Manzanillo, Col, 1 de diciembre de 2016.

Versión Estenográfica de la Conferencia sobre la Ciberseguridad como Asunto de Agenda Nacional, en el marco de los trabajos del 46 Foro de Autoridades de Privacidad Asia-Pacífico (Foro APPA), llevada a cabo en el Salón "Karmina", del Hotel Barceló Karmina Palace Deluxe en esta ciudad.

Presentador: Damos paso a la Conferencia sobre Ciberseguridad como Asunto Nacional.

Hará uso de la palabra el Coordinador Ejecutivo del INAI, José de Jesús Ramírez Sánchez.

Adelante, por favor.

Moderador, Lic. José de Jesús Ramírez Sánchez: Agradecemos la presencia de todos ustedes en esta interesante Conferencia denominada La Ciberseguridad como Asunto de Agenda Nacional.

La ciberseguridad es muy relevante para la salvaguarda de la privacidad, porque provee a los individuos la protección de la información digital que está en los sistemas interconectados como asuntos de seguridad nacional, pues estamos ante el tratamiento de datos personales y sensibles de los ciudadanos vinculados a las actividades de procuración o administración de justicia.

Por eso consideramos que lo que expondrá nuestro conferencista será un verdadero faro para los que estamos interesados en tan interesante temática.

Por lo tanto, sin más preámbulo, agradecemos la presencia del contralmirante Juan Carlos Vera Salinas, de la Secretaría de Marina.

El contralmirante es del Cuerpo General de Ingenieros en Ciencias Navales por la Heroica Escuela Naval Militar.

Ha efectuado las siguientes maestrías: Maestría en Administración Pública en el Instituto de Estudios Superiores en Administración Pública; Maestría en Cadena de Suministros y Logística en la Universidad de Cataluña, España; Maestría en Administración Naval en la Escuela de Guerra Naval de Uruguay; también la Maestría en Administración Militar de Operaciones Conjuntas y Combinadas en la Escuela de Guerra en París, Francia, y actualmente se encuentra cursando la Maestría en Administración Naval en el Centro de Estudios Superiores Navales de la Secretaría de Marina Armada de México.

Ha sido instructor en el Buque Escuela Velero Cuauhtémoc.

Sin más preámbulo, le damos la palabra al contralmirante Juan Carlos Vera Salinas.

Contralmirante Juan Carlos Vera Salinas: Muy buenas tardes.

Antes que nada, es para mí un gran honor estar ante distinguido foro.

Agradezco primeramente la atención que tuvo la doctora Ximena Puente de la Mora, Comisionada Presidenta del INAI.

Me siento muy honrado de estar enfrente de un auditorio tan selecto, conformado por académicos y funcionarios públicos a nivel mundial que se encuentran preocupados en la mejora de una de las seguridades más importantes del ser humano, como es la protección de la vida privada y de sus datos personales.

Sin más preámbulo, comienzo la exposición de mi tesis que fue presentada en el Colegio de la Defensa Nacional en 2014, en donde realicé la Maestría en Seguridad Nacional en el Colegio de Defensa Nacional.

Hay un polemologista de la guerra que dice que pronunciarse contra la guerra es batir el aire con sonidos huecos, pues tales medios no refrendan a los gobernantes ambiciosos, injustos o poderosos, o lo que es lo mismo, entregar el propio país reblandecido o desarmado; mejor dicho, malamente armado y desconociendo el empleo de las

armas a la esclavitud de las naciones guerreras, que pueden ser menos civilizadas, pero que cuentan con mayor criterio y prudencia.

Esto significa que desafortunadamente la guerra, como lo diría Clausewitz, siempre va a ser la continuidad de la política por otros medios. Se podría decir que es una cuestión inherente al ser humano.

De tal manera que para la presentación utilizaré el siguiente esquema, la introducción, un marco teórico del ciberespacio, los conflictos en el ciberespacio, las Fuerzas Armadas en el ciberespacio, dos cibercomandos, las conclusiones y las recomendaciones.

Primeramente, antes de poder continuar, quisiera poner esta diapositiva en la que está el Estado Mexicano, que según las teorías del Estado, se conforma por territorio, población y un gobierno.

Y para evitar que se cumpla con los objetivos y los intereses nacionales, se va a ver siempre amenazada por los siguientes antagonismos o amenazas que podremos ver posteriormente, como son los fundamentalismos religiosos, los conflictos bélicos, el terrorismo, las pandemias, los ciberataques, la corrupción, los grupos antisistémicos, una delincuencia organizada transnacional, el narcotráfico, grupos armados, la migración y los desastres naturales.

De tal manera que estas van a llevar siempre a cabo lo que se conocen como las amenazas y van hacer su acción sobre las áreas estratégicas, geográficas y funcionales.

De tal forma que aquí podemos ver en el mapa conceptual cómo se clasifican los antagonismos, que son riesgos, presiones dominantes y los factores adversos, y los primeros marcados en amarillo muestran que con una sola aplicación de lo que es el poder nacional se puede eliminar este tipo de riesgo.

Pero cuando ya tenemos una amenaza que puede ser del tipo emergente o tradicionales, se necesita emplear todo el poder nacional, y es papel de todos los entes de la sociedad y de todas las instituciones el poder enfrentar este tipo de situaciones que se derivan de una hipótesis, ya sea de conflicto o de guerra.

De tal manera que podemos ver la clasificación de las amenazas o antagonismos que pueden afectar al Estado Mexicano, como son los factores adversos que no son antropogénicos, que son causados más que nada por las cuestiones naturales, las presiones y las presiones dominantes.

En donde yo quiero señalar que en las presiones dominantes, como en el último caso, se muestran los ataques cibernéticos. Y posteriormente las amenazas donde puede haber una guerra o una intervención o ataques con armas de destrucción masiva.

Es importante mencionar que, por primera vez en la historia del Estado Mexicano, derivado del Plan Nacional de Desarrollo se presentó en el 2014-2018, un Programa para la Seguridad Nacional.

