PROPOSICIÓN CON PUNTO DE ACUERDO, PARA EXHORTAR A DIVERSAS AUTORIDADES A FACILITAR LA COORDINACIÓN Y COMUNICACIÓN ENTRE LAS ÁREAS CON FUNCIONES DE CIBERSEGURIDAD DE DEPENDENCIAS Y ORGANISMOS FEDERALES, ANTE LA FALTA DE UN PLAN NACIONAL EN LA MATERIA, A CARGO DEL DIPUTADO JOSÉ SALVADOR ROSAS QUINTANILLA, DEL GRUPO PARLAMENTARIO DEL PAN

El suscrito, José Salvador Rosas Quintanilla, Diputado Federal del Grupo Parlamentario de Acción Nacional de la LXIV Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto por el artículo 6, numeral I, fracción I, y 79 del Reglamento de la Cámara de Diputados, someto a consideración de esta asamblea la presente proposición con punto de acuerdo por el que se exhorta a Alfonso Durazo Montaño, titular de la Secretaria de Seguridad y Protección Ciudadana, a Alejandro Gertz Manero, titular de la Fiscalía General de la República, a Luis Rodríguez Bucio, comandante de la Guardia Nacional, y a Luis Cresencio Sandoval González, Secretario de la Defensa Nacional, para facilitar la coordinación y comunicación entre las diversas áreas con funciones de ciberseguridad de dependencias y organismos federales, ante la falta de un plan nacional en la materia, la fragmentación de los esfuerzos para mitigar el problema y el incremento de la participación delictiva en el mundo digital, al tenor de las siguientes

Consideraciones

El salto tecnológico traído por la introducción de los computadores personales abrió una especie de "Caja de Pandora" al posibilitar a los usuarios un campo inexplorado por cualquier individuo, organización o gobierno. Con la puesta a disposición de casi cualquier persona de la población a un "mundo sin reglas", conocido por algunos periodistas digitales como la Wild West Web,[1] la posibilidad de crecimiento y desarrollo parecían ilimitadas, donde los sectores público y privado hicieron uso de estas plataformas para poder eficientar sus actividades y cumplir sus objetivos, mientras que los individuos comenzaron a tener acceso a información, fotografías, videos y demás productos audiovisuales, los cuales estaban previamente confinados a las colecciones personales o las bibliotecas públicas de unos cuantos países en el mundo.

Esta especie de utopía digital, si bien era utilizada para aspectos sumamente positivos, como la divulgación y la colaboración en línea, algunos sujetos y organizaciones comenzaron a emplearlo como una herramienta de seguimiento y espionaje de los usuarios. Sea un ciudadano de a pie o algún funcionario de mucha relevancia política, los usuarios han comprometido mucha de su información personal ante la fugaz adopción de estas herramientas en las últimas dos décadas, pero el nulo análisis de riesgos, respecto a la construcción de un perfil en línea y los mecanismos de seguridad existentes para proteger la información personal que los acompaña, ha derivado en un escenario donde las vulnerabilidades de sujetos e instituciones son tantas, que muchas de ellas no han sido posible de ser observadas hasta después de acontecimientos de gran magnitud en la materia. Igualmente, ante la falta de especialistas en el rubro, aquellos con conocimientos técnicos en la materia se han logrado posicionar, de manera legal o ilegal, en posiciones privilegiadas, logrando consolidar una industria multimillonaria que ha desbancado a la actividad petrolera como la más prolífera en nuestros tiempos, donde la frase "data is the new oil"[2] ha sido del gusto de muchos de los empresarios del ramo, lo que refleja el peso que éste tiene para un sector político y empresarial, más allá de si éste dicho es verdad o no.

Ante un atractivo como éste, dilucidar el presente panorama muestra una mayor cantidad de riesgos que de beneficios, los cuales se han ido canalizando y focalizando con el incremento de la intervención estatal en el mundo digital, debido a las exigencias sociales y éticas, al igual que las oportunidades económicas, que el mundo digital ha gestado en tiempos recientes.

Por tal motivo, resulta sorpresivo que el gobierno mexicano no haya logrado concentrar en un organismo las actividades en el rubro, donde las funciones se encuentran fragmentadas en diversos organismos, públicos o privados

(como la Policía Cibernética de la Comisión Nacional de Seguridad o los cuerpos de ciberseguridad de instituciones bancarias), que colaboran en hacerle frente a la problemática desde sus múltiples frentes, lo que denota una muy importante deficiencia en la materia, ya que la ciberseguridad es uno de los principales rubros para la protección de la seguridad nacional en un contexto de digitalización total de la vida cotidiana. Los problemas, explicitados por mí en exhortos anteriores, al igual que por legisladores de otras bancadas, como la iniciativa de Ley de Seguridad Informática de la Senadora Jesu?s Luci?a Trasvin?a Waldenrath de MORENA, presentada en marzo de 2019,[3] denotan un problema común observado por distintos frentes ante un vacío que no puede ser dejado de lado, ya que éstas tecnologías están permutando cada uno de los rincones de las actividades que realizamos, incluyendo las gubernamentales, al mismo tiempo que están cambiando a velocidades inconcebibles, donde los propios países desarrollados están encontrando problemas para mantenerse a la par de las exigencias en seguridad que el mundo digital demanda.

