataque golpea al Gobierno de Estados Unidos

Piratas informáticos vinculados al espionaje ruso se infiltraron en el sistema de correo electrónico utilizado por la Agencia de Ayuda Internacional (USAID, en inglés) del Departamento de Estado estadounidense para entrar en la red informática de grupos y organizaciones críticas con el Kremlin, según anunció ayer la compañía Microsoft. El ataque se produce a pocas semanas de la primera cumbre entre el presidente de EE UU, Joe Biden, y su homólogo ruso, Vladímir Putin, en Ginebra (Suiza) el 16 de junio.

<https://elpais.com/internacional/2021-05-28/un-ciberataque-de-origen-ruso-vuelve-a-golpear-al-gobierno-de-estados-unidos.html>

---

## CIBERGUERRA

### Los Hackers Militares en EE.UU:

La estrategia ofensiva Cyber Command estableció un nuevo precedente con una operación diseñada para deshabilitar o acabar con Trickbot, la botnet más grande del mundo, que se cree que está controlada por ciberdelincuentes rusos. Pareciera que los cibersoldados de los EEUU atacarán a los actores extranjeros, incluso a los que trabajen como delincuentes no estatales. Por otra parte AFCEA informa sobre el Ala 67 de la USAF (brazo Air Forces Cyber) realizó una campaña contra la guerra de información de Rusia durante el último año, respondió al compromiso de SolarWinds y ayudó a garantizar la seguridad digital de las elecciones de 2020

<https://www.wired.com/story/cyber-command-hackers-trickbot-botnet-precedent>

---



[https://www.afcea.org/content/cyber-gunslingers-defend-key-military-and-national-assets?utm\\_source=Informz&utm\\_medium=Email&utm\\_campaign=Informz%20Email&\\_zs=plIVg1&\\_zl=ebVg7#](https://www.afcea.org/content/cyber-gunslingers-defend-key-military-and-national-assets?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=plIVg1&_zl=ebVg7#)

---

## CIBERCONFIANZA

### TikTok recopilará información biométrica en los EEUU

TikTok, el popular servicio de intercambio de vídeos, ha revisado su política de privacidad en los EEUU. Estas nuevas condiciones permiten que se recopile automáticamente información biométrica, como por ejemplo reconocimiento facial y huellas vocales del contenido que sus usuarios publican en la plataforma. Por primera vez, los legisladores estadounidenses están lidiando con una plataforma importante que no se basa principalmente en los Estados Unidos y no se creó sobre la base de los ideales estadounidenses de libertad de expresión.

<https://unaaldia.hispasec.com/2021/06/tiktok-recopilara-informacion-biometrica-en-los-eeuu.html>

[https://www.cigionline.org/articles/why-doesnt-tiktok-get-policy-makers-attention/?utm\\_source=google\\_ads&utm\\_medium=grant&gclid=CjwKCAjwwqaGBhBKEiwAMk-FtJwXI\\_nLO-TQrKh35xKw0CW3I4XWWMG23bO-otxZOaSQzQO\\_fI4nQkxoCI2kQAvD\\_BwE](https://www.cigionline.org/articles/why-doesnt-tiktok-get-policy-makers-attention/?utm_source=google_ads&utm_medium=grant&gclid=CjwKCAjwwqaGBhBKEiwAMk-FtJwXI_nLO-TQrKh35xKw0CW3I4XWWMG23bO-otxZOaSQzQO_fI4nQkxoCI2kQAvD_BwE)

### 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 24 de mayo: <https://us-cert.cisa.gov/ncas/bulletins/sb21-151>

Semana del 31 de mayo: <https://us-cert.cisa.gov/ncas/bulletins/sb21-158>

Semana del 7 de Junio: <https://us-cert.cisa.gov/ncas/bulletins/sb21-165>

### El malware Emotet se destruye en todas las computadoras infectadas del mundo

Emotet, una de las redes de bots de spam de correo electrónico más peligrosas de la historia reciente, se está desinstalando hoy de todos los dispositivos infectados con la ayuda de un módulo de malware entregado en enero por las fuerzas del orden. La eliminación de la botnet es el resultado de una acción policial internacional que permitió a los investigadores tomar el control de los servidores de Emotet e interrumpir el funcionamiento del malware.

<https://www.bleepingcomputer.com/news/security/emotet-malware-nukes-itself-today-from-all-infected-computers-worldwide//>

---

## CIBERFORENSIA

### Los dispositivos de Amazon compartirán WiFi con otros desconocidos

En septiembre de 2019, Amazon anunció 'Sidewalk', una nueva funcionalidad que llegará a los dispositivos desarrollados por la empresa el próximo 8 de junio. El objetivo de Amazon es crear una red inalámbrica de largo alcance, con la que proporcionar conectividad a dispositivos que no dispongan de ella. El funcionamiento de esta red es similar al funcionamiento de 'Find my' disponible en dispositivos

---



Apple, que utilizan dispositivos de la marca cercanos para enviar a los servidores de Apple información de localización cifrada. De esta forma los dueños pueden recuperarlos si se han perdido.

<https://unaaldia.hispasec.com/2021/06/sidewalk-la-funcionalidad-con-la-que-tus-dispositivos-de-amazon-comparten-wifi-con-dispositivos-de-desconocidos.html>

---

## CIBERDELITO

### NOVELA GRÁFICA DE LA SERIE RESILIENCE: BUG BYTES

Los comics llegaron al ciberespacio, **Bug Bytes**, la segunda novela gráfica de la Serie Resilience de CISA, comunica los peligros y riesgos asociados con los actores que utilizan las redes sociales y otras plataformas de comunicación para difundir información errónea, desinformación y mala información (MDM) con el único propósito de sembrar dudas en el mundo. mentes de las audiencias objetivo para orientar su opinión. Los lectores siguen a la protagonista Ava, que usa su ingenio y habilidades periodísticas para descubrir una campaña de desinformación destinada a dañar la infraestructura de comunicaciones crítica 5G en los Estados Unidos.

<https://www.cisa.gov/publication/resilience-series-bug-bytes>

---

## NOVEDADES

### PARA TENER EN CUENTA

**“El coeficiente intelectual medio de la población mundial, que desde la posguerra hasta finales de los años 90 siempre había aumentado, en los últimos veinte años está disminuyendo”**

<https://www.lalinternaazul.info/2021/01/12/el-coeficiente-intelectual-medio-de-la-poblacion-mundial-esta-disminuyendo/>

---

Copyright ©

\* | 2021 | \*

\* | Escuela Superior de Guerra Conjunta | \*

Todos los derechos reservados.

\* | Observatorio Argentino del Ciberespacio | \*

Sitio web: <http://www.esgcffaa.edu.ar/esp/oac-boletines.php> Nuestra dirección postal es:

\* | Luis María Campos 480 - CABA - República Argentina |

\* Nuestro correo electrónico: \*

[|observatorioargentinelciberespacio@conjunta.undef.edu.ar |](mailto:observatorioargentinelciberespacio@conjunta.undef.edu.ar) \*