Este programa que se deriva del Plan Nacional de Desarrollo, es el documento rector de la política de seguridad nacional del Estado Mexicano, tratándose de un documento que adopta una aproximación multidimensional. Es decir, toma en cuenta a la escuela de Copenhague, la Escuela de Seguridad de Estatus Céntrica, y la Escuela de Seguridad que dan actualmente los países como el Japón y el Canadá enfocada en las necesidades humanas.

Que esta es una visión congruente con la visión del Ejecutivo Federal, dando las siguientes prioridades temáticas: Una consolidación del sistema de seguridad nacional, un desarrollo de la cultura de la seguridad nacional.

Toma en cuenta la posición geopolítica de México, y toma en cuenta el escenario de seguridad interior, así como las amenazas globales para la seguridad nacional.

Antes de continuar, yo quisiera agradecer toda la importancia que tiene este foro por lo que es la transparencia y por la protección de los datos, y precisamente una de las Fuerzas Armadas, una de las misiones de las Fuerzas Armadas es dar la seguridad y defensa.

Y actualmente en eso se conforma mi tesis, que es necesario proteger más todos esos datos y todo lo que se le llama las infraestructuras críticas que tiene un país.

Como lo podemos ver, hace pocos días, antes de venir ante este foro tan importante, se hizo viral esta fotografía de Mark Zuckerberg, el creador de Facebook, en donde estaba festejando su cuenta número de 500 billones de adherentes a Facebook.

Pero lo interesante es que en la parte de atrás se mostraba su computadora. Cualquiera diría: ¿Bueno, por qué es importante esta fotografía? Porque si ustedes pueden ver, en la parte de lo que es la cámara se encuentra perfectamente cubierta por una cinta de aislar y lo que es el micrófono.

Se dio a conocer que había sido hackeada su cuenta y le habían quitado toda su información, de lo que ustedes han estado hablando, sobre los datos personales. Entonces siendo él el creador de Facebook ya no tiene ni siquiera tampoco una confianza en lo que es el ciberespacio.

Igualmente también hace algunos días un gusano metido por un hacker denegó el servicio a cuentas tan importantes como Twitter, News, Time y Spotify, entre otros, entre ellos diciendo que también hubo robo de información a través del ciberespacio.

Para poder llevar a cabo todo lo que hemos estado tratando a lo largo del día, es necesario proteger toda esa información.

De tal manera que actualmente ustedes pueden ver, por ejemplo, en esta lámina muy interesante se puede, en donde nosotros vemos hacia los Estados Unidos, los países europeos como son España, Francia, que ya han sido atacados literalmente por otros Estados para obtener información o bien para atacar su infraestructura crítica, como pueden ser las instalaciones nucleares, como lo vamos a ver posteriormente, bases de datos.

Entonces de ahí que surge la necesidad de proteger toda esta información.

De tal manera, que vamos a ver primeramente qué es el ciberespacio.

El ciberespacio es un ámbito intangible, de dominio global, soportado por las tecnologías de la información y utilizado por la interacción de los individuos, entidades gubernamentales públicas y privadas; dentro del ambiente de la información, su carácter único y distintivo está enmarcado en el uso de la electrónica y del espacio electromagnético, en la creación, almacenamiento, modificación del intercambio en la explotación de la información a través de redes interdependientes.

Es una realidad que tenemos aquí, que ustedes pueden ver lo que es el costo del ciberdelito. Tan sólo para México el año pasado reportado por *Cyber Deck*, el robo de identidades y el robo causado por ciberdelito, ya sea por negación de servicios, le costó a México tres mil millones de pesos, por robo de identidades. A lo que es Estados Unidos le costó 38 mil millones de dólares.

Y así nosotros podemos ver, por ejemplo, la comunidad europea, 13 mil millones de dólares; Brasil, ocho mil millones de dólares.

Pero la situación se complica aún todavía más porque el ciberespacio y la utilización de las tecnologías de la información es ya una realidad.

No podemos, ese es un camino ya que no puede, no tiene camino hacia atrás. Entonces lo que hay que hacer es tratar de proteger esa información y esas infraestructuras críticas que se encuentran dentro del país.

Esta lámina muestra cómo en el 2013 nosotros teníamos 51.2 millones de usuarios de las tecnologías de la información y de cómputo; se estima que para el año 2020 aproximadamente la tendencia es que haya más de 85 millones de mexicanos utilizando las tecnologías de la información.

La información en archivos, comunicaciones y controles que se efectúan en el ciberespacio impactan la infraestructura crítica de nuestro país y su afectación se traduce en riesgos y amenazas a la seguridad nacional, finanzas, información y comunicación tanto política

y tecnológica, así como controles de las infraestructuras críticas, inclusive también tráfico aéreo y marítimo, entre otros.

Las Fuerzas Armadas también utilizan el ciberespacio para su administración y almacenaje de datos y la utilización de redes en Intranet e internet para sus comunicaciones, sistemas de mando y control, tanto en tiempo de paz como en tiempo de guerra.

Las naciones más aventajadas tecnológicamente, como podemos ver, están utilizando el ciberespacio como campo de batalla, denominándolo “la quinta dimensión de la guerra”.

Asimismo, por la relevancia que su uso representa, el ciberespacio es tema de libros, publicaciones, artículos e investigaciones relativos a considerarlo como un nuevo dominio en donde se realizan las guerras del futuro.

De tal forma que, como podemos ver en la ilustración, se ha escrito ya muchísimo, uno de los grandes libros es “El manual de Talli”, “Los principios de la ciberguerra”, que es una guía para los oficiales militares; “La guerra en la red, los nuevos campos de batalla”.

