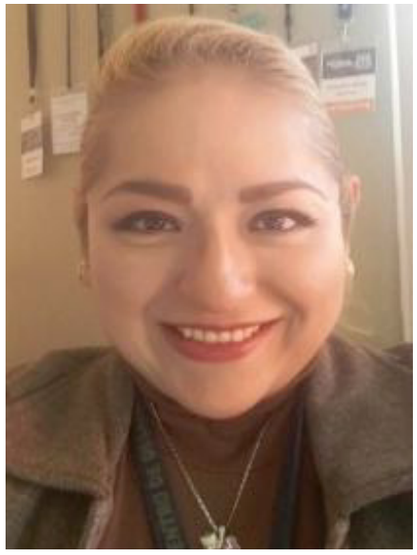
"CIBERSEGURIDAD: APRENDIZAJE DISRUPTIVO EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y LA SEGURIDAD NACIONAL "

Cybersecurity: Disruptive Learning in the Protection of Critical Infrastructures and National Security

Recibido: 06 / 08 / 2019 Aprobado: 31 / 10 / 2019



Licenciada
Alejandra Morán Espinosa
México

Licenciada en Derecho, Licenciada en Derecho por la Facultad de Estudios Superiores Acatlán, candidata a Maestra en Política Criminal, Diplomada en Criminalística con formación docente en la UNAM y diversas universidades privadas, conferencista, articulista e instructora en temas jurídicos relacionados con: seguridad informática, derecho informático, ciberdelitos, TIC, protección de datos personales, informática forense y Ciberespionaje entre otros. Ponente y conferencista en temas jurídicos relacionados con la seguridad informática y los delitos informáticos, docente de la materia de Derecho Informático en la FES Acatlán para alumnos y para profesores en el área de Tecnologías de la Información y Comunicación aplicables al Derecho, recientemente responsable del primer proyecto institucional de Investigación en Derecho Informático (IUSTICS) en la FES Acatlán. Es asesora de desarrolladores de software independientes e integrante de la comisión especializada de evaluadores de aspirantes a peritos auxiliares en el área de informática forense del Tribunal Superior de Justicia del Distrito Federal con sede en FES Acatlán (Áreas de evaluación: Derecho informático y Auditoria Informática), y responsable del único proyecto de Investigación, docencia y difusión en Derecho Informático y la Ciberseguridad en la UNAM denominado IUSTICS, con sede en FES Acatlán. Invitada como sector académico a eventos con la Estrategia Digital Nacional, así como, recientemente integrante y ponente del "5to. Encuentro Latinoamericano sobre: Ciberseguridad, Delitos Cibernéticos e Informática Forense" que literalmente incorpora a la UNAM, como una de las 15 instituciones del sector académico más importantes en la conformación de la actual Estrategia Nacional de Ciberseguridad. amoran@unam.mx y amoran@iustics.tech

RESUMEN

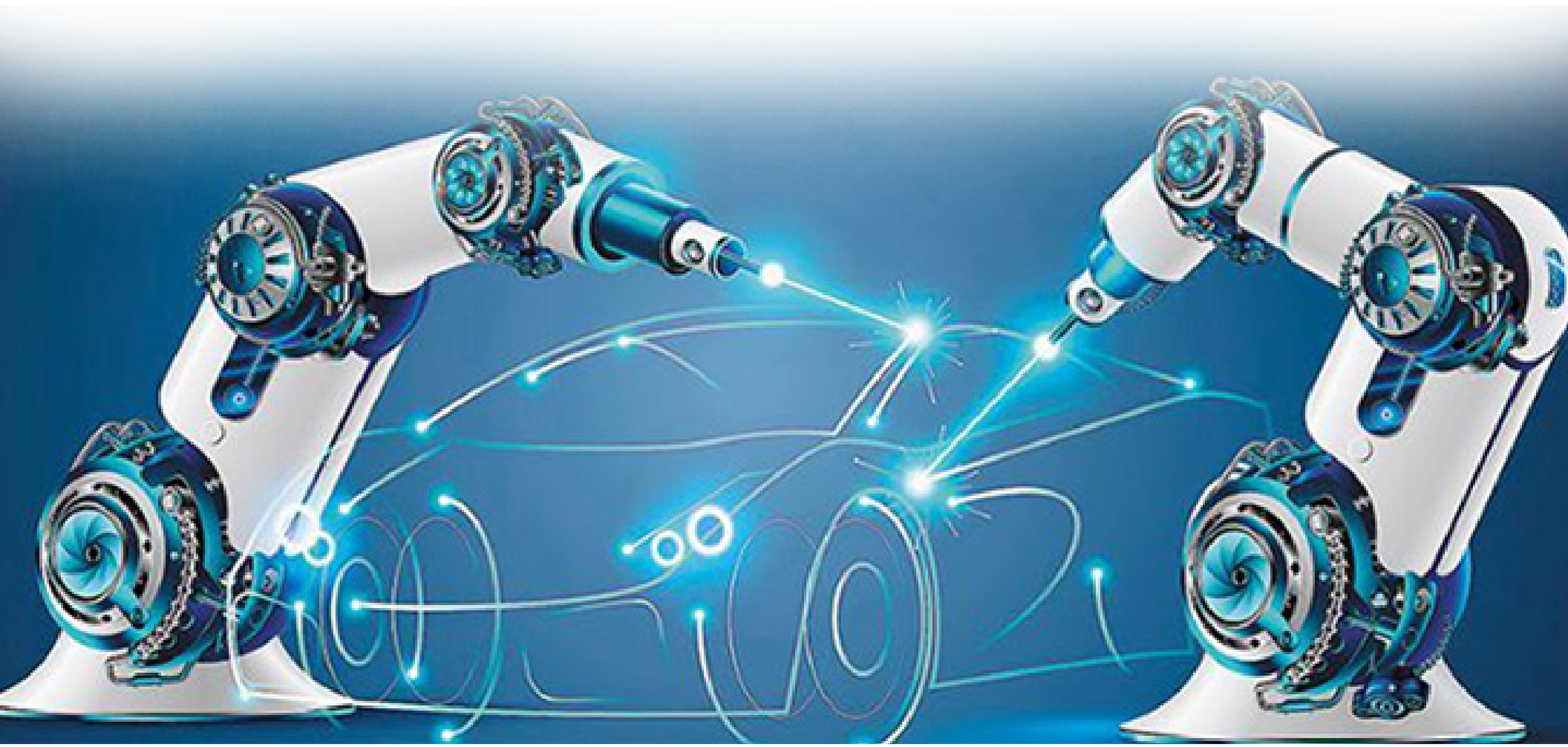
Ante la creciente posibilidad de un ataque cibernético a las infraestructuras críticas de un país, no bastan la seguridad cibernética o la seguridad nacional, debe evolucionarse decididamente a un modelo de protección que implique todos los aspectos, que sume a los avances en la ciberdefensa de los países; con un cambio del modelo de pensamiento, a uno complejo, multifactorial y radical e invariablemente integral, aquel que modifique la forma tradicional de proteger, debe atenderse como un todo a la Ciberseguridad.

