ALGUNAS CONSIDERACIONES DE LA CRIMINALIDAD ELECTORAL COMETIDA POR CIBERATAQUES COMO EXPRESIÓN DE LA SEGURIDAD INTERIOR MEXICANA

Israel Alvarado Martínez*
Nelly Montealegre Díaz**

*Profesor investigador invitado del INACIPE.
**Maestra en Administración de Justicia por el INACIPE.

PALABRAS CLAVE *KEYWORDS*

Resumen. El proceso electoral de 2018 será el más grande de la historia reciente en el país, lo cual genera importantes retos en la procuración de justicia y la efectiva investigación de los delitos electorales.

Además de ello, con los avances tecnológicos, las actuales elecciones se apoyan en el uso de redes informáticas que pueden ser susceptibles al fenómeno delictivo del ciberataque. Es por eso que el presente artículo hace un análisis sobre el fenómeno delictivo cibernético y los focos que deben ser atendidos a fin de blindar las elecciones de 2018 de dicho fenómeno

Abstract. The 2018 electoral process will be the biggest event in recent history in the country; this generates significant challenges in the pursuit of justice and the effective investigation of electoral crimes.

In addition, with technological advances, the current elections rely on the use of computer networks that may be susceptible to the criminal phenomenon of cyber attack. That is why this article analyzes the cybernetic crime phenomenon and the issues that must be addressed in order to shield the 2018 elections of the phenomenon mentioned.

SUMARIO:

INTRODUCCIÓN

En un primer apartado se hace cargo de establecer lo que se entiende por ciberataques, para que en un segundo momento se señalen tanto aspectos generales, como peculiaridades de las expresiones de la criminalidad electoral que puede cometerse a través de la *web*.

En el tercero de los apartados se aborda el planteamiento de que la seguridad nacional tiene como una de sus expresiones a la seguridad interior, y los antagonismos que se presenten contra la estabilidad democrática y el Estado de Derecho derivados de los ciberataques, además de ser expresiones criminales que se encuentran en el terreno de la seguridad pública, constituyen expresiones que vulneran la seguridad interior.

Dentro del apartado cuarto se presentan reflexiones sobre los principales problemas que presentan los ciberataques en la comisión de delitos electorales, tanto del orden tecnológico como de tipo jurídico-procesal.

En el apartado quinto presentamos algunas propuestas específicas para mejorar el *statu quo* del tema en cuestión.

I. LOS CIBERATAQUES

Existen múltiples y constantes ataques procedentes del ciberespacio a los sistemas de seguridad de la información de gobiernos, empresas, instituciones del sistema financiero, infraestructura crítica de servicios y de información, es decir, no existe ningún sistema que pueda ser protegido al 100 %, y si a ello le sumamos los intereses e información que pueden verse comprometidos con su vulneración, el riesgo y las capacidades que se requieren para su protección constituyen un desafío en el que no deben escatimarse recursos, y mucho menos incurrir en el exceso de confianza, ya que eso puede hacernos más vulnerables.

La Organización del Tratado del Atlántico Norte (OTAN), establece que los ciberataques son elementos de la *guerra híbrida*, al considerar que las amenazas cibernéticas desafían las fronteras estatales y organizacionales. De ahí que en su glosario de términos 2014, los define como: «la acción tomada para interrumpir, denegar, degradar o destruir la información residente en una computadora y/o red informática, o la computadora y/o la red informática en sí».

Un ejemplo de lo que podría ser un ciberataque en el ámbito electoral lo tenemos en las elecciones presidenciales de los EE UU. Según lo manifestaron el Buró Federal de Investigación, (FBI, por sus siglas en inglés) y la Agencia Central de Inteligencia (CIA, por sus siglas en inglés), «Rusia interfirió en las elecciones presidenciales… con el objetivo de apoyar al candidato republicano, Donald Trump», por la antipatía que al Kremlin y al presidente Vladimir Putin les generaban «Bill y Hillary Clinton, y

por la certeza de que si la exsecretaria de Estado ganaba las elecciones sería más inflexible con cuestiones relacionadas con los derechos humanos».