Es importante mencionar que tanto los Estados Unidos como los europeos, los miembros de la OTAN están muy preocupados y ya han escrito mucho al respecto, inclusive ya han generado doctrina y ejercicios en conjunto en la OTAN y en México ya empieza a crearse una gran preocupación sobre la protección a las infraestructuras críticas por medio del ciberespacio, de tal manera que no solamente es entre los académicos, sino que también ya hay muchas publicaciones que son asequibles para todo tipo de público, en donde se tratan este tipo de situaciones de los ciberdelitos o ciberamenazas.

También dentro de las instituciones dedicadas a lo que es la seguridad nacional se han escrito varias tesis como, por ejemplo, la ciberdefensa en las fuerzas armadas, una perspectiva conjunta, la conformación de un grupo de guerra electrónica especializado en las ciberguerras para el apoyo de las operaciones navales en la Armada de México, el establecimiento de un grupo multidisciplinario de operaciones de información, en apoyo a las operaciones navales.

Todas éstas, mismas que pueden ser consultadas en los centros de estudios superiores navales.

La pregunta de investigación que llevó a cabo para resolver esta tesis es: ¿Cuáles serían esos fundamentos estratégicos que serían propuestos para validar la creación de un organismo militar, con capacidades para actuar en el ámbito del ciberespacio, con objeto de prevenir riesgos y amenazas a la defensa nacional?

El objetivo de la investigación fue identificar los fundamentos estratégicos que validarían la creación de un organismo militar, con capacidades para actuar en el ámbito del ciberespacio, para prevenir los riesgos y amenazas a la defensa nacional.

De tal manera que el propósito fue proponer estos fundamentos estratégicos y estructurales para la creación de un cibercomando para las Fuerzas Armadas que permitieran prevenir los riesgos o amenazas en el ciberespacio.

El supuesto de investigación que guió el trabajo de investigación, fue que la creación de un cibercomando fortalecería las capacidades estratégicas de las Fuerzas Armadas Mexicanas, para la defensa nacional en el ciberespacio, considerando los riesgos y amenazas provenientes de entes antagónicos, ya sean nacionales o extranjeros.

De tal forma que fue una investigación meramente del tipo hermenéutica, investigando los tipos de investigaciones que ya había y la interpretación por medio de apoyo de gente experta, de los textos que ya existen, que hablan al respecto.

Primeramente no podemos crear nada que no esté dentro del marco legal de la legislación mexicana.

El referente es la Constitución Política de los Estados Unidos Mexicanos, en su artículo 89, fracción VI, establece que es facultad del Presidente de la República el preservar la seguridad nacional y disponer de la totalidad de las Fuerzas Armadas Permanentes,

llámense el Ejército, la Armada y la Fuerza Aérea, para la seguridad interior y defensa exterior de la Federación.

También dentro de la Ley de Seguridad Nacional, se establece que las amenazas son aquéllas que atentan contra la seguridad nacional y son los actos tendentes a consumar el espionaje, sabotaje, terrorismo, interferencia extranjera en los asuntos nacionales que puedan implicar una afectación en el Estado Mexicano.

Dentro de la Ley Orgánica de la Armada de México, se le dan a la Secretaría de Comunicaciones y Transportes las atribuciones para administrar, controlar y supervisar, así como fomentar los servicios de comunicación, llámense entre ellos el internet.

Lo más importante también que el Plan Nacional de Desarrollo, que es la política pública para crear el desarrollo a nivel nacional, se establece como la meta número uno, la de un México en Paz, que este es uno de los objetivos coyunturales que es necesario preservar, para alcanzar los objetivos permanentes.

Se establece que de acuerdo a los objetivos, estrategias y líneas de acción, se considera diseñar e impulsar una estrategia en seguridad de la información, y la de fortalecer la cuarta dimensión de las operaciones de seguridad del ciberespacio y la ciberseguridad.

Igualmente, el CISEN, el Centro de Investigación y Seguridad Nacional, por sus siglas CISEN, tiene dentro de sus funciones emitir sexenalmente la Agenda Nacional de Riesgos.

En ella, en la Agenda Nacional de Riesgos 2014-2018 se establece que se debe de contemplar y atender la vulnerabilidad cibernética del Estado Mexicano, y garantizar la integridad y la disponibilidad de la información de las personas e instituciones públicas y privadas de México, haciendo hincapié que este es uno de los principales riesgos que se contemplan en la Agenda Nacional de Riesgos.

Finalmente, con respecto al marco jurídico del ciberespacio, la Ley Orgánica del Ejército y Fuerza Aérea Mexicana, establece que tiene como misión general defender la integridad, la independencia y la

soberanía de la nación, así como garantizar la seguridad interior, entre otras.

Con respecto a la institución que represento, la Secretaría de Marina Armada de México, tiene como misión y atribución emplear el poder naval de la federación para la defensa exterior y coadyuvar en la seguridad interior del país.

Hace rato le preguntaban al maestro sobre las cuestiones legales; el problema con el ciberespacio es que poco se ha escrito para tratar de legalizar este tipo de situación, y más en las cuestiones del Estado, de la guerra.

Como ustedes bien saben los tratados de Ginebra trataron primeramente de preservar la vida humana, de los heridos; posteriormente, en los segundo convenios de Ginebra, fue para los heridos; los terceros, para los prisioneros de guerra y los náufragos, pero nunca se ha tratado la cuestión de un derecho de la guerra, que es ya una realidad en la cuarta o quinta dimensión, como es conocida, que es en el ciberespacio.

Entonces, los primeros intentos fueron en el año 2004, cuando la Organización de los Estados Americanos establecieron una Estrategia Interamericana Integral de Seguridad Cibernética, promoviendo a través del Comité Interamericano Contra el Terrorismo y del Programa de Seguridad de Informática, Estrategias Nacionales sobre Seguridad Cibernética, quedando plasmadas en las resoluciones /03, referida al desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética.

Posteriormente, en el 2013, los países integrantes de la OTAN publicaron el manual de Tallin, donde se estipula el marco de Ley Internacional aplicable a la ciberguerra.

