ISSN: 1390-4299
1390-3691
No. 25

URVIO

Revista Latinoamericana de Estudios de Seguridad

Amenazas híbridas

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
FLACSO Sede Ecuador • Diciembre 2019

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

URVIO está incluida en los siguientes índices, bases de datos y catálogos:

- Emerging Sources Citation Index (ESCI). Índice del Master Journal List de Thomson Reuters.
- SciELO Ecuador. Biblioteca electrónica.
- Redalyc. Red de Revistas Científicas de América Latina y el Caribe, España y Portugal.
- ERIH PLUS, European Reference Index for the Humanities and the Social Sciences. Índice de referencias.
- JournalTOCS. Base de datos.
- Directory of Research Journals Indexing (DRJI). Directorio.
- Actualidad Iberoamericana. Índice internacional de revistas.
- CLASE, Citas Latinoamericanas en Ciencias Sociales y Humanidades. Base de datos bibliográfica.
- Directorio LATINDEX, Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal.
- DIALNET, Universidad de La Rioja. Plataforma de recursos y servicios documentales.
- EBSCO. Base de datos de investigación.
- FLACSO-ANDES, Centro digital de vanguardia para la investigación en ciencias sociales - Región Andina y América Latina - FLACSO, Ecuador. Plataforma y repositorio.
- REDIB, Red Iberoamericana de Innovación y Conocimiento Científico. Plataforma.
- MIAR (Matriz de Información para el Análisis de Revistas). Base de datos.
- LatAm Studies. Estudios Latinoamericanos. Base de datos.
- Google académico. Buscador especializado en documentación académica y científica.

FLACSO
ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

URVIO, **Revista Latinoamericana de Estudios de Seguridad**
Número 25, diciembre de 2019
Quito - Ecuador

ISSN 1390-4299 (en línea) y 1390-3691

URVIO, Revista Latinoamericana de Estudios de Seguridad, es una publicación electrónica semestral de FLACSO, sede Ecuador, fundada en el año 2007. La revista constituye un espacio para la reflexión crítica, el debate, la actualización de conocimientos, la investigación y la consulta sobre temas vinculados con la seguridad, el delito organizado, la inteligencia y las políticas públicas sobre seguridad en la región.

Disponible en:
http://revistas.flacsoandes.edu.ec/index.php/URVIO
http://www.flacsoandes.org/urvio/principal.php?idtipocontenido=13

Información estadística sobre tasas de aceptación e internacionalización en Urvio #25
- Número de trabajos recibidos: 11 manuscritos.
- Número de trabajos aceptados publicados: 7.
- Índice de aceptación de manuscritos: 63,63%
- Índice de rechazo de manuscritos: 36,36%.
- Número de revisores internacionales: 22
- Número de revisores nacionales: 2
- Número total de revisores por países: 6 (Argentina, Colombia, México, Chile, España y Ecuador).
- Internacionalización de autores: 4 países (Argentina, España, Costa Rica y México).

Redes sociales

@revistaurvio
@revista_URVIO
Blog: https://revistaurvio.wordpress.com/
Academia.edu: https://flacso.academia.edu/RevistaUrvio

FLACSO
ECUADOR

RELASEDOR
Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada

El Comité Editorial de URVIO decidirá la publicación o no de los trabajos recibidos, sobre los cuales no se comprometerá a mantener correspondencia. Los artículos serán sometidos a la evaluación de expertos mediante el sistema de doble ciego. Las opiniones y comentarios expuestos en los trabajos son de responsabilidad estricta de sus autoras y autores, y no reflejan la línea de pensamiento de FLACSO, sede Ecuador. Los artículos publicados en URVIO son propiedad exclusiva de FLACSO, sede Ecuador. Se autoriza la reproducción total o parcial de los contenidos siempre que se cite como fuente a URVIO, Revista Latinoamericana de Estudios de Seguridad.

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Tema central

Misceláneo

Estudios Globales

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Central topic

Miscellaneous

Global Studies

URVIO

Revista Latinoamericana de Estudios de Seguridad

Red Latinoamericana de Análisis de Seguridad y Delincuencia Organizada (RELASEDOR)
y FLACSO Sede Ecuador
ISSN 1390-4299 (en línea) y 1390-3691 - Diciembre 2019 - No. 25

Tema central

Diversos

Estudos Globais

doi.org/10.17141/urvio.25.2019.4007

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 25, diciembre 2019-mayo 2020
pp. 24-40 • RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad

Cyber-physical Facts: A Proposed Analysis for Cyber Threats in the National Cybersecurity Strategies

Juan-Manuel Aguilar-Antonio[1]

Recibido: 3 de junio de 2019
Aceptado: 22 de agosto de 2019
Publicado: 2 de diciembre de 2019

Resumen

El artículo presenta la categoría de hechos ciberfísicos, una propuesta para el análisis y la delimitación de amenazas en el régimen híbrido del ciberespacio. Se propone la hipótesis de que América Latina, y en particular México, no comprenden en sus Estrategias Nacionales de Ciberseguridad (ENCS) la naturaleza de las ciberagresiones ni la posibilidad de que una crisis surgida en el ciberespacio salte al espacio físico o material. Para probarla se presenta el contexto de la ciberseguridad en la región y se realiza una crítica de la ENCS de México. Después se hace un análisis comparativo de cinco casos de interés y referencia entre los estudios de ciberseguridad, para introducir el concepto de hecho ciberfísico. Por último, se aplica la propuesta a un estudio de caso y se muestra su utilidad para las ENCS, así como su grado de impacto en la esfera de la seguridad pública y nacional.

Palabras clave: crisis política; internet; protección de datos; seguridad cibernética; seguridad del Estado

Abstract

The article introduces the category of cyber-physical facts, a proposal for the analysis and delimitation of threats in the hybrid regime of cyberspace. The research objective is to test the hypothesis that Latin America, and Mexico in particular, do not understand in their National Cybersecurity Strategies (NCSS) the nature of cyber-attacks, nor the possibility that a crisis arising in cyberspace will jump into the physical or material ground. To prove this, the context of cybersecurity in the region is presented and also a critique of the NCSS of Mexico. Then, the

1 Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México (UNAM), México, alchemistffvii@hotmail.com, orcid.org/0000-0002-4686-685X

article makes a comparative analysis of five cases of interest and reference in cybersecurity studies to introduce the concept of cyber-physical fact. Finally, this proposal is applied to a case study, and its usefulness to the NCSS is shown, as well as its degree of impact in the sphere of public and national security.