Palabras clave:
Ciberseguridad, infraestructuras críticas, seguridad nacional, disrupción, estrategia nacional de ciberseguridad.

ABSTRACT

Given the growing possibility of a cyber attack on a country's critical infrastructures, cybersecurity or national security are not enough; there must be a decided evolution to a protection model that involves all aspects, which adds to the advances in the cyber defense of the countries. With a change of the thinking model, a complex, multifactorial and radical and invariably integral one, that modifies the traditional way of protecting, Cybersecurity should be understood as a whole.

Keywords:
Cybersecurity, critical infrastructures, national security, disruption, national cybersecurity strategy.



INTRODUCCIÓN

Mucho se ha dicho de la era digital y altamente tecnológica en la cual vivimos, pero nunca será suficiente, cada cosa dicha, cada frase acuñada, cada curso impartido, cada medida tomada, cada regulación creada y cada nota informativa publicada aportan mucho al tema, propiamente al de la cultura de la seguridad, pero ya es insuficiente, hay muchas cosas que proteger que van más allá de la cartera, el auto o la casa… notas informativas cotidianas reportan diariamente un apartado incluso específico, de aquellos incidentes o delitos cometidos a través de la tecnología o teniendo a ésta como objetivo, lo cual ya lo hace muy grave dado que ¡se está clasificando a la inseguridad misma!, y por tanto a los actos delictivos que le caracterizan, por tipo o gravedad de los mismos; lo cual no sería posible si no fuera tan variada, de hecho, podría sucederle a cualquier persona, empresa o gobierno y sucede no recientemente.

Hablar de inseguridad es cotidiano en cualquier lugar del mundo, ya que, en el momento histórico actual, con sus variadas y robustas herramientas tecnológicas, informatización generalizada, innovación y nuevos negocios y el excesivo flujo e intercambio transfronterizo de información por minuto, se realiza, pero sin saber mucho de la protección de la información y sin importar quién es el destinatario final, por un lado; por otro, si bien el momento y la propia tecnología con sus cada vez más variados entornos "Ciber", presenta un escenario de nuevas e impactantes oportunidades, implica a la vez nuevos retos y claramente nuevos riesgos, transformando tal cúmulo imparable de oportunidades que la conectividad y la interconexión[1] ofrecen, en un potencial imparable de riesgos y amenazas en el ciberespacio[2] y recientemente denominado ciberentorno[3], lo que es motivo suficiente para entender[4], informarse, atender, prevenir y proteger los activos de información y crear o actualizar la regulación jurídica necesaria que determine la responsabilidad de quien actúe lesivamente, tal como sucede en la vida cotidiana; incluido un cambio radical de pensamiento que supere los conceptos tradicionales de seguridad y por supuesto de inseguridad, para lo que la expresión Ciberseguridad es ideal, ya que contiene todos los campos de conocimiento necesarios para elevar al máximo, el nivel de seguridad que pueda tenerse y que nunca será ni perfecto, ni absoluto.

La necesidad de Ciberseguridad debe convertirse en una inclusión obligada legalmente en el tema, desde los aspectos introductorios hasta la aplicación y monitoreo de la situación y avances actuales. Incluso la creación de un observatorio internacional que facilite el aprendizaje, la generación de recursos humanos, materiales, herramientas, profundización en cifrado, y temas selectos de ciberdefensa para cuerpos especiales, generación de leyes modelo, homologación de definiciones, que de preferencia estuviera relacionada con algún tratado existente o nuevo, que facilite en la región los parámetros actuales de Ciberseguridad de todos, para todos dado el impacto masivo peligroso que tendría un ciberataque para cualquier país, ello facilitaría la protección de las distintas infraestructuras de un país; algo así como la ONU de la Ciberseguridad, lo más viable para un avance común en la protección de problemas comunes para la comunidad de países contra los ciberdelincuentes[5].

[1]Interconexión: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones.

[2]Ámbito artificial o lugar virtual donde usuarios de la red interactúan a través de un lenguaje, expresado en sentido de textos, imágenes, gráficos, sonidos etc., entendiendo dicha red como un tejido de computadoras interconectadas que guardan bases de datos y fuentes de información, a las cuales los usuarios pueden acceder. Genera situaciones de derecho reales a pesar de romper el ámbito espacial, es decir, se puede caer en una determinada situación sin importar la distancia de las mismas, dicha situación sigue generando consecuencias de derecho a pesar de que no se realicen en un plano físicamente tangible.

[3]Esto incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes o en dispositivos o la información que éstos generan. Las instalaciones y edificios donde residen los dispositivos también forman parte del Ciberentorno…"

[4] Los diferentes vocablos que han surgido y que continuarán surgiendo a partir de que, a cada conducta nueva se le asigne tal prefijo para diferenciarla de la conducta en la vida cotidiana, ejemplos de ello pueden ser las siguientes expresiones: Cibernauta, Ciberguerra, Cibernética, Ciberarmamento, Ciberataque, Cibernegocio, Ciberdelincuencia, Ciberconciencia, Cibertolerancia, Ciberinteligencia, Ciberaliados, Cibertratado o por qué no…Ciberpaz.

[5] Aquella persona (s), entidad y/o organización, interna o externa al sujeto pasivo o agraviado, que dolosa e ilícitamente realiza cualquier acto considerado hostil, directo o indirecto de cualquier intensidad, nivel, tipo y por cualquier medio contra la comunidad global de personas o naciones, contra su información, procesos, datos, infraestructura, sitios web, equipos o redes con cualquier fin, protegida o no, logre o no su objetivo. (Definición propia).