En el 2015, nuevamente auspiciada por las Naciones Unidas, se realizó la Tercera Cumbre Mundial sobre la Sociedad de la Información, logrando definir a la Sociedad de la Información, que se combine internacionalmente con líneas para la creación de capacidad,

diversidad cultural y la creación de confianza y seguridad, nuevamente, en la utilización de las tecnologías de la información.

Esos son los marcos conceptuales, las palabras con las que estamos refiriendo, que se hablan cuando se trata del ciberespacio, haciendo muy específicamente lo que son los *spam*, las ciberarmas, el ciberterrorismo, las ciberamenazas, las ciberdefensas, las ciberguerras, los ciberdelitos y la ciberseguridad.

De tal manera que lo más importante en estos casos son los ciberraptores, que se van a actuar en lo que se llama el ciberespacio o la cibernética, y que van a causar lo que puede llevarse a cabo, un ciberdelito, una ciberguerra, y que para protegernos de tales amenazas se tiene que hacer o llevar a cabo la ciberdefensa.

Aquí viene una situación: Con respecto a los ciberreactores, la situación y los estados, normalmente el derecho internacional, siempre el principal actor del derecho internacional son las naciones.

El problema con las ciberamenazas es que pueden provenir, tanto de una nación como un grupo, como es el grupo Anonymous, que ahí viene la problemática, que estos grupos pueden robar información y todos los datos personales fácilmente.

Vienen los *hackers* y los *crackers*, que desafortunadamente no hay una legislación completamente, todavía, para actuar en contra de ellos contundentemente.

Igualmente en este marco conceptual se pueden observar lo que son los ciberdelitos y lo que es el cibercrimen, poniendo especial atención en lo que es el ciberrobo, que puede ser desde el robo de identidad, de datos, hasta de recursos financieros; lo que es el ciberataque, que es directamente a las infraestructuras críticas de un país; el ciberespionaje, lo que se le llama la guerra económica o guerra tecnológica para poder robar lo que se le llaman los secretos tecnológicos de las empresas y que esto va considerarse como una ciberamenaza o como un ciberterrorismo, que este último es uno de los más graves, porque van a tener el enfoque de crear el terror a toda una sociedad de un país.

¿Cuáles son esos conflictos en el espacio? Son las acciones llevadas a cabo por un Estado para penetrar las computadoras, redes o sistemas de otro país, con el propósito de causar daños y disrupciones.

Esa es la definición que da Richard Clair, que es uno de los más versados sobre el tema de la guerra en el ciberespacio.

Aquí podemos ver cuáles. Analicé 51 ciberataques que se han dado en el trayecto de la historia, destacando como más importantes los siguientes:

En el 2006 fueron atacados los servidores del Departamento de los Estados Unidos y se descargaron de manera ilegal cientos de terabyte de información de todos los habitantes de los Estados Unidos.

Igualmente, en noviembre de 2006 fueron atacados los servidores de un colegio muy prestigiado, el War College, y descargaron toda su información.

En el 2007 Estonia alcanza un gran desarrollo y dependencia del uso del internet, estableciendo en su población el uso de tarjetas de identidad con firma digital, votación electrónica municipal y federal, entre otras.

Al reubicarse un monumento de la era soviética, surge una inconformidad de la minoría rusófona, tras la cual hubo ataques cibernéticos de negación de servicios a los bancos, gobierno, servicios básicos e inhabilitación de los servicios críticos nacionales; también se robaron toda la información y datos de las personas de Estonia, causando con ello un caos en toda la población.

Igualmente, en noviembre del 2007 Israel hackea los sistemas de defensa antiaérea de Siria y efectúa un ataque aéreo a la construcción de una planta nuclear, retrasando con ello su construcción.

En el 2008 un virus cibernético llamado Stuxnet entra en una planta nuclear en Natanz, la mayor ciberarma hasta entonces utilizada atacó

a la centrifugadora del software Siemens, utilizada para enriquecer el uranio, ocasionando el retraso en la construcción por más de dos años.

Se presume que fue perpetrado por los Estados Unidos, a través de un virus implantado con un USB por uno de sus trabajadores, desatando esto una ciberguerra mundial en el desarrollo de métodos de ciberataque, obligando al gobierno iraní a la creación de un cibercomando para hacer frente a los mismos y desarrollar la tecnología de la ciberguerra.

Posteriormente, en el 2010, creo que de todos son conocidos los famosos WikiLeaks, en donde se dio a conocer gran información diplomática de los Estados Unidos y de otros países que fue robada en la red.

Septiembre de 2011, con una capacidad desarrollada de ciberguerra, Irán roba la señal de un dron, iba volando el dron sobre territorio iraní, lo bajaron y le robaron toda la información que tenía para poderla duplicar.

En el 2014, robo de información de la empresa Sony Pictures para disuadir la presentación del estreno de la película La Entrevista, donde Estados Unidos realiza un complot para asesinar al mandatario norcoreano Yin Sin. Se presume que el ataque lo perpetró Corea del Norte. El gobierno de los Estados Unidos toma este asunto como un carácter de defensa nacional a partir de esa fecha importante.

Aspectos significativos.

Es de especial relevancia para la presente investigación el contenido de esta información, ya que en su contenido se notaron aspectos significativos, destacando entre ellos, primero, que los países que se encuentran en conflicto, al realizar un ataque armado, lo anteceden y acompañan de ciberataques a sus sistemas o redes de armas, y a las infraestructuras estratégicas del país objetivo.

Segundo. Dos países que se encuentran en algún tipo de conflicto están constantemente realizando ciberataques, entre ellos.

Tercero. Los países potencias tienen grupos, algunos no reconocidos y otros reconocidos como cibercomandos, que elaboran y acciones ciberarmas con diferentes fines.

La información indica que China, a través de grupos no reconocidos, se encuentra espiando y robando la información significativa de países que considera clave para sus intereses económicos, tecnológicos y militares.