Keywords: cybernetics security; data protection; internet; political crises; State security

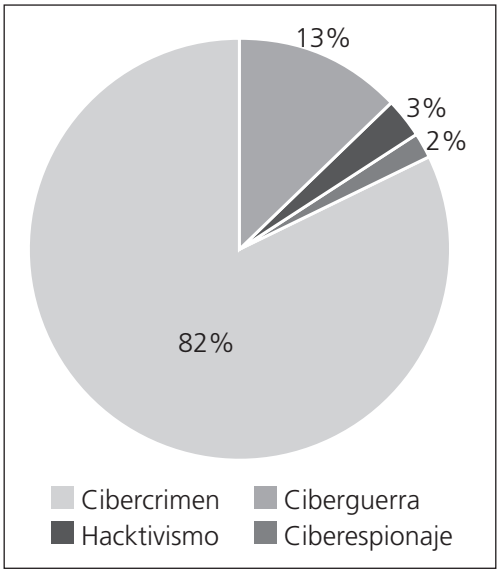
Introducción

La agenda de ciberseguridad es un reto entre las naciones de Latinoamérica, dada la velocidad de la evolución del ciberespacio. Entre los esfuerzos conjuntos de cooperación regional destaca el papel de la Organización de los Estados Americanos (OEA), con la publicación de la Estrategia Interamericana Integral de Seguridad Cibernética (2004) y la declaración de Fortalecimiento de la Seguridad Cibernética en las Américas (2012). En el plano unilateral, países como México, Argentina, Brasil, Colombia y Jamaica han estructurado Estrategias Nacionales de Ciberseguridad (ENCS), con importantes avances para consolidar una política de ciberseguridad, que forman parte de una tendencia creciente de la importancia del tema en la región (Cornaglia y Vercelli 2017).

Sin embargo, la creación de políticas de ciberseguridad enfrenta dificultades ante el incremento de ciberamenazas. Tan solo en el bienio 2012-2013 los ciberataques a entidades o sitios de internet públicos y privados crecieron más del 61 % (OEA y Symantec 2014). En 2014, países como Ecuador, Guatemala, Bolivia, Perú y Brasil se incluyeron entre las diez principales naciones con más computadoras infectadas por *malware*. Se sumaron Uruguay, Colombia y Chile, que estuvieron por encima de la media mundial de infección, situación que colocó a la región, junto a Asia, en las tasas más altas de virus maliciosos a escala global (PandaLabs 2015).

Las principales ciberamenazas en América Latina son ataques dirigidos por *malware* para robo de información sensible o confidencial. Las técnicas más utilizadas son el *spear-pishing* (correo electrónico diseñado para infectar un computador personal), y el *watering-hole* (infiltración de sitios web legítimos para mandar a través de ellos códigos maliciosos) (OEA y Symantec 2014). También, desde 2015 los troyanos dirigidos al fraude bancario han presentado un incremento considerable; se estima que el 92 % de las entidades financieras ha sufrido un ciberataque; 37 % del total resultaron exitosos (OEA 2018). Ese panorama presenta que las ciberamenazas se concentran en el sector y los usuarios privados. Situación que está en sintonía con las tendencias globales, como

Gráfico 1. Motivaciones detrás de ciberataques a escala global (2018)



Fuente: Pessiri (2019).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

parte de las cuales las actividades relacionadas con el cibercrimen son mayores (77,9% del total) que otras vinculadas a instituciones públicas o gubernamentales, como el ciberespionaje o hacktivismo (Pessiri 2019) (gráfico 1).

Es importante destacar que en América Latina no se ha presentado un ciberataque importante que involucre a actores privados con gubernamentales, con fines o motivaciones políticas, como el ataque de negación de servicio (DoS/DDoS[2]) acontecido en Tallin (2007) y Georgia (2008) o ataques enfocados al daño de Infraestructura Nacional Crítica (INC), como el de Stuxnet (2010).

En ese sentido, partimos de la hipótesis de que la región y sus ENCS no están preparadas para un ataque de tal naturaleza, y no consideran la posibilidad de que una crisis surgida en el ciberespacio pueda saltar al espacio físico o material. Para probar esto, utilizamos la metodología de estudio de caso para analizar la ENCS de México y hacemos una crítica a sus carencias y debilidades en el contexto actual de ciberamenazas. Posteriormente, hacemos un estudio comparativo de cinco casos de trascendencia en los estudios de seguridad, para presentar la categoría de hecho ciberfísico y su esquema de analítica para ciberamenazas.

Crítica a la ENCS de México

En México la penetración de internet representa el 60 % de la población, lo que significa 71,3 millones de cibernautas. La edad de los usuarios de internet se concentra entre los 18 y 34 años (83,4 %). Asimismo, el principal medio de acceso es a través de teléfonos inteligentes (89,7 %), y computadora de escritorio y portátil (34 %) (INEGI 2018). Durante 2017 las pérdidas económicas en ciberseguridad alcanzaron una cifra de 7,7 billones de dólares (Norton 2018). También, en el periodo 2013-2016 los ciberincidentes mostraron un incremento del 300 %, al pasar de 20 000 a 60 000, a la par de que se detectaron 5000 páginas de ciberfraude en el país (Parraguez 2018).

El principal medio de infección de computadores es a través de *malware* (98 %) y el resto se da a través de *spear-pishing* (Espinosa 2015). Resalta el incremento anual de efectividad de ambas modalidades de ciberinfección en 2015, con una tasa de crecimiento de 323 % para el *malware* y 409 % para *spear-pishing* (OEA y Symantec 2014). Norton (2018) resalta que los usuarios de internet gastaron 55,1 horas en promedio al año en resolver problemas vinculados a infecciones o amenazas provenientes del ciberespacio.

Ciberseguridad en el marco de la ENCS

La ciberseguridad es un tema posicionado en la agenda del gobierno de México. Desde 2013 existen al menos tres documentos que contemplan el tema y son clave para el diseño de políticas públicas: el Plan Nacional de Desarrollo (2013-2018), el Programa de Seguridad Nacional (2014-2018) y el Programa Nacional de Seguridad Pública (2014-2018). Asimismo, en 2017 se creó la Estrategia Nacional de Ciber Seguridad (ENCS), con lo cual México se convirtió en el octavo país en Latinoamérica en crear un documento de esta naturaleza.

Hasta 2018 la ENCS fue coordinada por múltiples instituciones, como la Comisión Nacional de Seguridad (CNS), la Secretaría

2 Un ataque DDoS tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Puede hacerse por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

de Gobernación (Segob), la Policía Federal (PF), con División de Policía Científica, la Secretaría de la Defensa Nacional (SEDENA) y la Secretaría de Marina (SEMAR). Datos de la Policía Científica destacan que hasta 2017 se atendieron 51 000 denuncias ciudadanas, más de 200 000 incidentes cibernéticos, se desactivaron 17 000 sitios fraudulentos y se emitieron más de 2000 alertas de ciberseguridad (ENCS México de 2017).

También, esta división de la PF gestiona el Equipo de Respuesta de Incidentes Informáticos (*CERT*[3] *MX*), el cual es miembro del Foro Global para Equipos de Respuesta a Incidentes y Seguridad (*FIRST*[4]). Por otra parte, las agencias gubernamentales utilizan el Manual Administrativo General de Gestión de Tecnologías de la Información, Comunicaciones y Ciberseguridad, de estándares ISO 27001. El Instituto Nacional Mexicano de Acceso a la Información, Transparencia y Protección de Datos Personales (INAI) colabora en esfuerzos por una mayor transparencia y disponibilidad de información y sensibiliza a los ciudadanos de sus derechos como usuarios de internet.

En indicadores internacionales, la Unidad de Inteligencia Económica de la Consultora Booz Allen Hamilton, que evalúa el ciberpoder entre las naciones que conforman el Grupo de los 20 (G20), posicionó a México en 11° lugar, a través de una medición de 39 indicadores en atributos que contemplan aspectos como el marco legal, regulatorio, económico y social, la tecnología implantada y la aplicación industrial (García 2018). Asimismo, el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT) posicionó a México en el lugar 18, de un total de 29, respecto a sus capacidades de acción y resiliencia en ciberseguridad (UIT 2014). A pesar de que esas mediciones consideran que el país detenta capacidades intermedias en cuestiones de ciberseguridad, es necesaria una crítica para mejorar la capacidad de acción de la ENCS y su capacidad de enfrentar ciberamenazas.

