r.esici.10(19):281-287,2018

China: ciberespionaje estratégico para su economía y defensa militar[1]

César Augusto Sanabria Casanova[2, *]

Resumen

El ciberespacio, es uno de los campos donde ha permitido el avances de los diferentes factores sociales, culturales, militares, económicos, tecnológicos y educativos, evolucionando el mundo actual a grandes velocidades, creando una nueva era, la era del internet de las cosas "IoT", donde esa gran era ha permitido la conexión y comunicación a nivel mundial, generando que la información y los sistemas informáticos tanto como hardware y software se han unos de los activos estratégicos más importante dentro de una organización o estado, apareciendo el cibercrimen hacia las organizaciones estatales o gubernamentales y privadas, donde los cibercriminales pueden obtener este gran activo estratégico para obtener beneficios, es por ello que realizaremos un análisis de cómo está estructurado la República Popular de China y su influencia en los ciberataque a los diferentes países.

Palabras clave: innovación, tecnología, China, seguridad nacional.

Clasificación JEL: O31, O33; O53, F52.

Abstract

Cyberspace is one of the fields where it has allowed the advancement of different social, cultural, military,

[1] Artículo de investigación.

[2] Tecnólogo en Análisis y administración de Riesgo, Especialización Técnica en Ciberinteligencia.

[*] cesara.sanabria@gmail.com.

Fecha de recepción: 19 de enero de 2018.

Fecha de aceptación: 11 de mayo de 2018.

Para citar este artículo: Sanabria, C. (2018). China: ciberespionaje estratégico para su economía y defensa militar. *Perspectivas en inteligencia, 10*(19): 281-287.

economic, technological and educational factors, evolving the current world at great speeds, creating a new era, the Internet of things era "IoT", Where this great era has allowed worldwide connection and communication, generating that information and computer systems as well as hardware and software have become one of the most important strategic assets within an organization or state, with the appearance of cybercrime towards State or governmental and private organizations, where cybercriminals can obtain this great strategic asset to obtain benefits, that is why we will carry out an analysis of how the People's Republic of China is structured and its influence on the cyber-attacks to the different countries.

Keywords: innovation, technology, China, national security.

JEL classification: O31, O33; O53, F52.

Introducción

El ciberespacio es unos de los campos de batalla que se ve involucrados cualquier nación en el mundo, aunque sea un campo virtual no tangible, se pueden presentar múltiples de lesiones de forma bit a bit, como también de forma física donde se es necesario realizar operaciones ofensivas, defensivas y de sostenibilidad, donde lo referencia la BBC mediante declaración de William J. Lynn III, el subsecretario de Defensa de Estados Unidos:

Los ataques son constantes y están creciendo en frecuencia e intensidad. Pueden destruir estructuras físicas y sistemas operacionales, paralizar ciudades y generar millonarias pérdidas, inclusive costar vidas. Pero los instrumentos de todo este caos no son balas, bombas o tanques; son "bits y bytes (Márquez, 2011).

Donde se debe tener en cuenta las diferencias entre los diferentes conceptos entre Ciberseguridad, ciberinteligencia, ciberataque, ciberespionaje, donde la ciberinteligencia y sus niveles "Estrategia, Operacional, Táctica", permite el análisis de los diferentes amenazas existentes y desconocidas, identificando las diferentes vulnerabilidades existentes dentro una organización tanto pública como privada, permitiendo así el fortalecimiento e implementación de la ciberseguridad.

En el medio informativo CNN (2017). Berlinger &Perry hablan de los riesgos informáticos, en donde existen múltiples amenazas, de las cuales, se encuentran divididas en diferentes modalidades, niveles y tipos de cibercrimenes que puede afectar a nivel nacional y organizacional.

TABLA 1. Cibercrímenes políticos.

Ciberataques puros	Ciberataques réplicas	Ciberataques contenidos
Ataques DDOS (CiberWars) – (ciberactivismo) Malware intrusivo	Ciberesionaje terrorista (Sniffers - Keylogger) Ciberguerra (ataque DDOS)	Ciberterrorismo – Online hate speech (odio en línea)

Fuente: elaboración propia a partir de LLinares (2012).

TABLA 2. Cibercrímenes.

Ciberataques puros	Ciberataques réplicas	Ciberataques contenidos
Hacking Malware intrusivos Malware destructivos Ataques inseider	Phoarming, scam, auction fraud	Distribución de pornografía en internet Ciberpiratería intelectual

Ciberataques puros	Ciberataques réplicas	Ciberataques contenidos
Ataques DDOS Spam Ciberocupation Red Antisocial network	Cyberspyware – Sniffers	
	Sponfing (DNS pofing, ARP spofing, IP spofing, Web spofing)	
	Ciberblanqueo capitales	
	Ciberextorsión	
	Ciberocupación	

Fuente: elaboración propia a partir de LLinares (2012).

Planteamiento central general

La Oficina de Información Diplomática (2019) habla y explica de la recolección de información de los factores sociales, político, educativo, cultural, geográficos, económico, militar, tecnológico y científico, permitiendo así un análisis detallado de las posibles amenazas y estrategias que puede utilizar la República Popular de China, en especial en el campo del ciberespacio.

En el medio *Mail Online*, en su publicación llamada ¿Qué es China? (2019) afirman que en el ciberespacio existe una gran fortaleza que permite el acceso a gran parte del territorio nacional e internacional para realizar cibercrímenes y/o ciberataques aprovechando las vulnerabilidades de los sistemas de información, obteniendo información de interés y permitiendo así potenciar la estrategia militar y económica.