El desarrollo de ciberarmas requiere de grandes inversiones, así como de personal o grupo especializado y de objetivos específicos.

Tengo que hacer la aclaración que la guerra es un conflicto de poder entre dos o más sujetos, en los cuales uno trata de imponer su voluntad sobre el otro, con fines de dominio económico, expansión territorial o imposición de voluntades.

Ha sido una actividad de instinto, llega a ser conceptuada y posteriormente como una ciencia. Existen una gran cantidad de definiciones de tipo de guerra.

Por ejemplo, esto me llevó a investigar que los chinos clasifican a sus armas haciendo hincapié en lo que es la guerra, la cuarta etapa que es la guerra mecanizada, en donde consideran ellos ya al ciberespacio como un campo de batalla.

Los Estados unidos, ellos, como lo podemos ver, tienen ya cuatro espacios, tenían cuatro espacios en donde se podía llevar a cabo el desarrollo de un teatro de la guerra, que es primeramente el terrestre, el segundo el marítimo, el aéreo y el espacial, porque ellos tienen la tecnología de poder hacer la guerra en el espacio.

Y para ellos ya es una realidad completamente, que es la quinta dimensión donde se puede llevar a cabo un conflicto bélico, que es el ciberespacio.

Es importante mencionar que para México en el Plan Nacional de Desarrollo se considera como el cuarto espacio en donde se puede llevar a cabo una amenaza. El ciberespacio.

Es difícil, pero se tuvo que analizar todo este tipo de situaciones de los polemologistas, habiendo estudiado la filosofía de Zunzu, de Maquiavelo, de Junini, de Clausewits, de Mahan, de Little Hard, de Michel y Dowsett, y dentro de sus libros podría yo sacar tres comunes denominadores.

El primero de ellos es que ven a la guerra a través de los tiempos como una condición humana y recurrente.

La segunda, que predicen una evolución en la teoría y formas de hacer la guerra. Ellos aceptan que debe de haber una evolución del pensamiento y de las estrategias para hacer frente a las amenazas de otros estados, adaptándose a los nuevos ámbitos en que esta se desarrolla.

Y la tercer es que en las teorías que ellos conciben obligan a elaborar nuevas estrategias, tácticas de ataque y de defensa para permutar a la guerra en el ciberespacio, ya que esta es una realidad inherente.

Cuenta de ello son los cibercomandos que diversos países están estructurando dentro de sus gobiernos, ya sea cibercomandos, agencias o centros especializados en el ámbito del ciberespacio para fortalecer su aspecto legal en acciones del cibercrimen, ciberdefensa y ciberataque, destacando entre ellos que ya es una realidad que lo tienen, Alemania, Argentina, Brasil, China, Colombia, Estados Unidos, España, Irán, Reino Unido, la OTAN y la Unión Europea.

Ahora las Fuerzas Armadas y el ciberespacio. ¿Cuál es la función de las Fuerzas Armadas en el ciberespacio y por qué tendríamos que estar ahí?

Las Fuerzas Armadas conciben dos situaciones: La primera es la seguridad; es decir, en inglés la acepción es Security, de poder hacer todas las actividades que se llevan a cabo en el ciberespacio sin ningún temor. Es una percepción.

Y la otra rama es la ciberguerra. Debemos de tomar en cuenta que México debido a su constitución y a su doctrina, la doctrina Estrada, única y exclusivamente, repito, concibe a la guerra solamente en casos de defensa. Jamás como una ofensiva.

Luego entonces si llegase a existir lo que se propone de los cibercomandos, tendría que ser única y exclusivamente conforme lo marca la constitución, para brindar lo que es la seguridad informática llevando a cabo la ciberseguridad y poder tener con ello el desarrollo del país.

Estos son, como podemos ver, un mapa esquemático muy rápidamente, en donde nosotros podemos ver; esta lámina yo la quiero utilizar porque nosotros no podemos pensar en que puede existir desarrollo sin seguridad. Es una balanza.

No hay ningún país que apueste más a tener una mayor seguridad, descuidando el desarrollo; o viceversa, que apueste a su desarrollo sin apostar a la seguridad. Debe de ser una relación simbiótica, debe de caminarse al parejo.

Si yo quiero tener un desarrollo, mas no crecimiento, debo de tener yo seguridad en el Estado. Por eso la importancia ante las nuevas amenazas que el Estado Mexicano debe de brindar y está brindando ya una seguridad a toda la información y a las infraestructuras críticas.

De tal manera que se tendría que actuar en lo que es en el ciberespacio, en las guerras declaradas y las guerras no declaradas.

La necesidad de la creación de un cibercomando para las Fuerzas Armadas está fundamentada en un requerimiento de defensa nacional, para el caso de la guerra y de seguridad interior en operaciones diferentes a las de la guerra, ambas en tiempos actuales.

Estos fundamentos surgen del análisis de la información compilada en la investigación que se realizó, lo que nos lleva a los siguientes fundamentos estratégicos.

El primero. La importancia del internet por su penetración en la sociedad ha creado de él una dependencia imprescindible para los gobiernos y la sociedad, por la exponencial cantidad de usuarios que crecen día a día realizando actividades financieras, políticas, sociales, militares, tecnológicas y diplomáticas, dando oportunidad a que países, grupos o hackers realicen actividades delictivas que ponen en riesgo la seguridad nacional, demandando esto la ciberdefensa.

El siguiente fundamento estratégico es debido a que la evolución del internet y sus vulnerabilidades son aprovechados por países potencias para realizar ciberataques a países enemigos o amigos, al amparo de carencia de un marco legal que regula las actividades que en él se desarrollan, usando el ciberespacio como campo de batalla de las guerras actuales y futuras, creando la necesidad de legislarlo, tipificando los ciberdelitos, así como el desarrollar capacidades para detectar las vulnerabilidades propias con el fin de corregirlas.

