

Suing spies. America's government is putting foreign cyber-spies in the dock. Some of its own hackers are not pleased

Enviado por Carlos Alberto ... en Sáb, 10/06/2018 - 14:27

Cita:

The Economist [2018], "Suing spies. America's government is putting foreign cyber-spies in the dock. Some of its own hackers are not pleased", *The Economist*, London, 13 de septiembre, <https://www.economist.com/united-states/2018/09/15/americas-government-i...> [1]

Fuente:

The Economist

Fecha de publicación:

Jueves, Septiembre 13, 2018

Revista descriptores:

Competencia mundial. Disputa hegemónica [2]

Formas de la competencia entre grandes empresas [3]

Formas de la guerra [4]

Relación economía y guerra [5]

Sujetos de la guerra [6]

Tecnologías militares - tecnologías de uso dual [7]

Tema:

La ciberseguridad y la posibilidad de atribuir responsabilidades por ciber-crímenes

Idea principal:

Corea del Norte ha planteado casos paradigmáticos de ciberataques, como los cometidos por Park Jin Hyok, hacker norcoreano, en los últimos años. Muchos de estos ataques han sido realizados desde territorio chino, y la justicia política pasa por encima de ellos. Las acusaciones contra los ataques de norcoreanos no son las únicas. En 2014 el gobierno de Barack Obama señaló a cinco oficiales del ejército chino de espionaje industrial, en 2017 Donald Trump acusó a dos oficiales del Servicio Federal de Seguridad ruso por ciberataques a Yahoo y en marzo de 2018 acusó a nueve ciudadanos iraníes de robo de secretos científicos cometidos en nombre de la Guardia Revolucionaria de Irán. Quizá el caso más dramático fue en julio de 2018, con la acusación a 12 espías rusos por interferir en las elecciones presidenciales de 2016.

Las evidencias forenses han mostrado que una atribución de cargos por crímenes cometidos en el ciberespacio no es imposible. Estados Unidos y sus socios pueden observar sin ningún problema el funcionamiento de sus adversarios.

Sin embargo, no todos están de acuerdo con la idea de recurrir a los tribunales en cuestiones del ciberespacio. Algunos de los hackers del gobierno estadounidense temen verse afectados por las represalias que esto pueda generar. Esto ya ha pasado en Italia, donde se juzgó en ausencia a oficiales de la Agencia Central de Inteligencia por secuestrar a un clérigo egipcio en

Milán. Estas preocupaciones son válidas, pero exageradas ya que los adversarios de Estados Unidos carecen de capacidad técnica y moral para actuar contra sus hackers. Estados Unidos es un adversario agresivo en el ciberespacio, pero no utiliza sus capacidades técnicas para vandalizar o robar bancos. Estados Unidos busca trazar una división entre el espionaje tradicional -al que parecen considerar poco peligroso- y otros crímenes cibernéticos a los que consideran más graves, como la piratería, el sabotaje y el espionaje con fines comerciales. Sin embargo, esta línea sigue siendo difusa y difícil de fijar.

Datos cruciales:

1. En 2016, Park Jin Hyok, hacker norcoreano, robó 81 millones de dólares estadounidenses del banco central de Bangladesh, es considerado el mayor robo de banca digital a una sola institución. Otros ataques famosos de Park Jin Hyok son: el de 2014 contra Sony y el ataque con *ransomwares* conocido como WannaCry 2.0 que afectó miles de computadoras. Actualmente Park tiene una denuncia penal ante el Departamento de justicia.

Nexo con el tema que estudiamos:

El ciberespacio plantea un nuevo reto para la seguridad de Estados Unidos, de sus contrincantes y de sus aliados. Este espacio virtual es hoy, el mayor cúmulo de datos y lugar donde transitan flujos inmateriales que permiten el funcionamiento sistémico, recordando que el dato y el flujo, al final son elementos estratégicos. Es claro que Estados Unidos buscará en los próximos años fortalecer su ciberseguridad, pero que también desarrollará un proceso de control efectivo sobre el ciberespacio.

Source URL (modified on 6 Octubre 2018 - 5:25pm): <http://let.iiec.unam.mx/node/1976>

Links

- [1] <https://www.economist.com/united-states/2018/09/15/americas-government-is-putting-foreign-cyber-spies-in-the-dock>
- [2] <http://let.iiec.unam.mx/taxonomy/term/12>
- [3] <http://let.iiec.unam.mx/taxonomy/term/17>
- [4] <http://let.iiec.unam.mx/descriptores-let/formas-de-la-guerra>
- [5] <http://let.iiec.unam.mx/descriptores-let/relaci%C3%B3n-econom%C3%ADa-y-guerra>
- [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>