Revisión de la ENCS de México

El objetivo general de la ENCS de México es:

> Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las Tecnología de Información de la Comunicación (TIC) de manera responsable para el desarrollo sostenible del Estado Mexicano (ENCS de México 2017).

El enunciado anterior contiene múltiples elementos vinculados a la creación de capacidades de resiliencia en el ciberespacio: su comprensión multidimensional (en la esfera social, económica y política) y la coordinación y cooperación de entidades públicas o privadas. Sin embargo, en su segunda parte es visible cómo la estrategia del país está concentrada en incrementar la penetración del internet y consolidar su uso como un derecho universal, más que en crear capacidades de resiliencia ante ciberamenazas. Esa conclusión es más visible al revisar su estructura:

> Objetivos estratégicos: sociedad y derechos, economía e innovación, instituciones públicas, seguridad pública, seguridad nacional.

3 CERT, del inglés *Computer Emergency Response Team,* es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

4 Siglas en inglés de *Forum of Incident Response and Security Teams.*

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

> Principios rectores: perspectiva de derechos humanos, enfoque basado en gestión de riesgos, colaboración multidisciplinaria y de múltiples actores.
> Ejes transversales: cultura de ciberseguridad, desarrollo de capacidades, coordinación y colaboración, investigación, desarrollo e innovación TIC, estándares y criterios técnicos, infraestructuras críticas, marco jurídico y autorregulación, medición y seguimiento.

La ENCS sostiene que sus objetivos estratégicos y principios rectores se concentran en aumentar el uso de internet en México. Esta visión se vincula al concepto de brecha digital, que representa la separación entre las personas que utilizan las TIC como una parte de su vida diaria y quienes no tienen acceso a ellas o no saben cómo utilizarlas (Gómez et al. 2018). La aún baja penetración de internet en México explica el énfasis del documento en mejorar su uso y acceso. Una primera crítica a la ENCS se basa en esta condición, dado que la reducción de la brecha digital entre usuarios y no usuarios corresponde a otro tipo de política pública.

Por otra parte, el apartado de la ENCS más vinculado al desarrollo de capacidades de resiliencia en el ciberespacio se concentra en sus ejes trasversales. Entre estos destacan: a) desarrollo de capacidades, b) coordinación y colaboración, c) infraestructuras críticas y d) marco jurídico y autorregulación. No obstante, la ENCS se presenta más como un documento en construcción que una política de ciberseguridad que contemple protocolos o mecanismos para consolidar capacidades de acción y reacción en materia de ciberseguridad.

Los apartados de desarrollo de capacidades, coordinación y colaboración contienen oraciones ambiguas que no se concretan en indicadores, metas concretas o cuantificables. A la par, estas secciones deben incluir un organigrama de la política de cooperación entre las instituciones del gobierno encargadas de la ciberseguridad, como la División Científica, SEDENA, SEMAR, Segob, etc., en el que destaquen las facultades de cada una en la ENCS (Espinosa 2015). Una tarea pendiente es identificar los vínculos y actores de la industria privada interesados en colaborar con el gobierno. En ese sentido, resalta que durante 2017, el mismo año de la publicación de la ENCS, la Cámara Nacional de la Industria Electrónica, Telecomunicaciones y Tecnologías de la Información (CANIETI) presentó un informe relacionado con el tema, en que solicitó al gobierno el establecimiento de una Agencia Nacional de Ciberseguridad que coordine la ENCS entre actores gubernamentales y privados, y establezca una ruta crítica para la gobernanza de internet en México (Parraguez 2018).

Un aspecto de interés es que en el eje transversal de INC se cita la Ley Nacional de Seguridad como documento rector de la política de ciberseguridad (ENCS de México 2017). Sin embargo, no se destacan acciones fundamentales para su protección, como la actualización del catálogo de INC de México, así como la diferenciación entre cuáles deben ser administradas por entidades públicas y privadas. Del mismo modo, no se sugiere la elaboración de guías y estándares para su protección (Calderón 2018?).

Por último, en el eje de marco jurídico y autorregulación, destacamos la necesidad de actualizar las legislaciones nacionales que engloban al ciberespacio, con base en lo establecido en el Convenio de Budapest (García 2018), una actualización sobre la clasificación de ciberdelitos punibles (Espinosa 2015) y la armonización de todas las leyes sobre delitos

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

informáticos (Parraguez 2018). Entre las normativas se encuentran: el art. 16 (referente a la inviolabilidad de las comunicaciones y la protección de los datos personales), de la Constitución Política de los Estados Unidos Mexicanos; los artículos 167 (sanción por la interrupción, interferencia e intervención de comunicaciones electrónicas), 202 (almacenamiento y difusión de pornografía infantil por medios electrónicos) y 211 Bis (acceso ilícito a equipos y sistemas de informática) del Código Penal Federal. También el Título IV, Capítulo IV (de regulación de la copia, alteración y reproducción de software y bases de datos) de la Ley Federal del Derecho de Autor y el Art. 298 (de pena al bloqueo del servicio de internet; intercepción de la información transmitida en redes públicas y no adopción de medidas para garantizar la confidencialidad y privacidad de comunicaciones) de la Ley Federal de Telecomunicaciones y Radiodifusión.

La crítica realizada a la ENCS de México devela que existe una marcada distancia entre el entorno actual de ciberamenazas a escala global y su contenido. Asimismo, no existe una concordancia o revisión para el aprendizaje de experiencias internacionales, para comprender el potencial del ciberespacio como un instrumento para vulnerar la seguridad pública o nacional, a escala local, nacional o internacional, que tome en cuenta que las crisis surgidas en esta arena pueden brincar del espacio virtual al material. Cómo propuesta de análisis para la promoción de una agenda de ciberseguridad, se presenta la categoría de hecho ciberfísico, que explicaremos a través de un estudio comparativo de cinco casos de interés para los estudios de ciberseguridad.

Revisitando Tallin: interpenetración de la escala local, nacional e internacional

