INSTITUTO DE INVESTIGACIONES
ESTRATÉGICAS DE LA ARMADA DE MÉXICO

DA 18/17

31/03/2017

Doctora
Patricia Trujillo

EL CIBERESPACIO, RECURSO Y RESPONSABILIDAD DE LOS ESTADOS.

RESUMEN:

Se establece una visión general del ciberespacio como un recurso del Estado y como tal, el cuidado del mismo, su impacto en el desarrollo económico de la nación, así como los nuevos modelos de negocio y comunicación a través del mundo virtual. Se mencionan las medidas que gobiernos, empresas y usuarios debieran adoptar para minimizar los riesgos y afectaciones ocasionados por el cibercrimen y los retos que en materia de ciberseguridad deben ser tomados en cuenta para evitar la vulnerabilidad del ciberterritorio.

PALABRAS CLAVE: ciberseguridad, ciberdelito, ciberdelincuencia, delitos electrónicos, ciberdelincuente, estrategia, retos.

ABSTRACT:

We can establish a general cyber space overview as a State´s resource and because of that, how careful the State must be, due to the impact of the virtual space in the economical development of the country thanks to new business models and communications existing in the net. Into the text, you will find security measures that government, enterprises and users of the net should take in order to minimize risks and affectations caused for cyber criminal organizations. In the same way you will encounter cyber security challenges that we have to face for preventing vulnerability into the virtual space, called cyber territory.

¿Por qué debemos cuidar el ciberespacio?

"Yo no creo que ninguno de nosotros puede hacer mucho por el rápido crecimiento de las nuevas tecnologías. Una nueva tecnología ayuda a impulsar la economía y cualquier discusión de frenar su crecimiento tiene que tener en cuenta las consecuencias económicas. Sin embargo, es posible que nosotros aprendamos a controlar nuestros propios usos de la tecnología."

Neil Postman

Hoy en día, el ciberespacio es considerado como un nuevo entorno operativo, tal como lo es el espacio terrestre, aéreo y marítimo. Las nuevas tecnologías y redes de comunicaciones propician que muchos sectores económicos, incluidos el sector gubernamental, basen su operación en esta red mundial. La Internet es utilizada por más de 3,600 millones de cibernautas alrededor del mundo[1]. Esto es cerca de la mitad de la población mundial. En México existen 65 millones de cibernautas, es decir 59% de los habitantes del país.[2]

Más de la mitad de nuestros ciudadanos utilizan la Internet como parte de su vida cotidiana para la comunicación, consulta de información e incluso para realizar la compra-venta de artículos o en operaciones financieras. Se resalta que el 51% de los internautas mexicanos son menores de 24 años de edad[3], lo que exige un ciberespacio más seguro. Y amerita a su vez, que los esfuerzos deban estar focalizados en entender el comportamiento de las nuevas generaciones.

El uso de Internet móvil se inició a finales de la década de los años 90´s. Desde entonces utilizaron tecnologías de datos móviles de baja velocidad como GPRS (General Packet Radio Service – Servicio General de Paquetes vía Radio) y EDGE (Enhanced Data Rates for Global System Mobile Comunication Evolution - Tasa de Datos Mejoradas para la Evolución del GSM). Estas, permitían aplicaciones básicas como correo electrónico, mensajes cortos multimedia, y una experiencia de navegación web muy elemental. Las tendencias de uso de datos móviles fueron crecientes en ese periodo. Sin embargo, fue hasta después de mediados de la década pasada que las conexiones de datos móviles empezaron a crecer dramáticamente con la aparición de nuevas terminales de usuario y la mejora en las velocidades de las redes. La reciente acometida de los teléfonos inteligentes o Smartphone son una fuerza clave en este significativo desarrollo del mercado de Internet móvil.

En el mundo en desarrollo, cada vez más países cuentan con accesos móviles de alta velocidad a Internet. Esto, impulsará aún más el número de usuarios de esta tecnología.

Queda de manifiesto así, la importancia de las comunicaciones móviles y el rol que juega el ciberespacio en la facilitación del acceso a Internet en países en desarrollo. Se están abriendo nuevas oportunidades para que el uso de las Tecnologías de la Información y las Comunicaciones (TIC´s) por el sector empresarial contribuya al desarrollo y la reducción de la pobreza[4].