El fundamento número tres del análisis de la información fue que el uso del ciberespacio como campo de batalla, su carencia de legislación y la naturaleza humana de tomar ventaja económica, política o militar a través de la ciberguerra, ya sea declarada o no declarada; fallas en los sistemas de ciberdefensa de los países objetivos crean la necesidad de evolucionar la guerra hacia un nuevo cuerpo que tenga la estructura, doctrina, conocimientos y recursos para que a través de un organismo especializado se desarrollen las ciberarmas y tenga la capacidad de enfrentar una ciberguerra.

El fundamento número cuatro es que la misión de las Fuerzas Armadas de la Defensa Nacional, así como el coadyuvar con la seguridad interior, la importancia y la penetración de las actividades en el ciberespacio lo hacen un factor generador de riesgo y amenazas a la defensa nacional y seguridad interior, por lo que las Fuerzas Armadas tenemos la obligación legal de tomar como antagonismo los ciberataques y ciberamenazas a las infraestructuras críticas, así como la estrategia nacional a implementar acciones para anularlas o minimizar sus efectos.

La visión de la ciberguerra es que considerando el ciberespacio como un medio de comunicación y transporte de datos y de información, la

Secretaría de Comunicaciones y Transportes tomó la responsabilidad de elaborar una iniciativa de Ley para regular, controlar, supervisar las actividades que en él se desarrollan, así como tipificar los ciberdelitos en una denominada Ley del Ciberespacio.

También se promovió a nivel internacional que la Unidad Internacional de Telecomunicaciones legislará el uso del ciberespacio como parte de las comunicaciones mundiales, lo que convirtió a México en un precursor en la materia.

Mientras tanto, la Policía Federal continuará ejerciendo el aspecto policial en el uso del ciberespacio a través de sus Centros CERT, que son centros para ataques cibernéticos para detectar y perseguir los actos de la ciberdelincuencia.

De tal manera de que se proponen las siguientes propuestas, armando las siguientes estrategias:

Conformar dentro de las estructuras de las fuerzas Armadas Mexicanas un cibercomando, enfocado a la defensa nacional con capacidad de ciberguerra.

La estrategia dos es que a través de la Secretaría de Comunicaciones y Transportes, al seno de la Unión Internacional de Telecomunicaciones fomentar internacional y nacionalmente la regulación del uso del ciberespacio.

La estrategia tres es la formación y adiestramiento de especialistas en informática dentro de las Fuerzas Armadas, lo que se conoce como hackers; para las Fuerzas Armadas serían los cibersoldados.

La estrategia cuatro es la colaboración entre la Administración Pública Federal, los tres niveles de gobierno, iniciativa privada y la academia, para el intercambio de información, aviso de ciberataques, acciones para ciberdefensa y promoción de una cultura de la ciberseguridad.

Es importante –recalco– que la defensa nacional es una obligación de todo un Estado, no únicamente de las Fuerzas Armadas.

La estrategia cinco es fortalecer la ciberseguridad y ciberdefensa, en el aspecto de software, hardware e infraestructura física, así como las regulaciones de seguridad informática.

¿Qué se concluye?

Que el ciberespacio en el internet se ha convertido en una herramienta indispensable y necesaria, a nivel nacional e internacional, por la importancia de su contenido, así como la potencial afectación por ciberataques, su uso se ha convertido en un asunto de seguridad nacional.

En el ciberespacio se realiza intercambio y almacenaje de información crítica, se controlan sistemas de infraestructura estratégica, llámense de PEMEX, Comisión Federal de Electricidad, del Sector Financiero, y las Fuerzas Armadas, a través del ciberespacio de sus redes, accionan y controlan sus sistemas.

Por su recién y rápida evolución crean vulnerabilidad que se pueden traducir en riesgos y amenazas a la seguridad nacional.

El mundo vive una guerra económica no declarada, donde los países, potencias que cuentan con estrategias definidas y con fines disuasivos, espían, roban información y están en condiciones de realizar ciberataques, con el fin de denegar y paralizar la infraestructura estratégica, en diferentes campos de poder de países enemigos o amigos.

Los pensadores estratégicos coinciden en reconocer la existencia de la guerra, como medio para la resolución de los conflictos.

Nuevamente, cuando la política falla es cuando viene la guerra.

Sus teorías y estrategias surgen de la evolución tecnológica y social.

Estas filosofías prevalecen en el tiempo, debido a que las situaciones o los conflictos de adaptan al dominio en donde se realiza la guerra.

La siguiente conclusión es que los países potencias han formado dentro de la estructura de sus Fuerzas Armadas o de su aparato gubernamental, agencias, centros o cibercomandos, con el fin de fortalecer la seguridad, la ciberdefensa y desarrollar las armas.

Los conflictos actuales se han caracterizado por el uso de estos cibercomandos en el ciberespacio, como campo de batalla.

Las recomendaciones son que se continúe estudiando en el Centro de Estudios Superiores Navales y en El Colegio de Defensa Nacional, la importancia del uso del ciberespacio y sus repercusiones en la seguridad interior o defensa nacional y el papel que las Fuerzas Armadas deben de llevar a cabo para proteger a la nación contra estos riesgos y amenazas a la seguridad nacional.

También la necesidad de que internacionalmente se elabore un acuerdo-carta para regular, controlar, supervisar las actividades y tipificar los delitos en el uso del ciberespacio y que bajo la autoridad de la Unión Internacional de Telecomunicaciones, con beneplácito de la ONU, se elaboren las propuestas de leyes, reglamentos y normatividad con el mismo fin.

Igualmente se establezca la conveniencia y la factibilidad de un cibercomando, que ya fue tomado en cuenta por ambas secretarías para proceder a conformar este tipo de cuerpos especiales.

Por su atención, muchísimas gracias.

Moderador: Realmente importante exposición, clara, precisa, demostró cómo el mundo del ciberespacio representa una compleja red de información de millones y millones de usuarios.