A manera de referente, el panorama señalado por el informe de la OEA (2014), "Tendencias de Seguridad Cibernética en América Latina y el Caribe", en América Latina y el Caribe este tipo de delitos cuesta alrededor de US$90,000 millones al año. Por su parte para tener como referente más actual, el propio informe de la OEA (2016), "¿Estamos preparados en América Latina y el Caribe?", que señala que en su calidad de cibercrimen, éste le costaba cada año al mundo hasta US$575,000, 2 millones al año, 0.5 por ciento del producto interno bruto global, lo que representa casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional, baste decir. (ENC:2017)

Ante un panorama nada esperanzador -como si no fueran suficientes las amenazas ya existentes-: por lo que es urgente, adecuar nuevas definiciones hasta cambiar la forma de pensamiento sobre la forma de proporcionar seguridad a la información y a las infraestructuras nacionales, ya que la seguridad tradicional debe adecuarse y mejorar permanentemente, ya que no solo se trata de proteger además de delincuentes comunes con delitos tradicionales, hasta protegerse ante la presencia ilícita, impactante y global de un relativamente nuevo tipo de delincuencia; sin duda alguna esto a través del aprendizaje obligado de la Ciberseguridad como nuevo modelo de protección de las infraestructuras de los países y a propósito de las conocidas ventajas que conlleva el trabajo conjunto de éstos, lo que justifica inequívocamente su aprendizaje y lo que parece la única manera de enfrentar, exitosamente, a la nada menos que ¡Delincuencia informática organizada!

SEGURIDAD CIBERNÉTICA A LAS INFRAESTRUCTURAS CRÍTICAS

El tema esencial para vivir con cierta tranquilidad y paz en la sociedad actual de cualquier lugar del mundo, es el tema de la seguridad, pública, personal o nacional, y recientemente de la seguridad de la información, término perfeccionado en su definición y aplicabilidad, y que en algunos años se ha dado en denominar Ciberseguridad, misma a la que se puede definir así:

ENC (2017) (México): "Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación."

UIT–T X.1205 (2010): "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno… Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad, integridad, que puede incluir la autenticidad y el no repudio; confidencialidad."

Definiciones necesarias que implican atender y elevar el nivel de seguridad de la información, ya que de ser accesada, vulnerada, atacada, expuesta o copiada, puede incluso poner en entredicho la reputación, el trabajo, la seguridad personal y familiar y en el caso de los estados y sus gobiernos, ¡la continuidad de los servicios públicos que prestan a los ciudadanos, necesarios para la continuidad de la vida misma de las personas!, en el peor de los casos el gravísimo colapso de éstos. Es aquí donde aparecen las diversas infraestructuras de los estados, ya que son precisamente éstas a través de las cuales se prestan esos servicios y existen en todos los países, lo que justifica su importancia global.

Se trata de proteger y salvaguardar los bienes más preciados en el momento social actual -activos que usuarios, empresas y gobiernos poseen-, donde el enemigo, el riesgo o el atacante, es: anónimo, especializado e invisible, ¡casi nada!, de ahí que el tema sea tan importante, porque las potenciales víctimas (los estados), no saben necesariamente, que deben prepararse para protegerse de personas, gobiernos, analfabetismo digital, desobediencia profesional, incumplimiento laboral, la obsolescencia jurídica o la continuidad de su aplicación cuando existe la normativa, donde el ideal sería la existencia de la propia Estrategia Nacional de Ciberseguridad para todos los países, porque los riesgos existen y seguirán existiendo, tan sencillo y tan confuso ya que se trata de protegerse de algo que podría o no, atacar; nada parecido a la vida cotidiana donde la mayoría es consciente para enfrentar de alguna manera a la delincuencia -que denomino solo para efectos didácticos- "tradicional", si se permite la expresión.

En principio, no entender que la seguridad absoluta no existe[6], poca atención provoca en los gobernantes respecto de la seguridad física, de la información de personas y gobiernos, la protección de todo tipo de recursos, de información, sistemas, de fronteras, comunicaciones, de los aspectos físicos, geográficos e informáticos, tan necesarios de proteger (hasta años recientes); lo que en sí mismo es una vulnerabilidad[7], donde la definición que se use para explicar el nivel de seguridad y atención que se tenga de ésta, depende de la óptica de estudio o de la autoridad que la defina, y lo que por ella debe entenderse para concientizar, aplicar y proteger, y en el peor de los casos defender.

Dados los argumentos vertidos, es que se convierte en cuestionable la poca atención al tema por algunos gobiernos, atendiéndose más veces solo por cuestiones políticas del gobierno en funciones –políticas, presupuestos, agenda, planes de desarrollo, etc.-, que con un programa o normativa permanente de protección de las funciones de salvaguarda de la seguridad nacional y sus infraestructuras, podría mantenerse eficiente, eficaz y fuerte; superando así, los planes de trabajo y plataforma política de los cambios de gobierno, la apatía por los temas de trabajo del gobierno anterior, planificación presupuestal o la propia brecha digital/generacional; lo que es justo, necesario, responsable y jurídicamente exigible. Con independencia del país, solo algunos gobiernos se han preocupado por informatizar algunos de sus servicios a través de la implementación de figuras como la del gobierno electrónico o e-gobierno[8] por ejemplo, que, si bien cumple cabalmente con el derecho humano de acceso a la información[9], no implica acciones de Ciberseguridad y menos aun involucra la protección cibernética de las infraestructuras del estado, y la poca atención es en su mayoría verdaderamente insuficiente, de forma que al accesarse ilícitamente a datos e información, ésta es considerada vulnerada y/o expuesta y ello puede suceder en un sin fin de ocasiones, donde el esfuerzo por continuar direccionando y facilitando las funciones de seguridad ciudadana y seguridad nacional del estado, así como la falta de acciones específicas, no necesariamente facilitan la protección de la información.