Desde que se «oficializó» esta intervención rusa en los comicios norteamericanos, el presidente Obama ofreció tomar «represalias contra Rusia por su supuesta intromisión cibernética en las elecciones presidenciales», acusación que el Kremlin ha negado sistemáticamente, pues según Obama solicitó a Putin poner fin a sus ciberataques.

Tales «represalias» del gobierno estadounidense no se hicieron esperar y, finalmente se anunció la expulsión de «35 "operativos de inteligencia rusos"», dándoles tan solo 72 horas para «abandonar el país a estos "diplomáticos" "non gratos" de la embajada de Washington y el consulado de Los Angeles (California)».

Adicionalmente, las reacciones se dirigieron a:

> …cinco entidades rusas: los servicios de inteligencia GRU (servicios secretos militares rusos) y FSB (el Servicio Federal de Seguridad), y tres empresas que les proveían de materiales. Cuatro oficiales de la principal agencia de espionaje también han sido sancionados. Además, la Administración Obama ha acordado el cierre de dos centros "recreativos" en Maryland y Nueva York propiedad del Gobierno ruso (Adalid, 2018).

II. EXPRESIONES DE LA CRIMINALIDAD ELECTORAL QUE PUEDEN COMETERSE A TRAVÉS DE LA *WEB*

A. ASPECTOS GENERALES

La próxima jornada electoral del 1º de julio, en particular la elección del próximo presidente de la República, coloca a México de cara a un momento decisivo para su desarrollo, no solo se trata de definir quién nos gobernará los próximos seis años, sino cuáles serán las relaciones que marcarán el desarrollo del Estado mexicano, es decir, si consideramos que la comunidad internacional enfrenta desafíos políticos, económicos, sociales, ambientales y tecnológicos, que de acuerdo con la opinión de expertos solo pueden enfrentarse mediante la colaboración pública-privada global, entonces la decisión que tome la población mexicana con su voto, definirá también la manera en la que se atenderán esos desafíos.

Se buscará influir en el ánimo de las personas que voten, tanto a favor como en contra, y es ahí donde entrarán al escenario nuevo elementos.

En principio podemos señalar a los actores no estatales cuyas conductas pueden tener diversas expresiones que impacten en los comicios, entre ellas las maniobras que pueden desplegar a través de medios electrónicos, los ataques a la ciberseguridad de las entidades relacionadas con las elecciones, campañas de las llamadas *fake news* (noticias falsas) y la filtración de correos electrónicos de la cuentas de funcionarios en veda electoral, entre otros.

Si consideramos el radar y la brújula que refiere Klaus Schwab (2017) bajo el contexto del orden internacional, resultado de los procesos electorales de otras naciones y las experiencias de procesos electorales recientes, se debe ponderar en los aspectos de organización y coordinación del proceso electoral, a quién o quiénes corresponde la responsabilidad de proteger la integridad de

la infraestructura del sistema electoral incluida la protección del ciberespacio, infraestructura que en mucho se parece a las denominadas *Infraestructuras Críticas* (IEC) (Arvizu, 2018), si es que no se quisiera reconocerse esa característica.

Al respecto, resultan diversos elementos de valoración, por un lado la aún no esclarecida y probable injerencia de agentes externos en el pasado proceso electoral presidencial de los Estados Unidos a la que ya nos hemos referido.

En este sentido, resulta interesante lo manifestado recientemente por la eurodiputada Teresa Jiménez Becerril, en su visita a México en la que señaló que: «uno de los peligros que desestabilizan la situación geopolítica actual son los ataques cibernéticos de Rusia en campañas electorales», así como la actual polarización política que vive el país y el desencanto social.