En una conversación que tuvimos hace unos días con el Contraalmirante ya hablaba él de dimensiones de guerra: la terrestre, la marítima, la aérea, el espacio, y hoy nos está exponiendo precisamente toda una exposición del ciberespacio.

Espacio que amerita contar con una regulación supranacional para prevenir riesgos, tanto para la penetración de los *hackers* en la

información personal como institucional, así como de toda una nación, de toda una defensa de la nación.

Es decir, no es lo mismo un espacio físico donde se resguarde información, que tiene medidas de seguridad y resguardos específicos, con cubrir espacios donde la inteligencia de los *hackers* tiene acceso a la información, tanto personal como institucional o de toda una nación, por lo tanto representa un reto, realmente, el garantizar la seguridad, no sólo de la persona sino de las instituciones y de la misma nación.

La exposición es excelente, nos muestra toda una gama de temas involucrados en este aspecto del ciberespacio, lo cual nos hace repensar cómo en la parte, en la normatividad deberíamos incluir este elemento esencial, en donde nuestra comunicación ya no solamente es telefónica o por escrito, sino también por estas vías de las redes.

Entonces aquí nosotros les preguntaríamos si tienen alguna inquietud o alguna duda para que podamos entrar en esa comunicación con el Contraalmirante.

Adelante, por favor.

Pregunta: Más que nada explicarles a todos que esto siempre se ha visto.

Aquí en México en 1950, en esos tiempos se le había evitado el voto a la mujer, durante ese tiempo muchas mujeres se unieron para exigir sus derechos como mujeres, pero todo es un plan gubernamental.

Anteriormente, en los años cincuenta los impuestos se pagaban por familias, era un solo impuesto por familia.

Cuando llega a surgir este voto, donde todas las mujeres se unen a exigir ese derecho, se perdieron de la obligación, que era de que ellos también iban a pagar un cierto aporte, que vienen siendo otros impuestos y ahora los impuestos se cobran individualmente.

Quiero más que nada aclarar que esto siempre se ha visto, sin embargo, nosotros a veces nos cegamos con cosas, no sé, estamos tapándonos los ojos nosotros mismos y nosotros debemos abrir los ojos a la luz, ver algo más allá.

Actualmente los ciberespacios, como usted lo comenta, contralmirante, es cierto todo eso.

Ahora, no sé, ustedes deben de ver todo esto, porque si se siguen tapando los ojos llegaremos a un grado de ignorancia donde nos van a dominar, porque de nada sirve que a nosotros nos estén dando estas exposiciones de cómo defender nuestros derechos, cuando tenemos miedo nosotros mismos de defender nuestros propios derechos. Eso no va, esto no serviría de nada.

Si se está dando una plática de cómo defender sus derechos, es precisamente para que ustedes aprendan cómo defenderlos, pero siempre y cuando acatando las obligaciones que tienen esos derechos.

Más que nada, nosotros como pueblo no tenemos ningún enemigo ni espías que a nosotros nos persigan o algo, sino que siempre se nos han tapado los ojos con el mismo gobierno, es algo que en México siempre sucede.

Muchas gracias.

Contralmirante Juan Carlos Vera Salinas: Antes que nada, primeramente quiero agradecer la opinión muy acertada. Efectivamente, México como tal no tiene ninguna hipótesis de guerra al día de hoy, no tenemos un país-estado que nos pueda atacar, pero ese es un punto de vista muy personal, más no el de mi institución, a la cual represento.

Lo mismo decíamos, nadie pensaba que íbamos a tener tres intervenciones por parte de los Estados Unidos, nadie pensaba que íbamos a tener dos intervenciones por Francia.

No podemos tener, no tengo una bola de cristal para poder decir que hoy no lo tenemos, pero mañana no les puedo asegurar que podamos tener, entonces la mejor manera de seguir protegidos, de que nuestra infraestructura crítica, toda la información que ustedes han vertido el día de hoy tan importante como son los datos, como es la información personal, la mejor manera de estar preparados es preparándonos desde ya, no esperar a que tengamos el problema

Pienso que siempre, a mí se me ha enseñado dentro de los estudios que he realizado, trabajar con la prospectiva y trabajar siempre con el escenario catastrófico, siempre. De tal manera de estar preparado para lo que pueda suceder.

Entonces creo que es el momento, y mi Secretaría a la que tanto amo, la Secretaría de Marina y la Secretaría de la Defensa Nacional, aún con los pocos recursos que tienen, ya se encuentran preocupados por empezar a crear estos cibercomandos, ya se tiene la gente necesaria, se está mandando a capacidad tanto a Estados Unidos como a Europa, para estar preparados y poder defender toda esa información que ustedes dijeron, todo ese derecho que tiene el ser humano, que es inalienable, que es el derecho a la información y la protección de sus datos.

Moderador: Si no hay ninguna otra pregunta, agradecemos la participación del Contralmirante Juan Carlos Vera Salinas.

¿Levantó alguien la mano?

Pregunta: Buenas tardes.

Moderador: Adelante.

Pregunta: Mi pregunta va dirigida a lo que acaba de mencionar, respecto a la tecnología que se está innovando para poder proteger cibernáuticamente la información como nación, confidencial y no tan confidencial.

Se rumora, o al menos lo que muchos oídos hemos tenido, es que la tecnología nacida en México, cualquier tipo, realmente el gobierno no

le invierte, por tal motivo este tipo de innovaciones se van a otros países.

¿Qué solución se le daría a esto si también hay rumores que no puede el Gobierno Mexicano invertir en tecnología por un tratado o contrato, no sé cómo se pueda definir, con expresidentes, y que marcaban un tiempo?

¿Usted qué solución daría o qué propuesta daría ante este tipo de situaciones, ya que no hay presupuesto tal cual para desarrollar tecnología, o no tanto para desarrollarla, sino simplemente para que se quede en México?

Contralmirante Juan Carlos Vera Salinas: Muchas gracias.

Muy interesante tu pregunta.