Ante tal escenario deben sumarse las amenazas existentes, –que no son precisamente lo que se conoce como "tradicionales"- lo que deja, permite visualizar un escenario a decir lo menos preocupante y urgente no solo para la seguridad de la información, literalmente para la propia seguridad nacional, como lo refiere excelentemente Baralt (2017), en su trabajo intitulado "Un reto para la Defensa Nacional en entornos intangibles", expresión que aplica perfectamente al presente trabajo, donde se particulariza en las infraestructuras críticas del estado y cuya inminente necesidad de protección, se corrobora con los innumerables trabajos realizados a nivel internacional que en diversidad de eventos y foros de intercambio de experiencias incluidas por supuesto, la diversas fuerzas de defensa y militares de los países participantes, son quienes encabezan la función protectora y defensora del estado, como en cualquier país, aportando a la comunidad internacional de países, información e investigación relevante de su experiencia, donde sin embargo, nunca son suficientes espacios de intercambio o siempre naciones ausentes.

Dadas primeramente las amenazas[10] existentes (riesgos, desastres naturales[11], conflictos sociales, ciberataques, entre otros tipos de incidentes de seguridad), en segundo lugar las debilidades[12] (p.e.

[6]El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de Titanio, encerrado en un búnker de concreto, rodeado por gas venenoso y cuidado por guardias muy armados y muy bien pagados. Aun así, no apostaría mi vida por él.

[7]Las debilidades identificadas en la ciberseguridad dentro de las dependencias o entidades de la APF, los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las empresas productivas del Estado, los Gobiernos Estatales, Municipales y Delegacionales, así como los particulares que potencialmente permiten que una amenaza afecte los activos de TIC, a la Infraestructura Información Esencial, así como a los Activos de Información.

[8]El gobierno electrónico es la aplicación de las tecnologías de la información y la comunicación (TIC) al funcionamiento del sector Público, con el objetivo de incrementar la eficiencia, la trasparencia y la participación ciudadana que tiene el gobierno de un país con sus gobernados".

[9]…la Corte Interamericana de Derechos Humanos ha señalado … "el concepto de orden público reclama que, dentro de una sociedad democrática, se garanticen las mayores posibilidades de circulación de noticias, ideas y opiniones, así como el más amplio acceso a la información por parte de la sociedad en su conjunto..."

[10]Amenaza: cualquier elemento, conducta, actividad, proceso, automático o manual, de cualquier índole, que aprovecha una vulnerabilidad generada o existente, para atentar contra la seguridad de un activo de información o de alguno de sus componentes y/o equipos y/o sistemas y/o procesos y/o software y/o redes y/o sitio web, comprometiendo la continuidad de la operación de la infraestructura y/o del servicio público prestado, se logre o no el objetivo de la amenaza.

[11]Aquéllos sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta: fuego y/o rayo), daños por agua (desbordamiento de un rio), otros desastres naturales (tornados o temblores).

[12]Debilidad: que puede poner en peligro la información, operación o infraestructura y alguno de sus componentes y/o equipos y/o sistemas y/o procesos y/o software y/o redes y/o sitio web, comprometiendo la continuidad de la operación de la infraestructura y/o del servicio público prestado, que provoque una afectación o daño grave y/o inmediato y/o general para el país o a alguno de los estados que lo conformen.

la falta de presupuesto o de concienciación o concientización[13]), en tercer lugar los riesgos[14] inminentes (ransomware, espionaje, terrorismo, ataques dirigidos o intencionados[15], y las correspondientes actividades "Cyber" de los ciberataques en general–conocidos también como defensa activa-), en cuarto lugar la escasa atención al desarrollo del tema en las agendas de algunos Estados[16] se suman nuevos entornos de riesgo como son: uso indiscriminado de Apps contaminadas, plataformas informáticas alojadas en otros países, las nubes o entorno cloud, la expansión de centros de datos (datacenters), el necesario flujo de datos transfronterizos, el internet de las cosas (IoT), la videovigilancia, los radares civiles y militares, las WiFi o redes abiertas; la falta de protocolos particularizados, los actos cotidianos de ciberespionaje, el analfabetismo tecnológico y la ausencia legislativa –que son un riesgo en sí mismos-, puede asegurarse que el panorama no es alentador y si muy atemorizante y urgente.

Lo anterior, sin considerar que exista un tipo penal ideal, garante y protector de las infraestructuras del estado y la información y procesos que contengan, y que podría presentar sus propios problemas ya que los elementos de la conducta típica no suelen reunirse en su totalidad ni fácilmente, ya que muchas veces la información no fue accesada u obtenida inmediatamente, los atacantes suelen estar presentes desde muchos meses antes, por lo que no se conoce mucho del proceso del ataque ni del dominio exacto de información que poseen, lo que dificulta la investigación y la correlativa relación con la tipificación criminal, en su caso, todo ello sin siquiera precisar el necesario contexto legal que debe aplicarse, -de existir éste-, lo que representa un grave problema de seguridad nacional por supuesto, ya que la ausencia o la obsolescencia normativa, solo dejan como resultado, pérdidas, daños e impunidad y provocan un estado de indefensión permanente.

Tratándose de tecnología y para el caso de estados y sus gobiernos, es que el hablar de Ciberseguridad se convierte en determinante dada la alta y necesaria dependencia tecnológica de éstos, lo que justifica fundadamente la protección de sus entidades públicas, misma que está considerada en la propia recomendación UIT Rec. UIT-T X.1205 (04/2008:2), por eso, proteger su seguridad perimetral, seguridad de la información y la de todos sus tipos de infraestructuras es primordial, prioritario y deseable, ya que avanzar en el modelo de madurez del uso y protección de la tecnología, no es nada fácil donde muchas veces los procesos de sucesión presidencial que se vive en cada país en algún momento producen la interrupción de los trabajos y funciones de protección, gestando cambios en políticas públicas, agendas, estrategias o el abandono de éstas, lo que es contrario al modelo de continuidad que sobre la protección de las infraestructuras esenciales y las infraestructuras críticas debe existir, por ello, el cambio de pensamiento es esencial, de ahí la presente propuesta denominada "Ciberseguridad: Aprendizaje disruptivo en la protección de Infraestructuras Críticas y la Seguridad Nacional", entendiéndose como disruptivo el hecho de que gracias a la aplicación directa de la Ciberseguridad, se produzca necesariamente una ruptura simbólica en la forma de trabajo y protección que brindan algunos Estados a sus infraestructuras críticas, superando significativamente la protección tradicional. Cambio determinante para la continuidad de los servicios públicos prestados a través de aquéllas, ante los riesgos propios o las vulnerabilidades del ciberentorno.