[1] Fuente: International Telecommunications Union (ITU), ICT Indicators
[2] https://www.amipci.org.mx/images/Estudio_Habitosdel_Usuario_2016.pdf
[3] https://www.amipci.org.mx/images/Estudio_Habitosdel_Usuario_2016.pdf
[4] EL ESPECTRO RADIOELÉCTRICO EN MÉXICO. ESTUDIO ACCIONES

Con la evolución del Internet y de las TIC´S, se obtuvieron grandes beneficios para los ciudadanos, empresas y naciones enteras. Este desarrollo favoreció un escenario propicio para la expresión de una nueva forma de criminalidad: la ciberdelincuencia.

Los ciberdelincuentes procuran las circunstancias idóneas para atacar a través de técnicas que vulneren la seguridad informática y afecten diversos sectores de la sociedad. En algunos casos, no son necesarios grandes conocimientos de parte del delincuente para efectuar algún cibercrimen. Un dato importante al respecto es que las redes sociales, se expresan hoy en día como el principal medio de contacto para atraer víctimas de ilícitos como la pornografía infantil o la trata de personas.

Al respecto, el reporte del Foro Económico Mundial en el año 2016, expresó la necesaria implementación de estrategias de ciberseguridad para la protección de las infraestructuras críticas con la finalidad de evitar los ciberataques y el fraude o robo de datos. Siendo éstos eventos, riesgos globales que se ubican entre los primeros diez lugares de daño a nivel de la web[5].

En la última década se evolucionó a una sociedad "híper-conectada". Hoy, las personas viven conectadas de forma permanente a la información a través de diferentes dispositivos como la radio, la televisión, el internet y el teléfono celular.

El uso de las tecnologías de la información y la incorporación del Internet al mundo real, es sin duda un factor de desarrollo global. De ello deriva una nueva revolución industrial mediante la inclusión del concepto del "Internet de las Cosas". La 4ª Revolución así llamada por algunos, se incorporará a la industria en la producción, distribución y manejo de los productos, adaptando servicios a los clientes en cualquier parte del mundo.

De esta forma, surgen conceptos como "Ciudad Inteligente" (CI). La CI se caracteriza por el uso intensivo de las TIC´s en la creación o en el mejoramiento de los sistemas que componen la ciudad, para crear, recopilar, procesar y transformar la información que incida en mejores servicios, y con ello mejorar la calidad de vida mediante el uso eficiente de sus recursos.

Por estas razones, es de suma importancia proteger el ciberespacio. Más aún cuando, en los últimos años tomó auge el término Crimen como un Servicio (Crime as a Service, por sus nombre en inglés) que sustenta que el cibercrimen proporciona herramientas y servicios a través de todo el espectro de la delincuencia en Internet, a los atacantes cibernéticos de bajo perfil hasta terroristas cibernéticos.

Retos en materia de Ciberseguridad

[5] www.3weforum.org/docs/Media/The GlobalRisksReport2016.pdf

Los ciberdelincuentes evolucionaron desde el nacimiento de las TIC´S. Así, en la década de 1970, se inició con la experimentación e investigación de las nuevas tecnologías. Durante los años ochenta, nació el termino *hacker*[6]. Un hacker representó al principio a un individuo, que motivado por la curiosidad, vulnera la seguridad de la infraestructura tecnológica, ubica su actuar como un reto y su proceder se califica como una "intrusión benigna". Sin embargo, en los inicios del siglo XXI, surgen nuevos personajes anónimos llamados Script Kiddies (SK)[7], quienes intentan causar daños y hacerse famosos sin tener claridad en los objetivos de su quehacer. Su actitud se transforma, y en el año 2005, los SK se convierten en cibercriminales con objetivos específicos.

Los SK evolucionados poseen principalmente motivos comerciales, utilizan nuevas técnicas como el *phishing*[8], *malware*[9] y redes de *botnets*[10]. En 2010, ya son ciberatacantes profesionales, poseen equipos sofisticados y surgen en este mismo periodo los grupos *hacktivistas* con intenciones políticas y estratégicas. Por tanto, en los últimos años, se han generado estructuras de Ciberdelincuencia Organizada (CO). La CO realiza ataques y ejerce sus servicios mediante la utilización de métodos y herramientas sofisticadas.