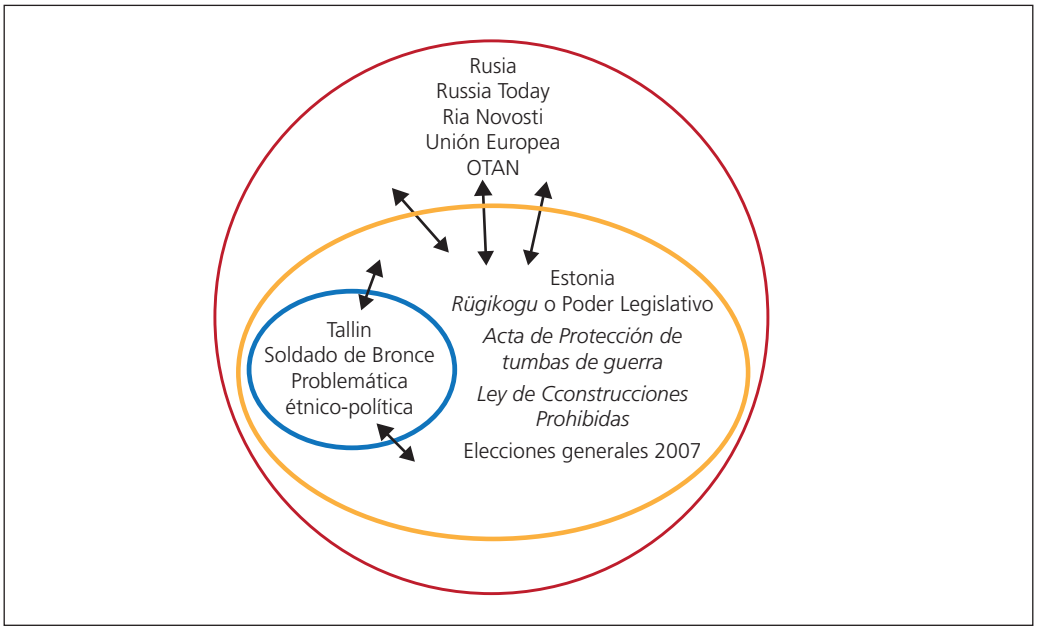
Existe un consenso generalizado entre los estudios de ciberseguridad en señalar a los ataques de Tallin, Estonia (2007), como el primer caso de trascendencia que involucra a internet como un instrumento capaz de vulnerar la seguridad nacional de un Estado. La relevancia del caso hizo que se hablara de internet como un mecanismo capaz de promover una revolución en la política internacional (Kello 2013), que se señalara al ciberespacio como una nueva arena de confrontación e influencia de las naciones (Hughes 2010), que necesita la construcción de la securitización para su uso y regulación (Hansen y Nissenbaum 2009).

Una particularidad que presentan los análisis centrados en Tallin es abordar el evento desde la óptica de la seguridad nacional, con implicaciones para la soberanía de Estonia. En este análisis se proponen tres escalas para su comprensión, que explican un hecho ciberfísico, y se muestra cómo una ciberamenaza puede moverse a diferentes escalas y esferas. La figura 1 refleja cómo se superponen los niveles; dentro de cada esfera existen actores y factores que influyeron en la crisis de Tallin.

Escala local-nacional. La crisis de Tallin empieza con una motivación local, que es la reubicación de un monumento soviético denominado "Soldado de Bronce". En primera óptica, su remoción se interpreta como un problema étnico-político que confrontó a dos sectores de la población, uno con raíces culturales estonias y otro de origen ruso-soviético (Schmidt 2013). Desde la perspectiva de la seguridad pública, el malestar político y civil que podía causar el evento no es menor, dado que 350 000 habitantes (26,5 % del total de

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

Figura 1. Interpenetración de escalas de seguridad en el ciberataque de Tallin (2007)



Fuente: elaboración propia.

la población del país) tenía algún grado de parentesco o filiación con Rusia o el periodo de dominación soviética. Tallin concentra una tercera parte de la población y era susceptible de sufrir fuertes disturbios.

La reubicación del monumento fue un tema central de la agenda parlamentaria desde enero de 2017 (BBC News 2007). De hecho, durante los meses previos a su remoción, el parlamento o *Riigikogu* legisló dos iniciativas para su reubicación: El Acta de Protección de Tumbas de Guerra, el 10 de enero, y la Ley de Construcciones Prohibidas, el 15 de febrero. Ese año el país celebró sus primeras elecciones generales que utilizaron el voto electrónico, hecho que formaba parte del proyecto de modernización tecnológica *X-Road*, cuyo objetivo era volver electrónicos todos los servicios del gobierno para 2015 (Detlefsen 2015).

En ese contexto, la confrontación entre un partido europeísta (Partido Reformista) y un partido cercano a Rusia (Partido del Centro) promovió que la reubicación se aplazara hasta después de las elecciones, el 4 de marzo (BBC 2007). No fue hasta después de la victoria del candidato reformista, Andrus Ancip, que el tema se retomó dentro del parlamento. Por último, se destaca que un discurso de Ancip, con comentarios despectivos hacia el monumento soviético, el 24 de abril, fue lo que detonó la convocatoria de protestas y consecuentes disturbios.

Escala nacional-internacional. Hasta la convocatoria de protestas en contra del gobierno, la crisis del "Soldado de Bronce" no se había transformado en un problema de ciberseguridad. Los disturbios del 26 de abril se consideraron la peor crisis de seguridad pública del país desde su independencia, pero no formaban parte de una problemática de

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

este tipo. El ataque cibernético se reveló al gobierno cuando este convocó a una reunión del Comité de Crisis para atender los disturbios de seguridad pública y los escenarios de inestabilidad política. Fue en esa reunión que las autoridades de Estonia recibieron la notificación de que los sitios gubernamentales habían empezado a recibir un tráfico inusual de datos, que causó problemas en los portales en línea y servicios estatales, evento que fue el inicio del ataque DDoS (Nguyen 2013).

El ciberataque perjudicó por completo la operatividad de todos los sitios del gobierno. También, portales privados y de noticias se vieron imposibilitados de compartir contenido. En el caso de los bancos, el ataque impidió operaciones como transacciones bancarias y el uso de cajeros electrónicos durante cuatro días. En este punto, resalta el papel de las agencias de noticias extranjeras, principalmente de origen ruso, que sí podían compartir información durante las protestas, mientras otros sitios no tenían esta capacidad. Eso generó desinformación (Detlefsen 2015).

En la vinculación de Estonia con el extranjero, una de las primeras acciones que ejecutó el CERT para reducir el flujo de información de *bots* fue bloquear todos los sitios de internet del extranjero, con especial énfasis en los provenientes de Rusia, ya que el 99 % de excesos de información de *bots* era de ese país (Schmidt 2013). Con estas acciones, el 30 de abril, el CERT y la policía de Tallin contuvieron el ciberataque y los disturbios en las calles. No obstante, la crisis de seguridad pública y nacional tomaría una nueva forma, al transformarse en una crisis diplomática y de política exterior, debido a las agresiones que recibió la embajadora Marina Kaljurand, en la embajada de Estonia en Moscú, que derivaron en la retirada de la diplomática de Rusia (Finn 2007).

El gobierno estonio presentó el tema de los ciberataques en su agenda de organismos multilaterales para pedir la asistencia y solidaridad de otros países. Lo hizo en la Unión Europea (UE), el 17 de mayo, durante la cumbre UE-Rusia (Martínez 2007) y, de forma unilateral, ante la Secretaría General de la Organización del Atlántico Norte (OTAN), en la que proclamó el artículo 5 de la alianza y exigió que los ciberataques fuera considerado una agresión contra todos sus miembros. La acción resultó exitosa, dado que impulsó la creación del Centro Cooperativo de Ciberdefensa de Excelencia (NATO CCDCOE por sus siglas en inglés), con la finalidad de mejorar la capacidad, cooperación e información de la OTAN ante ciberamenazas (Tamkin 2017).

Escala local-nacional-internacional. Esta escala muestra la interpenetración de la crisis del "Soldado de Bronce" en los tres niveles. La figura 2 presenta cada escala: problemáticas, actores involucrados y temporalidad de los sucesos. Expone cómo los sucesos detonadores de cada tema de seguridad difieren en cada nivel. Sin embargo, la interconexión entre la crisis de seguridad pública, el ataque DDoS como problema de seguridad nacional y la crisis diplomática y agenda de política exterior muestra una interrelación entre cada evento.