Al hacer referencia a una entidad pública como objeto de protección, se alude a las instituciones, dependencias y en general a cualquier secretaría, área, departamento, institución, dependencia, oficina, instancia, etc., que forma parte de la organización de la ad-

[13]Errores de los usuarios, del administrador o de configuración, deficiencias en la organización, alteración de la información, introducción de información incorrecta, degradación o destrucción de información, divulgación de ésta, falta de actualización de sistemas y programas.

[14] Riesgo : aquél que puede poner en peligro la información confidencial o sensible de personas, grupos vulnerables, financiera, presupuestal, identificativa, de salud, proveedores, de procesos, servidores públicos, expedientes judiciales, empleados, funcionamiento, investigaciones criminales, investigaciones científicas sobre la salud, operativos de seguridad ciudadana o pública, procedimientos internos, control y acceso de sistemas informáticos, de vigilancia, funcionamiento o distribución, etc. Comprometiendo la continuidad de un servicio o exponiendo información aún no firme o definitiva, de carácter estrictamente confidencial y de alta seguridad, incluso seguridad nacional.

[15] Manipulación de la configuración, suplantación de la identidad, abuso de privilegios de acceso, acceso no autorizado, interceptación de información (escucha), modificación de la información, denegación de servicio (ataque Dos o DDos). Debe precisarse que cuando un riesgo se vuelve real, causa invariablemente un incidente.

[16] Información fundamentada en otros materiales, como en los hallazgos que indican que analizados los datos de 191 entidades bancarias de toda la región de Latinoamérica, el 49% de las entidades bancarias aún no están implementando herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como Big Data, Machine Learning o Inteligencia Artificial, las cuales resultan muy importantes a la hora de prevenir ciberataques, (OEA:2018), por ejemplo; lo que indica por simple sentido común, que si los sistemas financieros que son un sector de lo más interesante para los criminales (véase: Harán J.M.:2018), no tiene la protección suficiente que aporta la ciberseguridad, entonces queda claro el porqué, no es posible encontrar mayor interés en la protección de las diversas infraestructuras de los países.

ministración pública de un país, para el caso de México, ejemplos de entidad pública serían las siguientes: la Oficina de la Presidencia de la República, las Secretarías de Estado, la Consejería Jurídica del Ejecutivo Federal, los Órganos Reguladores Coordinados en Materia Energética, entre otros, lo cual significa que prácticamente toda la administración pública de un país, debe estar incluida en la categoría de dependencia pública y por ende ser sujeto de protección.

Por otro lado, cuando se habla de infraestructuras críticas, claramente se hace alusión a un solo tipo de éstas, sin embargo, existen claras definiciones que diferencian el tipo de infraestructura (s) que puede existir en un país, a saber:

Infraestructuras estratégicas: Ley 8 (2011) (España), Artículo 2, inciso d): "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales."

Infraestructuras críticas: ENC (2017:21) (México): "… acciones encaminadas a establecer las acciones y mecanismos necesarios para minimizar la probabilidad de riesgos y vulnerabilidades inherentes en el uso de las TIC para la gestión de infraestructuras críticas, así como para fortalecer la capacidad de resiliencia[17] para mantener la estabilidad y continuidad de los servicios en caso de sufrir un incidente de ciberseguridad."

Ley 8 (2011) (España): Artículo 2, incisos: "**e)** Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre dichos servicios … **k)** Protección de infraestructuras críticas: el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia."

Directiva 2008/114/CE del Consejo (Unión Europea): "Artículo 2, inciso a): "El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;"

Como se desprende de las definiciones referidas, la diferencia entre los tipos de infraestructura es determinante para saber el nivel de protección que estas necesitan y el impacto que podría desencadenarse si fueran expuestas o atacadas y cualquiera de ellas claramente forma parte de alguno o de todos los órdenes de gobierno y muchas de ellas, son componente indispensable para la prestación de un servicio público esencial y en el caso más grave, inhabilitar el servicio o proporcionarlo pero integrar en él un elemento adicional que afecte directamente a toda la población que lo recibe, donde el servicio es el vehículo utilizado para ocasionar la afectación lo que permite clasificar en afectación directa de la infraestructura, teniendo a ésta como objetivo o usando a esta como medio para la comisión de un daño, por supuesto en el caso de la infraestructura critica sería más grave la afectación ya que se trata de aquellas que son de vital importancia para el mantenimiento del Estado o la seguridad nacional, incluso para la supervivencia de la vida.

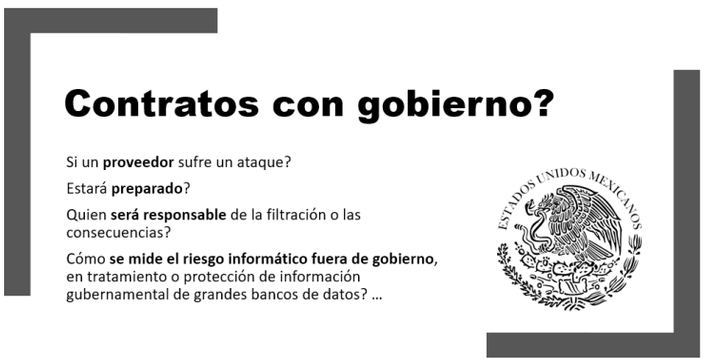
Los principales riesgos y amenazas a un país podrían involucrar alguno o varios de los aspectos que formen parte de la estructura funcional, jerárquica u organizativa de los siguientes servicios proporcionados por un estado:

1. Administración (servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional)
2. Instalaciones espaciales; Industria Química y Centrales Nucleares (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.)

[17]Ciber resiliencia puede entenderse como lo define Carrasco (2015) al decir: "…se ha definido partiendo de la definición de resiliencia y restringiendo las posibles fuentes de crisis a eventos tecnológicos y procedentes del ciberespacio, o también se ha definido limitando la dimensión afectada de la empresa a lo que son sus sistemas de proceso de datos y sus comunicaciones. Dada la complejidad de las organizaciones, y la interdependencia entre los distintos elementos que las forman: personal, entorno social, suministros, infraestructura TIC, procesos, ...; no se puede trazar una línea divisoria clara entre lo que supone la resiliencia de la misma y la ciber-resiliencia de sus sistemas. Una y otra están íntimamente relacionadas, es más, son un mismo concepto. No se puede crear una infraestructura tecnológica ciber-resiliente si la organización en sí no es resiliente."