El impacto en los procesos electorales de la posible injerencia de actores no estatales y su potencial direccionamiento en la geopolítica mundial han llevado a otros organismos como la OTAN a crear instituciones para su específica atención. Prueba de ello es el recientemente puesto en marcha Centro Europeo de Excelencia contra las Amenazas Híbridas (Hybrid CoE), que buscará respuestas ante los ciberataques y la propaganda, y que tiene como objetivo ayudar a mejorar sus capacidades civiles y militares, su resiliencia y su preparación para contrarrestar las *amenazas híbridas*, a las que el Secretario General de la OTAN, Jens Stoltenberg, definió como «cosas distintas combinadas, desde la propaganda y la desinformación hasta el uso de fuerzas regulares, desde los "tuits" hasta los tanques» (Galán, 2018).

Lo anterior avizora que en el escenario del próximo proceso electoral en México no podemos descartar las referidas amenazas híbridas que pudiesen presentarse como conductas de criminalidad electoral —expresión clara del ámbito de la seguridad interior, como expresión de la seguridad nacional mexicana— entre ellas las campañas de desinformación, la influencia de las personas con pareceres similares a líderes de opinión a través de campañas en redes sociales o el ataque a los sitios *web* de actores en el proceso electoral, por solo poner algunos ejemplos.

Lo antes expresado cobra actualidad en términos de lo que señalan algunos órganos especializados en ciberseguridad como la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA, por sus siglas en inglés), que en su *Informe de Amenazas 2017*, señalan que de acuerdo al contexto electoral actual, quizá podrían presentarse los ataques tanto a los sitios *web* como a las aplicaciones, denegación del servicio del sitio *web*, la fuga de información y el espionaje cibernético.

B. PECULIARIDADES DE LOS CIBERATAQUES EN EL PROCESO ELECTORAL MEXICANO COMO EXPRESIONES DE LA CRIMINALIDAD ELECTORAL

Debemos tener en consideración que, derivado de la «presunta» intervención rusa en los comicios del vecino del norte, tres senadores norteamericanos

(uno republicano y dos demócratas) dirigieron una misiva «al secretario de Estado, Rex Tillerson, para pedirle que proteja de la posible injerencia rusa las elecciones presidenciales en México». Señalaron que se encontraban «profundamente preocupados por recientes artículos de prensa que dicen que Rusia está usando tecnología sofisticada para mediar en las próximas elecciones en México», y lo exhortaron a «tomar más en cuenta la importancia de los sistemas electorales fuertes e independientes de México y América Latina».

Por su parte, en México, Benito Nacif, Consejero del INE, ha manifestado que en virtud de que «ningún partido ha presentado ante el árbitro electoral alguna queja o denuncia por el presunto ilícito a fin de que el INE emprenda una indagatoria», ese órgano electoral «no ha abierto ninguna investigación por la supuesta injerencia del Gobierno de Rusia en el proceso electoral en curso».

Ya nos hemos referido a la posibilidad de intervención de los actores no estatales mediante actos de ciberataque en los comicios de 2018 —julio— estos agentes no estatales de alta capacidad en el ciberespacio podrían ser de índoles muy diversas, por lo que centraremos el estudio en las *amenaza* generadas por *actores no estatales* —servidores públicos—, ni candidatos o funcionarios partidistas o electorales, tan solo el grueso de la población no calificada que pueda poseer las referidas capacidades, ya sea que se encuentren en el territorio nacional o fuera de él.

De tal suerte que, si consideramos lo establecido por la Ley General en Materia de Delitos Electorales, en particular lo señalado por los art. 7°, fracciones III, IV, VII, XI, XV y XVI; 13, fracciones I y II y 19, fracción I, a la luz de lo hasta aquí dicho, no resulta difícil imaginar un escenario complejo y negativo que tenga a los ciberataques en el corazón de la comisión de diversas conductas delictivas de tipo electoral.

Piénsese para el caso del primero de dichos artículos —el 7°— que las conductas que podrían resultar relevantes y susceptibles de ser cometidas mediante los ciberataques, son las siguientes:

1. Hacer proselitismo o presionar objetivamente a los electores el día de la jornada electoral en el lugar en que se encuentren formados los votantes, con el fin de orientar el sentido de su voto o para que se abstengan de emitirlo;
2. Obstaculizar o interferir el desarrollo normal de las votaciones, el escrutinio y el cómputo;
3. Solicitar votos mediante una amenaza; apoderarse, destruir, alterar, poseer, usar, adquirir, vender o suministrar de manera ilegal, en cualquier tiempo, materiales o documentos públicos electorales;
4. Publicar o difundir por cualquier medio los resultados de encuestas o sondeos de opinión que tengan por objeto dar a conocer las preferencias electorales de los ciudadanos durante los tres días previos a la elección y hasta la hora del cierre oficial de las casillas que se encuentren en las zonas de husos horarios más occidentales del territorio nacional, y
5. Realizar por cualquier medio algún acto que provoque temor o intimidación en el electorado que atente

contra la libertad del sufragio, o perturbe el orden o el libre acceso de los electores a la casilla.

Para el caso del art. 13, las conductas relevantes son alterar o participar en la alteración del Registro Federal de Electores, el Padrón Electoral o el Listado de Electores; así como alterar, falsificar, destruir, poseer, usar, adquirir, comercializar, suministrar o transmitir de manera ilegal, archivos o datos de cualquier naturaleza, relativos al Registro Federal de Electores, Padrón Electoral o Listado de Electores, en tanto que para el caso del último de los artículos, obstaculizar o interferir el escrutinio y cómputo de la consulta popular son conductas que podrían ser cometidas por un ciberataque.

Para estos casos, las punibilidades previstas van de los cincuenta a los doscientos días multa y de seis meses a siete años de prisión.

III. LA CRIMINALIDAD ELECTORAL COMO PROBLEMA DE SEGURIDAD INTERIOR

Según dispone el art. 2° de la Ley de Seguridad Interior, la seguridad interior es:

> La condición que proporciona el Estado mexicano que permite salvaguardar la permanencia y continuidad de sus órdenes de gobierno e instituciones, así como el desarrollo nacional mediante el mantenimiento del orden constitucional, el Estado de Derecho y la gobernabilidad democrática en todo el territorio nacional. Comprende el conjunto de órganos, procedimientos y acciones destinados para dichos fines, respetando los derechos humanos en todo el territorio nacional, así como para prestar auxilio y protección a las entidades federativas y los municipios, frente a riesgos y amenazas que comprometan o afecten la seguridad nacional en los términos de la presente Ley.[1]

Resalta en su definición el componente de la *gobernabilidad democrática* y el Estado de Derecho, que se traducen en intereses nacionales que permiten la integridad, estabilidad y permanencia del Estado mexicano, como expresiones de la seguridad nacional, regulada esta en el art. 3° de la Ley de Seguridad Nacional, lo que se encuentra además en concordancia con la fracción VI del art. 89 constitucional.

En este orden de ideas, el Estado mexicano debería estar consciente de la problemática que los ciberataques representan a la seguridad interior —y por consiguiente a la seguridad nacional— de México y desarrollar una Política Nacional de Defensa[2] que

[1] En términos doctrinales, se entiende como la «condición necesaria que proporciona el Estado para salvaguardar sus instituciones [y] su población», así como para «garantizar el desarrollo nacional y mantener el estado de derecho». Véase, Colegio de Defensa Nacional y Centro de Estudios Superiores Navales, *Glosario de términos unificados de Seguridad Nacional*, *Op. cit.*, voz: «seguridad interior». Por su parte, el Diccionario LID inteligencia y seguridad la define como el «conjunto de estrategias, decisiones y medidas diseñadas y puestas en marcha por instituciones relacionadas con la seguridad principalmente, con la finalidad de proteger las estructuras políticas, sociales y económicas de un país frente a desafiadores internos o externos», véase Antonio M., Díaz Fernández, *Diccionario LID inteligencia y seguridad*, Ministerio de la Presidencia, Gobierno de España/LID, Madrid 2013, p. 233, voz: «seguridad interior».