La importancia del análisis es señalar que la crisis de Tallin, al inicio, no correspondía a un problema de ciberseguridad. En un primer nivel se refería a un tema de seguridad pública en un espacio físico. Sin embargo, las condiciones y el contexto político permitieron la injerencia de actores extranjeros para utilizar la problemática local, en una plataforma (internet) que se consideraba una fortaleza de Estonia.

Por otra parte, el punto más álgido del caso de Tallin es cuando se combina la crisis de seguridad pública (en el espacio físico) y el

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

Figura 2. Escala local-nacional-internacional de la crisis del Soldado de Bronce y los ciberataques de Tallin (2007)

LOCAL TALLIN	**NACIONAL ESTONIA**	**INTERNACIONAL ESTONIA-RUSIA-UE-OTAN**	Escala de acción
Catalizador: Reubicación del Soldado de Bronce **Problemáticas:** Conflicto étnico-político Protestas y vandalismo Crisis de seguridad pública **Actores involucrados:** Policía y Alcaldía Tallin **Temporalidad:** 10 enero- 30 abril 2007	**Catalizador:** Comentarios del 1er Ministro Andrus Ansip **Problemáticas:** Ataque DDoS a servidores gubernamentales y privados de Crisis de seguridad Nacional **Actores involucrados:** Gobierno Estonio y Comité de Crisis, Banca Privada y Medios de Comunicación **Temporalidad:** 26 abril - 30 abril 2007	**Catalizador:** Agresiones de bots de origen ruso a sitios web de Estonia y agresión a Embajadora estonia en Moscú **Problemáticas:** Crisis diplomática Estonia-Rusia **Actores involucrados:** Estonia, Rusia, UE y OTAN **Temporalidad:** 30 abril - mayo 2007	
Étnico-político Seguridad Pública Opinión Pública	Seguridad Nacional Banca Privada Economía Opinión Pública Acceso a Información	Diplomacia Seguridad Nacional Seguridad Regional Seguridad Internacional	Espacios de superposición o inteppenetración

Fuente: elaboración propia.

ataque DDoS a todos los servicios electrónicos del gobierno y a entidades privadas (canales de noticias e instituciones bancarias). Es en ese punto de desequilibrio que las autoridades policiales y el CERT realizan las acciones clave, en aras de encontrar una solución a ambas problemáticas.

Posteriormente, la escala local-nacional se enlaza en el ámbito internacional por las tensiones diplomáticas entre Rusia y Estonia, dado el origen de los *bots* y las agresiones que recibió la misión diplomática estonia. En conclusión, la crisis de Tallin muestra cómo los eventos del espacio físico pueden brincar al ciberespacio para vulnerar diferentes niveles de seguridad de un actor estatal, característica que define a los hechos ciberfísicos.

Cinco casos de los estudios de ciberseguridad y el régimen híbrido del ciberespacio

En este apartado se discute cómo una ciberamenaza, desde la comprensión de una ENCS, es aquella que tenga implicaciones, consecuencias o impacto tanto en el espacio físico o material como en el virtual.

Para esto, se añaden al caso de Tallin otros cuatro casos de interés para los estudios de ciberseguridad: 1) el *Cablegate* de los papeles del Departamento de Estado de los Estados Unidos (Farrel y Finnemore 2013; Medcalf 2011); 2) el uso de redes sociales durante la Primavera Árabe (Auoragh 2012; Bachrach 2011); 3) el gusano *Stuxnet,* que atacó la base nuclear de

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

Tabla 1. Hechos ciberfísicos, narrativa virtual, material y espacios de interpenetración

Casos de análisis	Narrativa virtual	Narrativa material	Espacios de interpenetración
1. Ciberataques de Tallin (2007)	a. Ataque DDoS a todos los sitios gubernamentales y de empresas privadas. b. Interrupción de servicios bancarios y noticias.	a. Conflicto étnico-político entre estonios y rusos y protestas sociales. b. Traslado del Soldado de Bronce.	Seguridad pública y nacional. Ciberseguridad. Economía. Opinión pública.
2. Cablegate (2010)	a. Extracción de 251 a 287 documentos del Departamento de Estado. b. Publicación de los primeros 291 cables en cinco diarios internacionales y publicación del resto.	a. Tensión diplomática entre EEUU y países referidos en los cables. b. Atención en medios de comunicación y publicaciones de *The Guardian*, *The New York Times, El País, Le Monde y Der Spiegel*, y quejas diplomáticas.	Política nacional y diplomacia. Seguridad nacional. Ciberseguridad. Opinión pública
3. Uso de redes sociales en la Primavera Árabe.	a. Uso libre, sin restricciones de libertad de opinión, de la internet en Egipto y Túnez. b. Promoción de debates sociales respecto al régimen autoritario en Twitter y Facebook. c. Organización de protestas a través de redes sociales.	a. Protestas sociales en contra del régimen autoritario y la represión policiaca y militar contra civiles. b. Renuncia de los mandatarios o jefes de Estado y reestructuración política.	Política nacional. Seguridad pública y nacional. Ciberseguridad. Opinión pública.
4. Stuxnet (2010)	a. Planeación y diseño de un ciberataque entre actores estatales (EEUU e Israel) y no estatales (Microsoft). b. Creación de un *malware* con capacidad de afectar las centrífugas Siemens S7-315, y afectación de más de 1000 sistemas informáticos en la Central Nuclear Natanz, Irán.	a. Daños a las centrífugas de la central nuclear de Natanz, Irán. b. Retraso de tres años del programa nuclear iraní.	Seguridad nacional. Infraestructura crítica. Ciberseguridad.
5. LuzlSec (2011)	a. Protesta cibernética en contra de PayPal y Master Card. b. Convocatoria, amenaza y realización de ciberataques a sitios gubernamentales y empresas por 50 días.	a. Imposibilidad de usar redes públicas (FBI y CIA) y privadas (Sony y AT&T). b. Interrupción de comunicaciones y servicios gubernamentales y pérdidas económicas de la empresa.	Seguridad privada y gubernamental. Ciberseguridad. Hacktivismo económico.

Fuente: elaboración propia.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

Natanz, Irán (Detlefsen 2015; Lagner 2013) y 4) el conjunto de ciberataques a empresas privadas y portales gubernamentales del grupo hacktivista *LulzSec* (DiSanto 2015; Thaw 2013). En la tabla 1 se presenta el resumen del análisis, las implicaciones o consecuencias de la narrativa virtual y material, y los espacios de superposición e interpenetración.

La tabla 1 muestra al menos tres esquemas de análisis para cada caso de estudio: a) las escalas de seguridad (local, nacional o internacional); b) la interdependencia y cooperación de los actores o partes interesadas, que pueden ser gubernamentales o públicos (gobiernos nacionales o locales, instituciones policiacas) y privados (empresas, medios de comunicación, bancos, etc.); y c) la materialización de los efectos de una ciberagresión tanto en el ciberespacio como en el espacio físico.

Hechos ciberfísicos en el régimen híbrido del ciberespacio

El concepto de hecho ciberfísico representa una categoría de análisis para delimitar eventos, casos o unidades de estudio en que las dinámicas o procesos sociales tienen repercusiones, impactos o consecuencias que vinculan a internet y al espacio material. Pretende servir a los estudios de ciberseguridad y a los creadores de políticas de ciberdefensa y ciberseguridad. El argumento central de los hechos ciberfísicos es exponer que existen eventos que tienen efectos tanto en el mundo material como en el virtual. Asimismo, al manifestarse dentro de un espacio sin fronteras (como internet), estos pueden saltar a diferentes niveles e incluir a múltiples actores gubernamentales, nacionales o privados.

El concepto contempla cualquier canal de comunicación de la sociedad y sus actores (política, economía, comercio, cooperación internacional, etc.). En ese sentido, responde a la noción de que el ciberespacio es un régimen híbrido con características materiales e inmateriales, cuyos componentes físicos y virtuales coexisten en el mundo real, y con capacidad de impacto en las dinámicas sociales (Nye 2010; Demchak 2012).

La comprensión de lo ciberfísico como esquema de análisis híbrido de un fenómeno social puede mejorar con la comparación de conceptos semejantes como lo glocal y el enfoque de seguridad interdoméstico. El término glocal fue utilizado ampliamente dentro de la teoría social a finales del siglo XX, para analizar fenómenos y dinámicas sociales derivados del proceso de globalización, en que la reducción de fronteras (económicas, financieras, políticas, etc.) cambió las características típicas de los espacios locales y globales, entre los que era cada vez más indisociable determinar los límites de lo provincial e internacional. Así, glocal es un neologismo que combina ambas categorías. Fue utilizado para describir el incremento de la interacción de las fuerzas de la economía global con las respuestas de las comunidades locales y regionales, noción que promovió una nueva escala de análisis de la organización socio-territorial del Estado nación (Taylor 1996). Posteriormente, se usó para explicar fenómenos como los procesos de integración económica (Keeling 2004), las dinámicas financieras y multiculturales de grandes urbes (Curtis 2011; Sidaway 2006) y los fenómenos derivados de la migración (Hoerder 2010; Van Wijk y Bolhuis 2017).

Por otra parte, el enfoque de seguridad interdoméstica surgió como una categoría de análisis en el período posterior a la Guerra Fría. En ese momento se consideró obsoleta la visión de la seguridad nacional centrada en la

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

integridad territorial, frente a nuevas amenazas y retos para la seguridad nacional (Lindstrom y Luiijf 2012). Sirvió para la creación de los complejos regionales de seguridad en América, con lo que promovió una reinterpretación del concepto de seguridad más allá del aspecto militar, para incluir amenazas de diverso tipo o no tradicionales (Buzan, Waever y De Wilde 1998). Acuerdos de cooperación regional y procesos de integración económica incluyeron en su agenda asuntos como crimen organizado, narcotráfico, estabilidad política, migración, ecología y terrorismo (Benítez 2005).

Ambos términos ejemplifican cómo lo ciberfísico responde a una reconceptualización para abordar fenómenos de características híbridas, como los que competen a los estudios de ciberseguridad. En la figura 3 se representa el régimen de análisis mixto que distingue a los hechos ciberfísicos, emparentado con ambos términos citados.

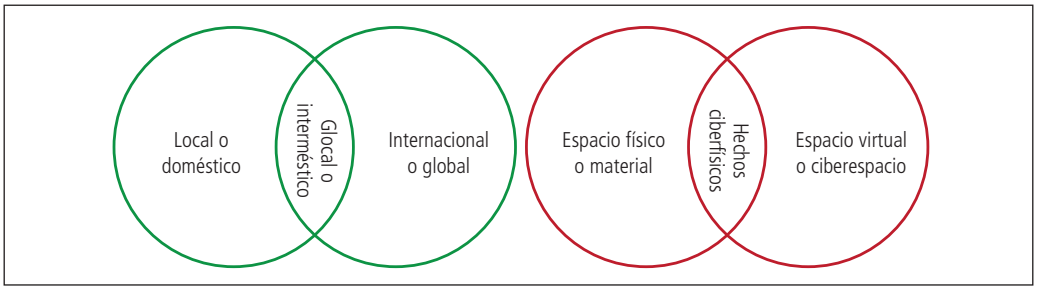
Interacción, cooperación y conflicto en el ciberespacio: actores y partes interesadas

La interacción de los actores del ciberespacio es otro asunto de interés dentro de la propuesta de los hechos ciberfísicos, dada la necesidad de enmarcar a los protagonistas del ciberespacio y localizar unidades de estudio que permitan utilizar la categoría. Esta acción es necesaria para que los estudios del ciberespacio puedan crear y operacionalizar estrategias dirigidas a construir una agenda de ciberseguridad.

La comprensión de los protagonistas del ciberespacio, desde el enfoque de la seguridad nacional, corresponde a una visión que pone en el centro al Estado nación y a los actores gubernamentales. No obstante, esta visión de seguridad acepta que, para promover una estrategia efectiva para crear protocolos o estrategias de ciberseguridad, es necesaria la participación de actores privados y no estatales. Una propuesta sólida en esa óptica es la de las partes interesadas (*stakeholders* en el texto en inglés), que clasifica a los actores del ciberespacio en tres grandes grupos (Klimburg y Healey 2012).

El primero son los actores estatales, en concreto, Estados nación e instituciones gubernamentales. Son entidades con los mejores y sofisticados recursos para influir en el ciberespacio, dada la capacidad de componer grandes equipos de seguridad informática y al hecho de que poseen infraestructura en telecomunicaciones. Entre las ventajas que los distinguen está ser entidades de gran tamaño

Figura 3. Categorías de análisis híbrido: seguridad interdoméstica, glocal y hechos ciberfísicos ques de Tallin (2007)



Fuente: elaboración propia con base en (Buzan, Waever y De Wilde 1998; Beck 1998).

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

y abarcar múltiples unidades de gobierno (locales, regionales o nacionales), así como diferentes esferas de influencia (política, educativa, comercial, etc.). Es muy complicado que una ciberamenaza afecte la totalidad de sus componentes. Otra fortaleza es que detentan un marco de normas legales e instituciones de justicia para someter a un ciberagresor. Entre sus desventajas está su lenta capacidad de reacción, dada la gran cantidad de unidades gubernamentales que deben coordinar. En esa clasificación se incluyen actores como Estados nación, organismos internacionales o regionales y gobiernos subnacionales.

El segundo grupo son los actores no estatales organizados. Comprende a las entidades fuera del Estado nación y de carácter privado con un nivel mínimo de organización. Entre estas se encuentran los creadores del *hardware* y *software* utilizado en el ciberespacio. Son las principales víctimas de ciberagresiones y delitos, a la vez que ejecutan la mayoría de las ciberoperaciones de internet, ya sea por intereses particulares o para apoyar a un gobierno. Los estudios de ciberseguridad ponen especial atención en estos actores, dado que poseen una capacidad de reacción más rápida que los actores estatales. Entre ellos se encuentran empresas de *software*[5] (Microsoft, Linux, etc.), empresas de seguridad informática (McAfee, Norton) y prestadores de telecomunicaciones (AT&T, Vodafone…), al igual que los más peligrosos grupos de cibercriminales (mafias y delincuencia organizada). Este grupo engloba: empresas trasnacionales y de *software*, portadores de telecomunicaciones, ONG, grupos criminales y grupos terroristas.