3. Agua (embalses, presas, almacenamiento, tratamiento y redes de distribución)
4. Centrales y Redes de energía (producción y distribución)
5. Gasoductos (extracción, almacenamiento y distribución)
6. Tecnologías de la Información y las Comunicaciones (las existentes, independiente del nivel de reducción de la brecha digital)
7. Salud (sector e infraestructura sanitaria hasta su usuario final)
8. Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, logística, etc.)
9. Alimentación (producción, almacenamiento y distribución)
10. Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones)
11. Infraestructuras defensivas nacionales (militares, aéreas y navales, oficiales, encubiertas y de contrainteligencia).

Además del listado anterior, deben reconocerse otro tipo de peligros, como el de la subcontratación o descentralización en la prestación de un servicio público, es tema de particular atención ya que existe mucha probabilidad de que la empresa privada que controle la prestación del servicio público estatal, no tenga la Ciberseguridad necesaria para proteger muchos aspectos la actividad adecuadamente.



Considerando que difícilmente existen protocolos de supervisión a terceros, un buen ejemplo de esto es el sucedido en 2018 con Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día, donde los temas centrales se relacionaron con acusaciones de robo de datos, interferencia política, chantajes y la adquisición indebida de información de por lo menos 50 millones de usuarios, solamente en Estados Unidos. Si hipotéticamente colocáramos a cualquier gobierno en el lugar de Facebook y a una empresa privada trabajando para éste la prestación de algún servicio público (conocido como descentralización), podría suceder lo mismo, el que un estado esté preparado -en el mejor de los casos- en Ciberseguridad, no asegura que quienes trabajen legalmente para éstos, estén tan preparados como el estado contratante.

Los servicios públicos referidos, se encuentran relacionados directa o indirectamente con la seguridad nacional o su información, entendiéndose esta en lo expresado por la Ley de Seguridad Nacional (2005) (Mexicana), Artículo 6, fracción 5 como: "…los datos personales otorgados a una instancia por servidores públicos, así como los datos personales proporcionados al Estado Mexicano para determinar o prevenir una amenaza a la Seguridad Nacional", de manera que es una de las funciones primordiales y prioritarias de cualquier estado, solamente realizado por su ejército, fuerza armada, la marina y/o la fuerza aérea, independientes o en conjunto, como en México que en éste último caso se le conoce como "Fuerza armada permanente" y que en términos de la ley referida indica: "Artículo 3.- Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

I. La protección de la nación… frente a las amenazas y riesgos…;
II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;…
V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional,…"

Adicionalmente y de forma clara especifica también: "Artículo 5.- Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. Actos tendientes a consumar espionaje, sabotaje, terrorismo, … en contra de los Estados Unidos Mexicanos dentro del territorio nacional;
II. Actos de interferencia extranjera en los asuntos nacionales;…
V. Actos tendentes a obstaculizar… operaciones militares o navales…;

VI. Actos en contra de la seguridad de la aviación;
VII. Actos que atenten en contra del personal diplomático;…
IX. Actos ilícitos en contra de la navegación marítima;…
XI. Actos tendentes a obstaculizar… actividades de inteligencia o contrainteligencia, y
XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico… para la provisión de bienes o servicios públicos."

Normativa que considerando que existen diversos actos posibles y que de cualquier forma puedan afectar a la seguridad nacional, serán invariablemente considerados como una amenaza a ésta, estableciéndose en la última fracción precisamente el tema que nos ocupa, refiriendo a los dos tipos de infraestructura más importantes, la infraestructura estratégica y aquella propiamente critica, dado lo cual en México cualquier ataque a este tipo de infraestructuras es considerado un ataque a la seguridad nacional, donde el cambio disruptivo no seria de orden normativo en principio, sino de continuidad de los trabajos realizados desde hace ya poco más de seis años.

Debe tenerse presente que, desde una óptica jurídica y de derecho internacional, es todo un reto el uso de tecnología para tres figuras del Derecho Internacional relacionadas con el conflicto y que aun en la actualidad generan polémica, siendo éstas: a) Uso de la fuerza (ataques armados con la aplicación de la tecnología conocidos como ciberataques), b) El espionaje o el ciberespionaje y c) El terrorismo o ciberterrorismo; temas difíciles y sensibles para la comunidad internacional de países, ya que representan muchas dificultades legales principalmente, desde la falta de precisión territorial (jurisdicción), hasta el problema de las definiciones homogéneas. Sin embargo, hay que recordar que para muchos estados, los principios del Derecho Internacional sí le aplican, ya que solo son nuevas herramientas en caso de conflicto internacional, pero ello no cambia el conflicto, solo lo diferencia de territorio y de armamento, y para responder precisamente a ese problema, se encuentra el Derecho Internacional, que provoca a su vez otros cambios en diversas ramas del mismo, como lo son el Derecho Humanitario Internacional y el Derecho de Guerra principalmente. (Morán:2013)

De esta manera es como el ciberespacio -contrario a lo que pudiera pensarse-, no es una zona totalmente libre de leyes donde cualquiera puede llevar a cabo todo tipo de actividades y conductas, incluyendo las hostiles; paulatinamente se aprecia que la norma jurídica tiende a regular conductas y aspectos de dicho entorno, solo que este proceso es bastante lento dado que no se esperaba la variedad y cantidad de amenazas que ahora se sabe que existen y de las cuales se han desprendido incalculables daños financieros en diversos países del mundo. Lamentablemente los aspectos regulatorios, llevan mucho trabajo y tiempo, ya que éstos se establecen precisamente en función de la aparición de los ciberataques -situación que precisamente propone este trabajo a contrario sensu para no esperar a que sucedan-, considerando que es un hecho cierto la comisión de éstos actos humanos o conductas que han sido inequívocamente hostiles y que pese a los esfuerzos de los atacantes por evitar ser localizados e identificados, suele conocerse en breve su estrategia, tiempo de ejecución y cuantificación aproximada de daños; donde el problema principal radica en el orden jurídico aplicable, debido a que para la determinación de la responsabilidad y su respectiva sanción, -como en cualquier otro delito-, deben identificarse con precisión los principios jurídicos aplicables a las circunstancias incluyendo la comisión de otras conductas delictivas, con ello determinar la norma jurídica adecuada y la jurisdicción que corresponda, sin embargo no siempre sucede, debe recordarse que si bien el Derecho Internacional es aplicable en una gran parte del territorio internacional, es precisamente en los territorios sujetos a excepción, donde los verdaderos ataques se organizan, atentando pública y cínicamente contra todo ordenamiento o tratado internacional que exista y su aplicación.

Debe decirse al respecto que en ciertas circunstancias, las actividades en el ciberespacio pueden ser consideradas como uso de la fuerza nacional o internacional, eso con base en el Artículo 2 párrafo 4 de la Carta de las Naciones Unidas (ONU:1945), que manifiesta: "Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas." Dicha Carta también establece que un estado puede responder a un ataque por internet -lo que ahora denominamos el Ciberespacio-, ejerciendo su derecho de legítima defensa en el caso de que el ataque sea equivalente a un ataque armado, ello con base en el Artículo 51 del mismo documento que establece: "Ninguna disposición de esta Carta menoscabará el derecho inminente de legítima defensa, individual o

colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales."

Es de esta forma como la propia Carta de las Naciones Unidas usa el término ataque armado para describir los actos contra los cuales está permitido el uso de la fuerza a través del derecho de legítima defensa, como se analizaba de la pr opia Ley de Seguridad Nacional en el caso de México, sin embargo, es innegable la relación entre los conceptos de agresión[18] y ataque armado, es decir, por ele- mental inteligencia y mínimo sentido común, es claro que todos los ataques armados se pueden equiparar a una agresión directa, pero también debe recordarse que la expresión "ataque armado" no está definida por ninguna convención y su significado está abierto a la interpretación de los Estados, de ahí que deba aplaudirse el esfuerzo de las regulaciones jurídicas de los países que si definen éstos preceptos.

Paralelamente, debe destacarse la propuesta de Feffrey (2012), quien explica los modelos utilizados para identificar si un ciberataque es un ataque armado: "El primer modelo es … basado en el enfoque, que comprueba si el daño causado por un nuevo método de ataque anteriormente podría haber sido logrado sólo con un ataque cinético. El segundo es … basado en los efectos… consecuencia, en la que la similitud del ataque a un ataque cinético es irrelevante y la atención se centra en el efecto general … estos tienen como víctima al Estado. El tercero es … de responsabilidad estricta, en la que los ciberataques contra infraestructuras críticas son tratados automáticamente como ataques armados, debido a las graves consecuencias que pueden derivarse de la desactivación de los sistemas."

Tal y como se ha venido identificando y con base en la clasificación de enfoques del autor, el ciberataque a una infraestructura crítica puede ser equiparado a un ataque armado, debiendo precisar que a este criterio también le son aplicables la consideración de los daños económicos causados, ya que el derecho internacional establece que los ataques económicos también son aplicables a la legítima defensa o autodefensa; daños que innumerables comunicados oficiales demuestran han existido y han sido consecuencia directa de ciberataques. Como si no fuera suficiente, debe sumarse a los criterios analizados y como refuerzo de éstos, lo establecido por Jens Stoltenberg, secretario general de la alianza militar de ministros de Defensa de la OTAN en 2017, dijo que la alianza estaba "…en el proceso de establecer al ciberespacio", como un dominio junto con la tierra, el mar y el aire, lo que significa que un ataque cibernético teóricamente podría accionar el Artículo 5 del tratado que está relacionado con la defensa colectiva, lo que significa que la OTAN, establece el ciberespacio como un dominio militar legítimo, donde se consideraría un ciberataque a una nación miembro como si afectara a los 29 aliados de la organización.

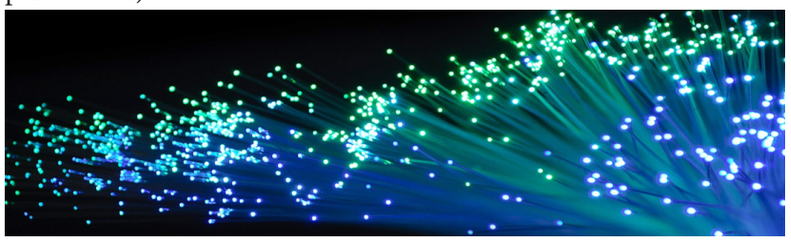
En la asignación de responsabilidad en la comisión de ciberataques, hay que remarcar que los Estados son legalmente responsables por las actividades de sus órganos, personas o instituciones siempre que actúen bajo su control, por tanto, hay responsabilidad internacional inmediata en esta materia. Por otra parte, en cuanto al tema de la intensidad de la autodefensa, se encuentra relacionada con los principios de distinción y de proporcionalidad, de tal forma que no contribuya a preservar el esfuerzo de guerra, de forma que la autodefensa debe ser proporcional al daño recibido y la acción debe darse para evadir un daño mayor sin afán de castigo o venganza. Lo que significa que el ciberespacio es oficialmente un territorio más donde desencadenar una guerra con tal de proteger los bienes jurídicos[19] de todos, tarea muy complicada si se tiene presente que el ciberdelito va en aumento año con año.

Quedan en el tintero algunos otros aspectos, dado que día a día la Ciberseguridad se vuelve más importante, como se comprueba

[18]Agresión: "…es cualquier uso ilegal de la fuerza, cualquier uso … que no sea legítima defensa contra un ataque armado o acción coercitiva por las Naciones Unidas.

[19]Bien jurídico, es de origen jurídico doctrinal y se refiere, en palabras de la Universidad de Navarra (s.f.), ".. a .. aquella realidad valorada socialmente por su vinculación con la persona y su desarrollo. Vida, salud, integridad, libertad, indemnidad, patrimonio… son bienes jurídicos. Pero también lo son la Administración pública, entendida como conjunto de circunstancias de funcionamiento de la Administración que posibilitan el desarrollo de las personas; también la Administración de Justicia, el medio ambiente, la salud pública…", tratándose de los bienes que debe proteger cualquier estado.

con su inclusión desde videojuegos hasta miniseries televisivas, por ello solo se enuncia uno de los pendientes más importantes: el problema de la inversión financiera (unos para protegerse y otros para atacar).