Hipótesis

a) La República Popular de China se encuentra realizando ciberataque como estrategia Económica y Militar.

b) Los sistemas de Información de la República Popular de china Tiene la Capacidad para realizar un ciberataque.

c) La tecnología implementada por la República Popular de china viene siendo obtenida a través de los Ciberataques.

d) Cuál es la verdadera actividad en el ciberespacio por parte de la República de China.

Metodología

Estudio de enfoque cualitativo, de tipo exploratorio para detectar ambientes y contextos iniciales acerca del ciberespionaje como estrategia política (exterior - interior), económica, militar, social, tecnológica y geográfica. Se realizó la recolección de datos bajo técnicas o procedimientos OSINT, que se constituyen en fuentes secundarias en procesos de metodología de investigación. A estos datos se les categorizó de forma abierta para identificar las estrategias que se utilizan en el ciberespacio por parte de la República Popular de China.

Resultados

Al analizar la información recolectada podemos evidenciar que la República Popular de China viene realizando una política Exterior, con el fin de realizar un cubrimiento geográfico que posteriormente son utilizados para labores en el ciberespacio permitiendo así la obtención de información para el fortalecimiento de su economía, tecnología y factor militar de forma silenciosa.

En la revista digital llamada *Deloitte, Nuevos Horizontes de Ciber Inteligencia* (2014) se evidencia que los diferentes laboratorios realizados por multiplex empresas se identificar que el ciberespionaje y los ciberataques utilizan diferentes tipos de herramientas con el fin de ocultar el origen del mismo, pero a través de laboratorios han identificado el código fuente donde posiblemente son orígenes de la República Popular de China.

Discusión - Hallazgos fundamentales

El Instituto Español de Estudios Estratégicos (IEEE), en su publicación *Ciber Seguridad en China* por Moran (2017) coligen la importancia de identificar e individualizar totalmente los diferentes tipos de ataques y ciberespionaje a nivel mundial, teniendo en cuenta que existen herramientas que permiten ocultar las diferentes características de los ciberatacantes, como hardware y software.

Conclusiones

La República Popular de China, viene desarrollando un sistema económico con el fin de sostener su modelo social comunista mixta, mediante el

fortalecimiento en los factores de comunicación, educación, tecnología, militar y cultural, permitiendo realizar múltiples tratados internacionales para exportar sus productos.

En el área de la tecnología viene implementando una evolución en sus sistemas tecnológicos generando política de exterior e interior para el fortalecimiento de este campo desde su capacitación de estudiante en sus primeros años de estudios como el intercambio de universitario con otros países, permitiendo su expansión a nivel mundial y generar fortalecer sus conocimientos en los diferentes campos principalmente en el campo tecnológico con dos propósitos.

El primero es el mejoramiento de los factores económicos, militares para su estabilidad del régimen socialista y el segundo con el propósito de implementar de forma clandestina, las diferentes actividades de ciberinteligencia y ciberespionaje, generando ciberataques por intermedio de terceros y su unidad de ciberseguridad 61398, para la adquisición de información de nuevas tecnología de los países que se encuentran con grandes avances tecnológicos e implementarlos a favor de la RPC, hay que tener claro que entre mayor capacidad tecnológica aumenta la posibilidad que sean mayor la efectividad estos incidentes informáticos permitiendo así el acceso no autorizados de la información de interés de sus inventarios no aliados.

Referencias

1. Álvarez, A. (2016). *Simposio electrónico internacional*. Recuperado de: http://www.asiared.com/es/downloads2/16_3-s_ana-sanchez.pdf
2. Anthony, S. (2013). *EXTREMETECH*. Recuperado de: https://www.extremetech.com/computing/159465-chinas-tianhe-2-supercomputer-twice-as-fast-as-does-titan-shocks-the-world-by-arriving-two-years-early
3. Arguelles, D. & Nagles, N. (2012). *Estrategias para promover procesos de aprendizaje autónomo*. 4ª ed., Bogotá D.C., Cundinamarca, Colombia: Universidad EAN.
4. Castaño, F. F., Garcia, L. L., & Granada, U. d. (s.f.). *Cruce de miradas, relaciones e intercambios*. Recuperado de: http://www.ugr.es/~feiap/ceiap3/ceiap/capitulos/capitulo50.pdf
5. Deloitte (2014). *Deloitte* Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/CISO/Ciber_seguridad.pdf
6. Gobierno de España, Ministerio de Asuntos exteriores y de Cooperación (2017). *China, República Popular (de) China*. Oficina de Información Diplomática. Recuperado de: http://www.exteriores.gob.es/documents/fichaspais/china_ficha%20pais.pdf
7. Griffith, K. (2017). *Dailymail*. Recuperado de: http://www.dailymail.co.uk/news/article-4937010/Clues-suggest-China-suspect-massive-Equifax-hack.html
8. Berlinger, J. & Perry, J. (2017). *CNN Edición Internacional*. Recuperado de: http://edition.cnn.com/2017/04/27/asia/china-south-korea-thaad-hack/index.html
9. LLinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid, España: Marcial Pons.
10. Móra, D. (2017). *IEEE*. Instituto Español de Estudios Estratégicos. Recuperado de: http://www.ieee.es/en/Galerias/fichero/docs_informativos/2017/DIEEEI01-2017_CyberChina_DRM.pdf