El tercer grupo son los actores no estatales no organizados, que realizan operaciones o campañas de bajo nivel en el ciberespacio. Ese tipo de acciones son conducidas por pequeños grupos de individuos, sin nivel de jerarquía, o por actores individuales. Una característica suya es la ausencia de una autoridad o cadena de mando, que limita su nivel de operación y capacidad de daño. A diferencia de las grandes organizaciones criminales o grupos delictivos bien estructurados, este tipo de actores no desempeñan actos de cibercrimen de alto valor, además de que sus campañas son de corta duración. La clasificación engloba: hackitivistas, pequeños grupos criminales e individuos autónomos.

Por otra parte, un proceso de interacción en el ciberespacio supone dos vías: la cooperación o el conflicto. De acuerdo con Kello (2013), esta dinámica se presenta en cuatro escenarios.

- Estatal a estatal: corresponde a una acción en el ciberespacio ejecutada por un actor estatal o gobierno hacia otro actor de las mismas características.
- Privado a estatal: representa los ciberataques u operaciones de actores no estatales organizados o no organizados, dirigidos a activos estratégicos de Estados o gobiernos.
- Privado a privado: señala los procesos de cooperación o agresión entre dos entidades no estatales, ya sean estas organizadas o no organizadas.
- Estatal a privado: define la colaboración o agresión de un gobierno o actor estatal con una entidad privada, ya sea organizada o no organizada.

5 Son empresas que diseñan *software* o soporte lógico de un sistema informático, lo cual comprende los componentes que hacen posible la realización de tareas específicas y todas las funciones que permite un ordenador.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

Estudio de caso: comprensión de los ataques al SPEI desde los hechos ciberfísicos

El marco de análisis de los hechos ciberfísicos puede aplicarse al caso concreto de México, y la crítica a su ENCS, en dos importantes ciberataques al Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México (BM), en 2018. El primero fue detectado a finales del mes de abril e involucró a tres bancos privados, una casa de bolsa y una caja de ahorro popular. Se estima que hubo pérdidas de alrededor 300 000 000 de pesos (Valdelamar 2018).

El segundo fue ejecutado en octubre de 2018, a través de la aseguradora AXA, institución privada mediante la cual los agresores infiltraron el SPEI y realizaron múltiples operaciones anómalas. Tras ese ataque, tres instituciones gubernamentales –el BM, la Secretaría de Hacienda y Crédito Público (SHCP) y la Comisión Nacional Bancaria y de Valores (CNBV)– elevaron a rojo el nivel de alerta de seguridad informática en las operaciones del SPEI (Estañol 2018). Posteriormente, la firma de ciberseguridad *Fire Eye* expresó que el culpable del ciberataque fue el equipo de hackers APT38, una cédula norcoreana encargada de ejecutar ciberataques a bancos de naciones extranjeras para obtener recursos para su país, famosos por haber vulnerado 16 instituciones bancarias en 11 países y haber extraído 100 000 000 de dólares (Lara 2018).

Los ataques al SPEI presentan una importante área de oportunidad para consolidar una agenda de ciberseguridad y delimitar el nivel de impacto de las ciberamenazas, en la cual se puede utilizar el esquema de los hechos ciberfísicos, dada la importante afectación que sufrieron el BM y las partes interesadas, que no contempla la ENCS de México. En la tabla 2 se presenta un análisis desde esta propuesta.

Tabla 2. Análisis de ataques al SPEI como hechos ciberfísicos

Caso de análisis	Narrativa virtual	Narrativa material	Escalas	Partes Interesadas	Tipo de ataque
Ataques al SPEI en México (2018)	A. 1er ataque en abril: involucró a tres bancos privados, una casa de bolsa y una caja de ahorro popular. B. 2do ataque en octubre: a través de AXA, por quien se infiltraron el SPEI.	A. El prestigio de los bancos, clientes y activos se vio afectado, con pérdidas de 300 000 000 de pesos. B. El BM, la SHCP y la CNBV elevaron a rojo el nivel de alerta de seguridad informática en las operaciones del SPEI, afectando todas sus operaciones.	A. Escala local -nacional: dado que afectó a instituciones bancarias locales y nacionales. B. Escala nacional-internacional: dado que afectó al BM y a una aseguradora de origen francés. Asimismo, los atacantes eran de Corea del Norte, Estado agresor.	A. Actores estatales: BM, SHCP y CNBV. Actores no estatales organizados: casa de bolsa, caja de ahorro popular y APT38. B. Actores estatales: BM, SHCP, CNBV. Actores no estatales organizados: APT38, *Fire Eye* y AXA.	A. Privado a Estado; privado a privado. B. Privado a Estado Estado a Estado.

Fuente: elaboración propia.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 25 • diciembre 2019-mayo 2020 • pp. 24-40
ISSN 1390-4299 (en línea) y 1390-3691

Conclusiones

Las ENCS en América Latina y México están alejadas de la comprensión actual de las ciberamenazas y el potencial del ciberespacio para vulnerar la seguridad pública y nacional. Esta distancia explica el alto grado de incremento anual de ciberagresiones entre los Estados de la región y el hecho de que detente las tasas globales más altas de infección por virus maliciosos y ciberataques a instituciones bancarias, junto con Asia.

El análisis devela que las ENCS no contemplan protocolos que involucren diferentes escalas de análisis (local, nacional e internacional), así como protocolos de acción o vinculación entre las partes interesadas del ciberespacio (actores estatales, actores no estatales organizados y no organizados) para la prevención de ciberamenazas.

La ausencia de vínculos entre actores públicos y privados ha incrementado los ciberataques a bancos y actores privados. La poca presencia de ataques de corte político como ciberespionaje, hacktivismo o ataques a INC ha hecho que las ENCS no tengan protocolos concretos en contra de este tipo de agresiones. Otro aspecto importante es que no existe una acción de aprendizaje, estudio o análisis de casos de trascendencia que involucren al ciberespacio y su impacto en el espacio material y virtual, para crear una ENCS y determinar los grados de impacto de una ciberagresión.

En México, la ENCS es ambigua y confunde la disminución de la brecha digital entre la población con la necesidad de poseer una política de ciberseguridad y el desarrollo de capacidades de resiliencia. Es necesario crear un organigrama de responsabilidades y atribuciones de las instituciones públicas y privadas encargadas de la ciberseguridad y homologar las legislaciones nacionales vinculadas al ciberespacio. El gobierno mexicano debe aprovechar la disposición de la industria privada para crear una Agencia Nacional de Ciberseguridad, a la par de actualizar su catálogo de INC, con división de responsabilidades de su administración entre entidades públicas y privadas.

La propuesta de análisis de los hechos ciberfísicos sirve para comprender cómo una amenaza surgida en el ciberespacio se traslada al espacio físico, y viceversa. También ayuda a delimitar las partes interesadas que construyen una ENCS efectiva, los niveles y esferas de impacto, y los tipos de clasificaciones para los diferentes ciberataques. Después de la revisión de los cinco casos seleccionados, se considera que la propuesta se ajusta al análisis de los ataques al SPEI en México (2018), y puede ser replicada a otro estudio de caso en materia de ciberseguridad.

Bibliografía

Auoragh, Miriyam. 2012. "Social Media, Mediation and the Arab Revolutions." *TripleC* 10 (2): 518-36.

Bachrach, Judy. 2011. "Wikihistory: Did the Leaks Inspire the Arab Spring?". *World Affairs* 174 (2): 35-44.

BBC News. 2007. "Tallinn tense after deadly riots". 28 de abril, http://news.bbc.co.uk/2/hi/europe/6602171.stm

Beck, Ulrich. 1998. *¿Qué es la globalización?* Barcelona: Paidós.

Benítez, Raúl. 2005. "Defensa y seguridad hemisférica hacia el siglo XXI: el desafío de la cooperación multinacional". En *Seguridad Hemisférica: debates y desafíos*, editado por Raúl Benítez, 11-31. México: UNAM/CISAN.

Buzan, Barry, Ole Waever, y Jaap de Wilde. 1998. "Security: A New Framework for Analysis". Boulder: Lynne Rienner.

Calderón, José. 2018?. "Infraestructura crítica en México: el enfoque hacia el futuro", 3 de mayo, https://bit.ly/2KBqepW

Cornaglia, Silvina, y Ariel Vercelli. 2017. "La ciberdefensa y su regulación legal en Argentina (2006-2015)". *Urvio. Revista Latinoamericana de Estudios de Seguridad,* 20: 46-62. doi.org/10.17141/urvio.20.2017.2601

Curtis, Simon. 2011. "Global Cities and the Transformation of the International System". *Review of International Studies* 37 (4): 1923-1947.

Demchak, Chris. 2012. "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure." *Journal of Comparative Policy Analysis: Research and Practice* 14 (3): 254-269.

Detlefsen, William. 2015. *Cyber Attacks, Attribution, and Deterrence: Three Case Studies.* Leaventh: US Army Command and General Staff College.

DiSanto, Philip. 2015. "Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud". *Columbia Law Review* 115 (4): 941-82.

ENCS (Estrategia Nacional de Ciberseguridad) de México. 2017. 31 de mayo de 2019, https://bit.ly/2AEvAtU

Espinosa, Iván. 2015. "Hacia una estrategia nacional de ciberseguridad en México". *Revista de Administración Pública* 50 (1): 115-147.

Estañol, Adrián. 2018. "La aseguradora AXA sufre un ciberataque en el Sistema de Pagos Electrónicos". *Expansión,* 23 de octubre, https://expansion.mx/empresas/2018/10/23/axa-sufre-un-ciberataque-en-el-spei

Farrell, Henry, y Martha Finnemore. 2013. "The End of Hypocrisy: American Foreign Policy in the Age of Leaks". *Foreign Affairs* 92 (6): 22-26.

Finn, Peter. 2007. "Protesters in Moscow Harass Estonian Envoy Over Statue". *The Washington Post*, 3 de mayo, https://wapo.st/2Kv0Y61

García, Arturo. 2018. *Ciber México: voluntades y acciones en el ciberespacio*. S.l.: IUS Ediciones.

Gómez Navarro, Dulce Angélica, Raúl Arturo Alvarado López, Marlen Martínez Domínguez, y Christian Díaz de León Castañeda. 2018. "La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México". *Entreciencias: Diálogos en la Sociedad del Conocimiento* 6 (16): 49-64.

Hansen, Lene, y Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53 (4): 1155-1175.

Hoerder, Dirk. 2010. "Recent Methodological and Conceptual Approaches to Migration: Comparing the Globe or the North Atlantic World?". *Journal of American Ethnic History* 29 (2): 79-84.

Hughes, Rex. 2010. "A Treaty for Cyberspace". *International Affairs* 86 (2): 523-541.

INEGI (Instituto Nacional de Estadística y Geografía). 2018. "Comunicado de Prensa Núm. 105/18". https://bit.ly/2MWpoab

Keeling, David. 2004. "Latin American Development and the Globalization Imperative: New Directions, Familiar Crises". *Journal of Latin American Geography* 3 (1): 1-21.

Kello, Lucas. 2013. "The meaning of the Cyber Revolution: Perils to Theory and Statecraft". *International Security 38* (2): 7-40.

Klimburg, Alexander, y Jason Healey. 2012. "Strategic Goals and Stakeholders". En *National Cyber Security Framework Manual,* editado por Alexander Klimburg, 66-107. Tallin: NATO/CCD/COE.

Lara, Paul. 2018. "Atacaron al SPEI crackers norcoreanos, asegura firma de EU". *Excelsior,* 4 de octubre, https://bit.ly/2ySnW08

Langner, Ralph. 2013. "To Kill a Centrifuge-A Technical Analysis of What Stuxnet's Creators Tried to Achieve." Hamburgo: The Lagner Group.

Lindstrom, Gustav, y Eric Luiijf. 2012. "Political Aims & Policy Methods. En *National Cyber Security Framework Manual,* editado por Alexander Klimburg, 66-107. Tallin: NATO CCD COE.

Martínez, Ricardo. 2007. "Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE". *El País*, 18 de mayo, https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

Medcalf, Rory. 2011. "Diplomacia, transparencia y opinión pública". *Política Exterior* 25 (141): 114-121.

Nguyen, Reese. 2013. "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare". *California Law Review* 101 (4): 1079-129.

Norton. 2018. "Norton Cyber Security Insights Report Global Results", https://symc.ly/2G8VNnU

Nye, Joshep. 2010. *Cyber Power*. Cambridge: Harvard University Press.

OEA (Organización de los Estados Americanos). 2018. "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe", https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

OEA (Organización de los Estados Americanos) y Symantec. 2014. "Tendencias de Seguridad Cibernética en América Latina y el Caribe", https://symc.ly/2Ownq0i

PandaLabs. 2015. "Informe Anual 2014". https://bit.ly/2GYRy08

Parraguez, Luisa. 2018. "Quo Vadis? Mexico's National Cybersecurity Strategy", Wilson Center, 31 de mayo, https://bit.ly/2TpovYY

Pessiri, Paolo. 2019. "2018: A Year of Cyber Attacks". *Hackmageddon,* 15 de enero, https://bit.ly/2Da7k7d

Schmidt, Andreas. 2013. "The Estonian Cyberattacks". En *The fierce domain. Conflicts in cyberspace 1986-2012*, editado por Jason Healey, 168-193. Washington, D.C.: Atlantic Council.

Sidaway, James. 2006. "On the Nature of the Beast: Re-Charting Political Geographies of the European Union". *Geografiska Annaler. Series B, Human Geography* 88 (1): 1-14.

Tamkin, Emily. 2017. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?". *Foreign Policy*, 27 de abril, https://bit.ly/2HCvY4H

Taylor, J. Peter. 1996. "Embedded Statism and the Social Sciences: Opening up to New Spaces". *Environment and Planning* 28 (11): 917-928.

Thaw, David. 2013. "Criminalizing Hacking, Not Dating: Reconstructing The CFAA Intent Requirement". *The Journal of Criminal Law and Criminology (1973-)* 103 (3): 907-948.

UIT (Unión Internacional de Telecomunicaciones). 2014. "Índice mundial de ciberseguridad y perfiles de ciberbienestar", https://bit.ly/2H0e6xL

Valdelamar, Jassiel. 2018. "5 entidades y 300 mdp, involucrados en ciberataque: Banxico". *El Financiero,* 16 de mayo, https://elfinanciero.com.mx/economia/5-entidades-fueron-afectadas-por-ciberataque-banxico

Van Wijk, Joris, y Maarten Bolhuis. 2017. "Awareness Trainings and Detecting Jihadists among Asylum Seekers: A Case Study from The Netherlands". *Perspectives on Terrorism* 11 (4): 39-49.