Las respuestas actuales, como los Equipos de Respuesta ante Emergencias Informáticas (CERT),[4] como el de la UNAM y la Policía Federal,[5] o la Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Público,[6] operan como paliativos ante un escenario que demanda una respuesta institucional de mucha mayor envergadura, que no solamente se enfoque a actividades de seguridad de manera reactiva, sino que comience a desarrollar código, tecnologías y métodos propios para nuestra seguridad de carácter preventivo, donde el hecho de depender del desarrollo de mecanismos de seguridad privados o extranjeros puede derivar en un escenario de mayor riesgo si alguno de los usuarios de estas herramientas es vulnerado, ya que los errores y debilidades se tornan compartidos al depender de los mismo instrumentos.

Sobre esto, facilitar la coordinación y comunicación entre las diversas áreas con funciones de ciberseguridad de dependencias y organismos federales, organizada por parte de la Secretaría de Seguridad y Protección Ciudadana, o de alguna otra secretaría, al igual que un órgano encargado de articularlo del lado del ejército, la Marina y las Fuerzas Armadas mexicanas, como la Secretaría de la Defensa Nacional, se vuelven opciones plausibles ante la falta de un plan claro en la materia y la inducción de programadores, usualmente conocidos como “hackers”, en las actividades delictivas del crimen organizado, ya sea por cuenta misma,[7] como el famoso caso del grupo “Bandidos Revolution Team” (conocidos por su intervención al SPEI en 2018), o por medio de los cárteles nacionales, donde existe evidencia de su participación con grupos como el Cártel de Sinaloa.[8]

Por ello, presento ante esta honorable asamblea, la siguiente proposición con

Punto de Acuerdo

Único. La honorable Cámara de Diputados exhorta a ?Andrés Manuel López Obrador, presidente de los Estados Unidos Mexicanos, a Alejandro Gertz Manero, titular de la Fiscalía General de la República, a Alfonso Durazo Montaño, titular de la Secretaria de Seguridad y Protección Ciudadana, a Luis Rodríguez Bucio, Comandante de la Guardia Nacional, y a Luis Cresencio Sandoval González, Secretario de la Defensa Nacional, para reconfigurar la red de telecomunicaciones militares, de la Policía Federal y la Guardia Nacional, para facilitar la coordinación y comunicación entre las diversas áreas con funciones de ciberseguridad de dependencias y organismos federales, ante la falta de un plan nacional en la materia, la fragmentación de los esfuerzos para mitigar el problema y el incremento de la participación delictiva en el mundo digital.

Notas

1 Sonia Livingstone. (2018). It's time to end the wild west of the web, 2 de diciembre de 2019, de London School of Economics. Sitio web:

https://blogs.lse.ac.uk/parenting4digitalfuture/2018/09/14/its-time-to-end-the-wild-west-of-the-web/

2 The Economist. (2017). The world's most valuable resource is no longer oil, but data, 2 de diciembre de 2019, de The Economist. Sitio web:

https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

3 Jesu?s Luci?a Trasvin?a Waldenrath. (2019). Que reforma y deroga diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática, 2 de diciembre de 2019, de Gaceta Parlamentaria. Sitio web: sil.gobernacion.gob.mx/Librerias/pp_ContenidoAsuntos.php?SID=9244d87beac0b562ae899ea2729229bd&Clave=3836691

4 Rodrigo Riquelme. (2018). ¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)?, 2 de diciembre de 2019, de El Economista. Sitio web: https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuest a-ante-Emergencias-Informaticas-CERT-20180122-0009.html

5 Ídem

6 Redacción Milenio. (2019). México y EU intercambian datos sobre ciberseguridad, 2 de diciembre de 2019, de Milenio. Sitio web: https://www.milenio.com/politica/comunidad/mexico-y-eu-intercambian-datos-sobre-ciberseguridad

7 Rubén Mosso. (2019). Así operaba el grupo de hackers detenidos en León, 2 de diciembre de 2019, de Milenio. Sitio web: https://www.milenio.com/policia/hackers-leon-operaba-cartel-bandidos-revolution-team

8 Redacción. (2019). Hackers reclutados por cárteles: la alianza delictiva en la red, 2 de diciembre de 2019, de La Silla Rota. Sitio web: https://lasillarota.com/nacion/hackers-reclutados-por-carteles-la-alian za-delictiva-en-la-red-hackers-beltran-levya/255890

Dado en el Palacio Legislativo de San Lázaro, a 11 de febrero de 2020

Diputado José Salvador Rosas Quintanilla (rúbrica)