Derivado de la expresión de la CO, la Policía Federal, bajo la instrucción de la Secretaría de Gobernación y la Comisión Nacional de Seguridad, desarrolló la Estrategia de Ciberseguridad (EC).

La EC tiene como objetivo principal hacer frente a la ciberdelincuencia. Su propósito es continuar con los esfuerzos del Gobierno de la República para lograr un México en Paz. Se encuentra por tanto, alineada al Plan Nacional de Desarrollo 2013-2018 y al Programa Nacional de Seguridad Pública 2014-2018.

6 Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

7 Un script kiddie es un inexperto que interrumpe en los sistemas informáticos mediante el uso de herramientas automatizadas pre-empaquetadas y escritas por otros

8 Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

9 Malware es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

10 Botnet es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

La EC, se sustenta en tres ejes principales:

- Dirigir acciones de prevención y atención de los delitos cibernéticos mediante la difusión masiva de información y orientación a la ciudadanía e instituciones públicas y privadas.

- Detección y atención oportuna de amenazas y ataques cibernéticos a fin de reducir, neutralizar o mitigar las afectaciones a la ciudadanía y los sectores económicos del país.

- Fortalecer las capacidades técnico-científicas para la investigación de delitos cibernéticos.

La Policía Federal como órgano desconcentrado de la Secretaría de Gobernación en México, cuenta en su estructura con siete Unidades Administrativas denominadas: Divisiones.

Una de ellas, es la División Científica, la cual cuenta con tres coordinaciones, una de ellas es la Coordinación para la Prevención de Delitos Electrónicos, la cual despliega funciones que la constituyen como la Unidad de Ciberseguridad (UC) de la Policía Federal. Esta Unidad lleva a cabo acciones de prevención e investigación de conductas ilícitas a través de medios informáticos, monitorea la red pública de Internet para identificar conductas constitutivas de delito y efectúa ciberinvestigaciones. Opera el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), el cual se encarga de vigilar la integridad de la infraestructura tecnológica estratégica del país.

El CERT-MX activa áreas especializadas en temas de prevención e investigación de delitos informáticos. Es la única instancia autorizada y acreditada a nivel federal para el intercambio de información con policías cibernéticas nacionales, organismos policiales internacionales y más de 360 equipos de respuesta a incidentes de seguridad informática del orbe. Dicha acción la realiza con el objetivo de identificar y atender posibles ataques en agravio de infraestructuras informáticas gubernamentales o contra la ciudadanía en general. Hoy cuenta con la certificación en el estándar internacional ISO/IEC 27001:2013 emitida por la British Standard Institution (BSI).

Ejemplo de algunas acciones realizadas a través de la Unidad de Ciberseguridad son:

- En 2016, la Policía Federal logró la detención de 5 presuntos integrantes de una red internacional de defraudadores cibernéticos. Es de destacar que se utilizaron técnicas de investigación novedosas que permitieron la captura de los sujetos relacionados con distintas carpetas de investigación así como averiguaciones previas.
- Así mismo, se realizó un operativo contra la Trata de Personas, derivado de los trabajos en coordinación con: la Fiscalía Especial para los Delitos de Violencia Contra las Mujeres y Trata de

Personas (FEVIMTRA) Organización Internacional de Policía Criminal (OIPC-INTERPOL) y el Inmigration and Custom Enforcement and Homeland Security Investigations (ICE-HSI) así como con las áreas hermanas de Gendarmería y la Coordinación de Criminalística. El esquema logró el aseguramiento de una banda delictiva, deteniendo a 10 sujetos relacionados a una red criminal.

- En materia de Pornografía Infantil, a lo largo de la administración 2013-2018, se logró la detención de 105 individuos. Ello, con la participación de las otras Divisiones de la Policía Federal en coadyuvancia con FEVIMTRA, INTERPOL, ICE-HSI.

Los eventos antes citados, sólo para resaltar algunos de los que tuvieron mayor impacto social.