Al respecto, por ejemplo, las Fuerzas Armadas en México empleamos el punto cinco, ni siquiera llegamos al punto cinco, es el punto 47 del Producto Interno Bruto, tan solo arriba de Guatemala. Somos el último país que invierte en sus fuerzas armadas. Sin embargo, dentro de nuestras posibilidades nosotros tenemos, la Secretaría de Marina tiene el INIDETAM.

Y lo que es más importante, cuando no se tienen recursos la visión de nuestros líderes, el señor almirante secretario y el señor general secretario hacen lo que se llaman las alianzas, y van a crear las sinergias necesarias, por ejemplo el INIDETAM, que es el centro de investigaciones científicas por parte de la armada, tiene alianzas con el INAOE, que es el Instituto Nacional de Astrofísica Óptica y Electrónica, del Instituto Politécnico Nacional, se tienen alianzas con el CONACyT.

Y entonces con un gran deseo de hacer las cosas, nosotros hemos llegado a tener ya una tecnología propia que hace que no dependamos del extranjero. Eso es muy importante, sobre todo en lo que se le llama la dependencia tecnológica, al igual que la Secretaría de la Defensa Nacional.

Con respecto a lo de los tratados que hayan hecho otros presidentes, no tengo el conocimiento para poder decir, pero yo puedo decir que el único freno que tiene un país es su voluntad.

Cuando queremos hacer, no vamos a los otros países que pensamos que tienen poder sobre nosotros, no es más que el que le damos nosotros.

Si nosotros tenemos la determinación de hacer las cosas bien, de que la gente tenga confianza en nosotros, nadie, nadie se los va a poder quitar.

Moderador: Muchas gracias, contralmirante.

¿Alguna participación?

Bueno, pues agradecemos…

Pregunta: Sí, muy breve.

Contralmirante Salinas, muy interesante su exposición porque habla un poco de algo que suena a ficción, la guerra del ciberespacio.

Pero hablando un poco en el ámbito de su dependencia, de la Marina, o si las amenazas en el ciberespacio a través de los satélites pueden afectar los mares, territorial, la parte patrimonial, que es muy vasta, que pueden haber también saqueo de recursos.

Entonces la pregunta es: ¿Si a través del ciberespacio y con la tecnología satelital la Marina puede cuidar la seguridad de los mares?

Contralmirante Juan Carlos Vera Salinas: Una pregunta muy interesante, que esto me obliga a exponerse.

Si cerráramos los números, México tiene cerca; vamos a cerrarlo, dos millones de kilómetros cuadrados de territorio.

Debido a los 11 mil kilómetros de costas que tiene por su situación geopolítica y su situación geoestratégica de tener dos salidas a ambos

océanos más grandes del mundo, el Océano Pacífico y el Océano Atlántico, que si realmente yo hubiera estado en los zapatos de Américo Vespucio hubiera puesto en los mapamundis a México en el centro, porque realmente eso es México; México es el centro y el puente del mundo, es un hub, que así lo debemos ver, así lo ven mis líderes, como un espacio.

El espacio marítimo que debe de ser cuidado es dos veces más que el territorio que estamos pisando, son cerca de cuatro millones de kilómetros cuadrados donde México tiene una completa soberanía, que es mío, de él y de todos ustedes, una riqueza inmensurable la que existe en esos espacios –entre comillas– “vacíos”.

Sí, desafortunadamente siempre las necesidades son mayores que los recursos –una Ley de Economía– y pocos son los medios, pero muchas las ganas y la inventiva, de tal manera que sí, efectivamente, la Secretaría de Marina, Armada de México tiene convenios con la Secretaría de Comunicaciones y Transportes, para vigilar por medio de satélites, de fotografía satelital, todo lo que es la zona económica exclusiva.

También –como es importante– para poder controlar hay que conocer.

Quiero decirles que gracias a esa información que da la fotografía satelital, es que la Secretaría de Comunicaciones y Transportes, la Secretaría de Gobernación y la Secretaría de Marina, ya tienen el inventario completo de las islas, cayos y arrecifes del territorio nacional, que era uno de los compromisos que se tenía ante la Organización Marítima Internacional, y gracias a esa información que dan los satélites tenemos conocimiento de cuál es nuestro mar territorial y nuestra zona económica exclusiva, que el Derecho Internacional nos asigna conocer un país bioceánico, tanto en el Golfo de México y en el Océano Pacífico.

No sé si con ello dé respuesta a su pregunta tan interesante.

Moderador: Muy bien.

Daríamos por terminada este panel.

Agradecemos la participación del contralmirante Juan Carlos Vera.

En nombre del Pleno del Instituto, hago entrega de un reconocimiento por su excelente participación.

Contralmirante Juan Carlos Vera Salinas: Muchísimas gracias.

Yo quiero decir que hace algunos días el alto mando tuvo a bien, con aprobación del Senado, ascenderme a la siguiente categoría que hoy ostento y estoy haciendo un Curso en Alta Gerencia Militar.

Gracias.

En esta Alta Gerencia Militar, como diría sir Winston Churchill, que la mejor arma de todo general es el conocimiento de su país y la cultura, y realmente es obligación de todo general y de todo almirante conocer a la perfección su país.

Tuve la oportunidad de que fue la doctora, la Presidenta del INAI, y ella nos comentaba que, por ejemplo, ¿por qué debería de existir un Instituto Nacional de Acceso a la Información?, que cuando ella fue a los países escandinavos le preguntaron: ¿Y por qué no dar esa información?

Pero cuando es un derecho, todo derecho tiene que ser protegido y para eso están las instituciones del Estado, como la nuestra.

Muchas gracias.

Presentador: Con esta conferencia damos por concluida la sesión abierta del Cuadragésimo Sexto Foro de Autoridades de Privacidad Asia-Pacífico, agradeciendo las aportaciones y conocimientos de todos nuestros panelistas, así como el interés mostrado por todos ustedes, en este importante evento.

Tengan todas y todos muy buenas tardes.

---o0o---