[2] Entendida como el «conjunto de principios y criterios con que el Estado orienta su función de defensa, con vistas a preservar la integridad, la independencia y la

contemple la defensa del ciberespacio, valiéndose de la inteligencia geoespacial que permita «hacer uso de la ciencia y la tecnología de gestión de la información geoespacial, incluyendo la adquisición, almacenamiento, análisis y procesamiento, exhibición y difusión de información georreferenciada»[3] como estrategia nacional que permita actuar tanto a nivel estratégico, como operacional y táctico.

Debemos estar conscientes de que la prevención de este tipo de actividades solo podrá realizarse a través del «estudio y análisis permanente de los posibles escenarios nacionales e internacionales para anticipar sus impactos en la seguridad y defensa de la Nación, adquiriendo un alto grado de certidumbre para prever y decidir respecto a la ocurrencia»[4] de los posibles escenarios, pues los impactos a las áreas estratégicas, tanto geográficas como funcionales, podrían ser muy elevados, sobre todo si tenemos en cuenta que podría tratarse de un problema interméstico, como los hipotéticos ataques rusos en nuestras elecciones próximas.

En este orden de ideas, la problemática hasta aquí señalada trasciende el ámbito tradicional de la seguridad pública y entra, también, en el terreno de la seguridad interior, por lo que la actuación de las autoridades del sistema de justicia penal, incluso las especializadas en materia electoral, resultan insuficientes, pues se encuentran dirigidas a la prevención, investigación, persecución, procesamiento y ejecución en el ámbito delictivo,[5] mas no de tipo securitario nacional.

Consecuentemente, y como ya hemos señalado, la Política Nacional de Defensa del ciberespacio debería implicar acciones de seguridad interior a cargo las autoridades federales (tanto Fuerzas Federales como Fuerzas Armadas)[6] y acciones de seguridad nacional a manos de las instancias encargadas de la Seguridad Nacional,[7] las que deberían estar orientadas a «identificar, prevenir, atender, reducir y contener riesgos y amenazas a la seguridad interior».[8]

IV. PROBLEMAS QUE PRESENTAN LOS CIBERATAQUES EN LA COMISIÓN DE DELITOS ELECTORALES

Uno de los grandes desafíos de los ciberataques lo constituye su investigación, aunado a que carecemos de un marco jurídico robusto para su prevención y eventual sanción. Pero las mayores limitantes corresponden a factores exógenos, es decir, tienen como origen la complejidad del ataque como tal y

soberanía de la nación; garantizar la seguridad interior y contribuir al desarrollo nacional». *Vid.* Colegio de Defensa Nacional y Centro de Estudios Superiores Navales, *Glosario de términos unificados de Seguridad Nacional*, *Op. cit.*, voz: «política nacional de defensa».

[3] *Ibídem.*, voz: «inteligencia geoespacial».

[4] *Ibídem.*, voz: «prevención».

[5] *Cfr.*, Alvarado Martínez, Israel, «La respuesta gubernamental ante el problema de la inseguridad», *Salud pública de México*, Edición Especial, vol. 49, 2007.

[6] Según lo establecido en el art. 4°, fracción II de la *Ley de Seguridad Interior*.

[7] En términos de lo preceptuado por el Título Segundo de la *Ley de Seguridad Nacional*.

[8] *Vid.*, art. 4°, fracción II de la *Ley de Seguridad Interior*.

sobre todo la sofisticación y los avances en las capacidades de los agentes.

Si bien la primera herramienta de la que se valen quienes realizan ataques de esta naturaleza es la del anonimato, son las referidas capacidades las que los hacen buscar mayores espacios de penetración y de protección. Al respecto, el referido informe de la ENISA, señala que dentro de las técnicas más utilizadas para los ataques se encuentran la imitación de origen, la imitación de intención, las pantallas de humo, los segmentos de código, y la encriptación.[9] Lo anterior, sin duda coloca en una desventaja a los investigadores, que deben acudir al esfuerzo colaborativo nacional e internacional para la protección.

El Estado mexicano ha desarrollado amplias capacidades en materia de ciberseguridad, las cuales deben colaborar en la protección del proceso electoral, y el diseño con prospectiva de planeación estratégica le permitirá tener las mejores herramientas.

Lo cierto es que la posibilidad de que algunos de los riesgos mencionados se actualicen —y se conviertan en amenazas— es latente, por lo que debemos estar preparados para cualquier ataque procedente de agentes no estatales de alta capacidad en el ciberespacio.

Pero en términos de seguridad pública, vinculados a la categoría de la criminalidad electoral, el panorama tampoco es halagüeño.

La determinación de la competencia espacial, la aplicación de una normatividad específica, la complejidad criminalística y probatoria, la dificultad demostrativa mediante estrategias de litigación y la identificación de los imputados, son solo algunos de los problemas que presentan los ciberataques en la comisión de delitos electorales.

Si bien la normatividad aplicable[10] dispone la competencia en favor de la federación para investigar, perseguir y sancionar los delitos electorales cuando se inicien, preparen o cometan en el extranjero, siempre que produzcan o se pretenda que produzcan efectos en el territorio nacional, la ubicación de los países donde se desplieguen las conductas podría estar indeterminado por desconocerse, puesto que al ser utilizada la *Dark web* o *Deep web*, la información con la que se cuente podría ser limitada por el uso de servidores *proxy* o VPN que impiden el rastreo de la navegación de un usuario, el cambio frecuente de dominios y el uso de combinaciones alfanuméricas aleatorias.

A pesar de la existencia de normas específicas en materia de procuración de justicia penal electoral (como el art. 24, fracción IV de la referida Ley General

[9] Las 15 amenazas y sus tendencias que se identifican en el informe son: (i) el *malware*, (ii) los ataques basados en *web*, (iii) los ataques de aplicaciones *web*, (iv) el *phishing*, (v) la denegación de servicio, (vi) el *ramsomware*, las *botnets*, (vii) la amenaza interna, (viii) la manipulación física/daños/robo/pérdida, (ix) el incumplimiento de datos, (x) el robo de identidad, (xi) la fuga de información, (xii) el *software* diseñado para ejecutarse en servidores *web*, (xiii) con el objetivo de identificar vulnerabilidades, (xiv) el *spam* y (xv) el espionaje cibernético. European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2017… Op. cit.*, , p. 09, disponible en: [https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017], consultado el 23 de febrero de 2018.

[10] Art. 2°, fracción I del Código Penal Federal; 50, fracción I, inciso b) de la Ley Orgánica del Poder Judicial de la Federación y 21, fracción III de la Ley General en Materia de Delitos Electorales.

en Materia de Delitos Electorales), que imponen la obligación a la Fiscalía Especializada en materia de Delitos Electorales de la PGR, para establecer los protocolos estandarizados para la Federación y las entidades federativas en materia de investigación y persecución de los delitos electorales, incluyendo incluso el uso de la fuerza pública, estos no existen en materia de ciberseguridad.

V. PROPUESTAS

Ante la problemática que hemos señalado, proponemos las siguientes estrategias y líneas de acción:

- Desarrollar una Política Nacional de Defensa del ciberespacio que abarque la protección de los diferentes procesos electorales que se llevan a cabo en el país.
- Fortalecer los mecanismos de coordinación para la atención a incidentes de seguridad cibernética entre todas las instancias de gobierno que tengan injerencia en materia de ciberseguridad.
- Impulsar el cumplimiento y el desarrollo de procedimientos para evaluar y fortalecer el funcionamiento de los equipos de respuesta a incidentes de ciberseguridad en el ámbito del ejecutivo federal.
- Establecer esquemas cooperación internacional en materia de ciberseguridad para prevenir y enfrentar ataques a los sistemas informáticos del país.
- Establecer protocolos estandarizados para la Federación y las entidades federativas en materia de investigación y persecución de los delitos electorales llevados a cabo mediante los ciberataques.
- Buscar la cooperación de agencias de otras naciones con experiencias previas en estos procesos electorales a fin de documentar y prever los escenarios de riesgos que se presentan en estos casos.
- Establecer una política pública para robustecer el sistema informático del Instituto Nacional Electoral, que por tratarse de la elección de los líderes políticos que van a guiar el rumbo de la nación, requiere que se le destine los recursos humanos materiales y financieros necesarios, para cumplir con el propósito de la elección.
- Desarrollar operaciones de ciberseguridad en México, previo, durante y posterior al proceso electoral para detectar posibles actores en territorio nacional, que pretendan afectar el proceso electoral a través del ciberespacio y que tengan en cuenta la inteligencia de las amenazas.
- Apoyarse en instituciones o empresas extranjeras para la identificación de posibles antagonismos que puedan afectar el proceso electoral del Estado Mexicano.
- Fortalecer los mecanismos de ciberseguridad en redes informáticas que van a ser utilizadas en el sistema del INE, con relación con *hardware* y *software*, actualizados y mecanismos de seguridad de última generación.
- Desplegar un enfoque holístico en la estrategia que incluya como actor principal a la sociedad y la iniciativa privada.
- Contratar empresas extranjeras pioneras en la implementación de mecanismos de seguridad en el ciberespacio,

para proporcionar seguridad al sistema del INE antes, durante y después, de ser necesario contratar hackers a través de las redes, recomendados por la CIA o la DIA.

- Capacitar a expertos en seguridad en el ciberespacio, ciberguerra y ciberseguridad en el extranjero, para poder enfrentar las problemáticas globales en el ciberespacio.
- La conformación de un grupo multidisciplinario e interinstitucional de expertos en ciberseguridad.
- La conformación de Fuerzas de tarea conjuntas que den respuesta a riesgos comunes en materia de ciberseguridad.
- Desarrollar líneas de acción para capacitar y adiestrar especialistas en contra de ciberataques que pretendan alterar los resultados electorales en las elecciones presidenciales.

VI. BIBLIOGRAFÍA

Adalid, Carolina M., «EEUU expulsa a 35 agentes rusos de Inteligencia por injerencia en las elecciones presidenciales», *El Mundo*, 29 de diciembre de 2016, disponible en: [http://www.elmundo.es/internacional/2016/12/29/58656101ca474188338b461f.html], visitado el 23 de febrero de 2018.

Alvarado Martínez, Israel, «La respuesta gubernamental ante el problema de la inseguridad», *Salud pública de México*, Edición Especial, vol. 49, 2007.

Arvizu, Juan y Alberto Morales, «Advierte diputada europea de ataques cibernéticos rusos en campañas electorales», *El Universal*, 13 de febrero de 2018, disponible en: [http://www.eluniversal.com.mx/nacion/politica/advierte-diputada-europea-de-ataques-ciberneticos-rusos-en-campanas-electorales], consultado el 23 de febrero de 2018.

Colegio de Defensa Nacional y Centro de Estudios Superiores Navales, *Glosario de términos unificados de Seguridad Nacional*, Secretaría de la Defensa Nacional/Secretaría de Marina, México, 2016.

Díaz Fernández, Antonio M., *Diccionario LID inteligencia y seguridad*, Ministerio de la Presidencia, Gobierno de España/LID, Madrid 2013.

European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends*, enero 2018, Heraklion, Grecia, p. 09, disponible en: [https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017], consultado el 23 de febrero de 2018.