Por otra parte, en término de retos en materia de ciberseguridad en nuestro país se destacan los que se aprecian de mayor importancia:

- Fortalecimiento de las acciones para generar una cultura en contra del cibercrimen en la ciudadanía así como en las empresas privadas y dependencias gubernamentales del país. Enfatizando en las poblaciones detectadas como de riesgo: niñas, niños, adolescentes, jóvenes y mujeres.
- Mejora en las capacidades de atención del cibercrimen mediante la implementación del Modelo de Policía Cibernética a nivel Nacional. Dicho instrumento, permitirá homologar y articular las capacidades del Estado Mexicano para hacer frente a los nuevos retos derivados del fenómeno del cibercrimen. Lo anterior para dar cumplimiento a las acciones definidas en el Programa Nacional de Seguridad Pública 2014-2018 que emana del Plan Nacional de Desarrollo 2013-2018.
- Cooperación Internacional que propicie, mejores respuestas en la prevención, contención e investigación de los delitos cibernéticos que se expresan a nivel global en el ciberespacio.
- Creación de un marco legislativo nacional en materia de delitos cibernéticos que permita brindar herramientas jurídicas para la prevención e investigación de los delitos cibernéticos.

Decálogo de Ciberseguridad

Para incrementar el nivel de seguridad de la información, a continuación se emiten una serie de recomendaciones generales.

1. Mantener actualizados los sistemas y aplicaciones de cómputo.

2. Utilizar contraseñas robustas con al menos 10 caracteres alfanuméricos y símbolos.

3. Emplear un doble factor de autenticación para servicios en línea, como las de correo electrónico y bancos.

4. Efectuar respaldos de manera periódica y guárdalos en discos externos.

5. No abrir documentos adjuntos y enlaces que vienen en correos de origen desconocido.

6. No generar depósitos antes de verificar que la operación sea legítima.

7. Desconfiar de correos y páginas con ofertas atractivas de artículos y servicios.

8. Comprobar el nivel de confiabilidad de los sitios web y la seguridad de su conexión (“https:// ”).

9. Configurar los parámetros de seguridad y privacidad en cuentas de correo electrónico y redes sociales.

10. Concientizar entre familiares, amigos y compañeros de trabajo la importancia de la seguridad de la información[11].

Conclusiones

En los siguientes años se ampliarán los servicios a través del Internet con el impulso del “Internet de las Cosas” y las “Ciudades Inteligentes”, lo que implicará nuevas amenazas y ataques en el ciberespacio. Por lo anterior, el fortalecimiento de las capacidades operativas para la prevención e investigación de los ciberdelitos representa un área de oportunidad para los gobiernos, quienes deberán establecer sus estrategias a fin de contrarrestar el fenómeno delictivo.

Existe un gran volumen de atacantes que no necesariamente usan técnicas avanzadas. Sin embargo, por la falta de prevención y concientización en ciberseguridad, se ven afectados un alto volumen de víctimas, con poca ganancia por ataque. Es decir, existe un alto volumen de ganancias obtenidas por la afectación a un alto volumen de víctimas, no obstante, dichas afectaciones se pueden prevenir a través de la concientización en materia de ciberseguridad.

Por otra parte, existen ciberdelincuentes más sofisticados que utilizan técnicas de intrusión innovadoras e ingeniería social para obtener ganancias en ataques dirigidos a víctimas con alto perfil

[11] Memorias del Coloquio “Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico”

económico, a través de los cuales logran obtener grandes beneficios económicos en un bajo volumen de víctimas.

En resumen, se establecen como retos en materia de ciberseguridad:

- Iniciativas que impulsen las capacidades en la investigación.
- Formación y desarrollo de fortalezas en ciberseguridad.
- Prevención como mecanismo de combate al cibercrimen.
- Cooperación nacional e internacional, y
- Armonización legislativa en la materia.

Es de suma importancia la asistencia legal mutua con otros países del orbe. Por ello, se considera valorar la importancia que tiene la adhesión de México al Convenio de Cibercriminalidad o Convenio de Budapest en términos de homologación legislativa a nivel internacional.

Lo anterior con la finalidad, de nivelar el camino a la investigación transfronteriza y se debe tener presente que la incursión de los cibercriminales, es una realidad que se incrementa día a día y que por tanto requiere una atención dinámica e integral.[12]

Finalmente, acorde con Neil Postman, si el*: 'Ciberespacio es una idea metafórica que se supone que es el espacio en el que se encuentra su conciencia cuando se está utilizando la tecnología informática a través de Internet…"* el cuidado que tengamos del mismo, reflejará el valor que le damos a nuestra propia seguridad.

[12] Memorias del Coloquio "Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico"