Estados Unidos apunta a la red eléctrica de Rusia en una guerra fría digital

Enviado por SilvanoHdz en Mar, 08/27/2019 - 12:14
Cita:

Sanger, David y Nicole Perlroth [2019], "Estados Unidos apunta a la red eléctrica de Rusia en una guerra fría digital",*The New York Times*, New York, 17 de junio, https://www.nytimes.com/es/2019/06/17/estados-unidos-red-electrica-rusia/ [1]

Fuente:
Artículo científico
Fecha de publicación:
Lunes, Junio 17, 2019
Revista descriptores:
Competencia mundial. Disputa hegemónica [2]
Formas de la guerra [3]
Relación economía y guerra [4]
Relaciones entre empresas estados y sociedad [5]
Sujetos de la guerra [6]
Tecnologías militares - tecnologías de uso dual [7]
Tema:
Ataques ciberneticos entre Estados Unidos y Rusia.
Idea principal:

Estados Unidos y Rusia se encuentran en medio de una nueva guerra fría, esta vez combaten a través del mundo digital. El gobierno ruso ha denunciado la existencia de un código informático estadounidense para sabotear la red eléctrica rusa. Funcionarios estadounidenses del Departamento de Seguridad Nacional y del Buró Federal de Investigaciones (FBI, por sus siglas en inglés), señalan que de igual forma, el gobierno de Rusia ha implementado un software malicioso que podría sabotear las plantas de energía eléctrica, los oleoductos y los gaseoductos, o los suministros de agua del país norteamericano.

Esta situación comenzó a intensificarse luego de la presencia de unidades de ciberataque y desinformación rusas en medio de las elecciones intermedias de 2018 en Estados Unidos. La Casa Blanca y el Congreso, aún mantienen en secreto las nuevas funciones que designaron en 2018 al Cibercomando de Estados Unidos (rama del Pentágono que se encarga de la seguridad cibernética del país). El 11 de junio de 2019, el asesor de seguridad nacional del presidente Donald Trump, John Bolton, aseguró que sus instituciones se encuentran trabajando para ampliar sus estrategias digitales. Mientras tanto, funcionarios estadounidenses, aseguran que esta nueva estrategia de seguridad nacional es preventiva pero también tiene una gran capacidad de ataque en caso de que se registre un enfrentamiento importante entre Moscú y Washington.

La decisión de introducirse en la red eléctrica de Rusia se tomó a partir de funciones legales poco conocidas, estas se especifican en el documento “Proyecto de ley de funciones del ejército” mismo que fue aprobado por el gobierno estadounidense a mediados del 2018. Con esta ley se vuelven legales las actividades militares clandestinas en el ciberespacio siempre y cuando estas acciones tengan el fin de disuadir ataques contra la nación estadounidense; así mismo, con este instrumento legal se otorga al Secretario de Defensa la capacidad de autorizar este tipo de actividades sin la necesidad de consultar al presidente.

Funcionarios de la seguridad nacional de Estados Unidos y el Pentágono, mencionaron a *The New York Times*, que no se habló a profundidad con el presidente Donald Trump respecto a las operaciones cibernéticas en Rusia. Esta decisión fue tomada como medida de cautela debido a que el presidente hubiera podido cancelarlas o hablar de ellas con funcionarios extranjeros, como lo hizo en 2017, cuando habló de una operación confidencial en Siria con el Ministerio de Relaciones Exteriores de Rusia. De cualquier forma, debido a que la nueva ley define las actividades militares cibernéticas como similares a la actividad militar en tierra, mar o aire, ya no es necesario que el presidente de Estados Unidos cuente con todos los detalles de dichas acciones. Mientras tanto, la mayoría de los datos sobre la irrupción digital del gobierno estadounidense en Rusia, se mantienen de manera confidencial.

La disputa actual entre Estados Unidos y Rusia lleva más de una década. Comenzó en 2008, después de que el gobierno ruso pudo infiltrarse en la red de comunicaciones clasificadas del Pentágono. Esta acción dio lugar a la creación del Cibercomando estadounidense, cuyas actividades se intensificaron durante el gobierno de Barack Obama. Cuando finalizó el primer periodo de mandato de Obama, los funcionarios del gobierno estadounidense descubrieron a un grupo de hackers rusos conocidos por los investigadores de seguridad privada como Energetic Bear (oso energético) o Dragonfly (libélula). En ese momento los trabajadores del gobierno suponían que este colectivo de expertos en cibernética no quería causar daño, pero en 2014, este grupo de ciberatacantes puso en peligro las actualizaciones del software que controlaba sistemas con acceso a los interruptores de energía. Después, cuando Trump llegó a la presidencia, los hackers rusos aumentaron sus ataques.

Con la llegada de Trump, el Cibercomando aumentó su defensa contra los atacantes de Rusia. Desean mantener la guardia arriba, pues esperan que los ciberatacantes rusos intenten provocar apagones en estados determinantes durante las elecciones del 2020. De tal manera, se espera que la estrategia de colocar el equivalente a minas terrestres en la red de energía de Rusia, sea un buen instrumento para disuadir al gobierno ruso.

Datos cruciales:

1. Desde 2012, Estados Unidos ha puesto sondas de reconocimiento en los sistemas de control de la red eléctrica de Rusia.

2. A principios de 2018 el Cibercomando de Estados Unidos culpó a Rusia de ser responsable del ciberataque más destructivo de la historia, mismo que paralizó a Ucrania y afectó a empresas estadounidenses como Merck y a FedEx.

3. En 2018, empresas de energía eléctrica de Estados Unidos y operadores de gas y petróleo de América del Norte, descubrieron que los mismos hackers que en 2017 desmontaron el sistema

de seguridad de Petro Rabigh, habían analizado su sistema operacional.

Nexo con el tema que estudiamos:

Este artículo ofrece información sobre el conflicto actual entre Rusia y Estados Unidos. Explica la importancia del mundo virtual en los conflictos entre naciones. De esta manera, expone nuevas formas de la guerra y los comienzos de un conflicto que tiene mucho por venir.

Proyecto de ley de funciones del ejército_Estados Unidos.pdf [8]

Links
[1] https://www.nytimes.com/es/2019/06/17/estados-unidos-red-electrica-rusia/
[2] http://let.iiec.unam.mx/taxonomy/term/12
[3] http://let.iiec.unam.mx/descriptores-let/formas-de-la-guerra
[4] http://let.iiec.unam.mx/descriptores-let/relaci%C3%B3n-econom%C3%ADa-y-guerra
[5] http://let.iiec.unam.mx/taxonomy/term/20
[6] http://let.iiec.unam.mx/descriptores-let/sujetos-de-la-guerra
[7] http://let.iiec.unam.mx/descriptores-let/tecnolog%C3%ADas-militares-tecnolog%C3%ADas-de-uso-dual
[8] http://let.iiec.unam.mx/sites/let.iiec.unam.mx/files/Proyecto%20de%20ley%20de%20funciones%20del%20ej%C3%A9rc