Evangelho de Araújo, Fabio, *Segurança das infraestruturas críticas de óleo e gás no Brasil: proposta para um programa de Estado*. Trabajo de conclusión del curso. Monografía presentada al Departamento de Estudios de la «Escola Superior de Guerra» como requisito para la obtención del diploma del «Curso de Altos Estudos de Política e Estratégia (CAEPE)», 2016, Rio de Janeiro, Brasil, 2016, disponible en [http://www.esg.br/images/Monografias/2016/ARA%C3%9AJO.pdf] , consultado el 23 de febrero de 2018.

Galán, Juanjo, «La OTAN y la UE inauguran en Helsinki un centro europeo

contra las amenazas híbridas», *Agencia EFE*, 02 de octubre de 2017, disponible en: [https://www.efe.com/efe/espana/mundo/la-otan-y-ue-inauguran-en-helsinki-un-centro-europeo-contra-las-amenazas-hibridas/10001-3396818], consultado el 23 de febrero de 2018.

Martín, Carolina, «Rusia interfirió "descaradamente" en las elecciones de EEUU, según el ex jefe de la CIA», El Mundo, 23 de mayo de 2017, disponible en: [http://www.elmundo.es/internacional/2017/05/23/59247283268e3e7b258b45b6.html], visitado el 23 de febrero de 2018.

NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Definitions*, Tallinn, Estonia, disponible en: [https://ccdcoe.org/cyber-definitions.html], consultada el 23 de febrero de 2018.

Raziel, Zedryk, «INE no indaga injerencia rusa», *Reforma*, 19 enero de 2018, disponible en: [https://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=1303631&md5=9fdabf310bc25f318d0b31ade2dd4f94&ta=0dfdbac11765226904c16cb9ad1b2efe], visitado el 23 de febrero de 2018.

Redacción, «Rusia interfirió en las elecciones de Estados Unidos para ayudar a Donald Trump, dice FBI. Presidente Obama advierte de que habrá represalias por esa piratería, que en Moscú rechazan», *La Nación*, 16 de diciembre de 2016, disponible en: [https://www.nacion.com/el-mundo/politica/rusia-interfirio-en-las-elecciones-de-estados-unidos-para-ayudar-a-donald-trump-dice-fbi/Q36FD4TUO5C7FPDFUWAAWKPB6M/story/], visitado el 23 de febrero de 2018.

Redacción, «Rusia interfirió en las elecciones de Estados Unidos para ayudar a Donald Trump, dice FBI. Presidente Obama advierte de que habrá represalias por esa piratería, que en Moscú rechazan», *La Nación*, 16 de diciembre de 2016, disponible en: [https://www.nacion.com/el-mundo/politica/rusia-interfirio-en-las-elecciones-de-estados-unidos-para-ayudar-a-donald-trump-dice-fbi/Q36FD4TUO5C7FPDFUWAAWKPB6M/story/], visitado el 23 de febrero de 2018.

Redacción, «Senadores piden al gobierno de Trump proteger a México de injerencia rusa», *El Universal*, 31 de enero de 2018, disponible en: [http://www.eluniversal.com.mx/mundo/senadores-piden-al-gobierno-de-trump-proteger-mexico-de-injerencia-rusa], visitado el 23 de febrero de 2018.

Schwab, Klaus, *Cinco prioridades de liderazgo para 2017*, World Economic Forum, 02 de enero de 2017, disponible en: [prhttps://www.weforum.org/es/agenda/2017/01/cinco-prioridades-de-liderazgo-para-2017/] consultado el 23 de febrero de 2018.

Souza de Carvalho, Regis de, *Proposta de arquitetura para coleta de ataques cibernéticos às infraestruturas críticas*, Instituto Militar de Engenharia, Río de Janeiro, Brasil, 2014, p. 14, disponible en: [http://www.defesacibernetica.ime.eb.br/pub/repositorio/2014_Regis_Carvalho.

pdf], consultada el 20 de febrero de 2018.
Ley General del Sistema Nacional de Seguridad Pública
Ley General en Materia de Delitos Electorales
Código Penal Federal
Ley de Seguridad Interior.
Ley de Seguridad Nacional
Ley Orgánica del Poder Judicial de la Federación