Aprender
Beneficiarse y
Crear conciencia ...

Para prevenir y afrontar a la
Ciberdelincuencia
apostando por una
Cultura de la Ciberseguridad

CONCLUSIÓN

En la actualidad el mundo globalizado, ampliamente informatizado e hiperconectado exige Ciberseguridad, ya que hace frente a riesgos y vulnerabilidades propias. Ello presenta un claro escenario de retos y desafíos en el tema, que además de fortalecerse deba transformarse y mejorar permanentemente, sumando el trabajo transdisciplinario que sea necesario para disminuir el riesgo latente al que todos los sectores -personas, empresas y gobiernos- estamos expuestos, evitando que al sumar las vulnerabilidades propias, se llegue a en peligroso estado de indefensión. A manera de conclusiones, se enlistan cuatro rubros que justifican realizar el pensamiento disruptivo que considere la aplicación de la Ciberseguridad como aprendizaje necesario e ideal en la protección de las Infraestructuras Críticas existentes y la Seguridad Nacional de nuestros países, basadas en un enfoque integral, a saber:

Técnicas: Uso de cifrado obligatorio; dobles autenticaciones (incluidas biométricas); crear "estándar modelo" único de gestión de riesgos, inclusión de diagnósticos de vulnerabilidades; realización de cibersimulacros, creación de alerta nacional; creación de centros de sensibilización y concienciación; auditorías integrales aleatorias (interconectadas entre instancias gubernamentales y con los CERT existentes); diseñar y considerar a la resiliencia cibernética en los procesos internos; diseño de herramientas, metodologías y operarios propios.

Sociales: Potenciar el aprendizaje en ciberseguridad incluido uso ético y responsable de la tecnología; fortalecer la cooperación con entes privados para mejora continua y desistimiento voluntario de conductas de sabotaje (eslabón más débil). Concientizar a los ciudadanos que la tecnología es una herramienta, no un arma.

Económicas: Priorizar la inversión estatal en ciberseguridad; atender acciones de Inversión en capacitación, investigación y formación en Ciberseguridad.

Jurídicas: Homologar definiciones generales útiles para las normas jurídicas, catalogar específicamente las infraestructuras críticas del país incluyendo al internet como una de éstas; sumarse o crear un tratado específico de Ciberseguridad que procure la cooperación e investigación internacional de delitos en las infraestructuras estratégicas y críticas[20]; sustituir las estrategias nacionales por legislación especial; convertir a la Ciberseguridad como objetivo común; incremento y reforzamiento permanente, de la capacidad táctica, operativa, de inteligencia y contrainteligencia (ciberdefensa) nacionales, con un equilibrio respetuoso de capacidades, jerarquía y funciones en ciberseguridad, evitando la militarización del ciberespacio y evitando llegar a los excesos, homologando el concepto real y jurídico de soberanía nacional digital, sin alimentar la ciberguerra que se dice hace tiempo ya comenzó.

Siendo los riesgos actuales desde el malware, la inteligencia artificial, los riesgos del Big Data, la videovigilancia, las nuevas redes (5G), hasta las Fake News que ocasionan riesgos por el impacto y movilidad social que generan, estos son los razonamientos, razones y motivos suficientes, para proponer y apostar por una cultura general y obligada de la Ciberseguridad como una prioridad de Seguridad Nacional en la política de los estados, que debe sucederse desde la disrupción del pensamiento tradicional de protección de las infraestructuras críticas, para superar la constante de aprender, desarrollar y aplicar Ciberseguridad solo hasta después de que suceda algún incidente.

[20]Como el caso de la Unión Europea que el 17 de mayo de este 2019, anunció que ya se aprobó un régimen para sancionar los ciberataques y se encuentra trabajado conjuntamente en el proceso de atribución de éstos a algún país, ya que la Unión no posee esa facultad.

REFERENCIAS

Abril, C. G. (2010). *El cuarto bios. Estudios sobre comunicación e información.* Madrid, España: Editorial Complutense.

Baralt B. N. (2017). Ciberseguridad: Un reto para la defensa nacional en entornos intangibles. *Revista Seguridad, Ciencia & Defensa. 3*(3), 53-71. Recuperado de http://revista.insude.mil.do/index.php/rscd/article/view/6/27

Carrasco, L. de S. (2015). Ciber-resiliencia, documento de opinión en web. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

Instituto Nacional de Estudios Históricos de las Revoluciones de México. (2015). *Derecho humano de acceso a la información.* México: CNDH. Recuperado de http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DHAccesoinformacion.pdf

Critifense. (2018). *Critical infrastructure cyber attack timeline*. Recuperado de http://www.critifence.com/papers/attack-timeline/files/SCADA%20Cyber%20Attacks%20Timeline

Directiva 2008/114/CE del Consejo (Unión Europea) (2008). *Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.* Siario oficial de la Unión Europea. Recuperado de https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Estrategia Nacional de Ciberseguridad. (2017). México. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Feffrey C. (2012). *Inside Cyber Warfare.* (2ª. ed.). New York, United States of America: O'reilly Media.

Harán J. M. (2018). Los ciberataques dirigidos a bancos más importantes de los últimos tiempos. Recuperado de https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/

Ley 8. (2011). *Medidas para la protección de las infraestructuras críticas.* Jefatura del Estado, «*BOE*» núm. 102, de 29 de abril, Referencia: BOE-A-2011-7630, España. Recuperado de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Ley de Seguridad Nacional. (2005). México. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

Ley Federal de Telecomunicaciones y Radiodifusión. (2014). México. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_311017.pdf

Ley Orgánica de la Administración Pública Federal. (1976). México. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/153_120419.pdf

Morán E. A., Servín C. A. y Alquicira G. O. (2013). TIC (internet) y ciberterrorismo. *Seguridad*, 23. México: UNAM. Recuperado de https://revista.seguridad.unam.mx/numero23/tic-internet-y-ciberterrorismo

OEA. (2010). *Definición de e-gobierno*. Recuperado de http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx

OEA. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe.* Recuperado de https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

OEA. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016.* Banco Interamericano de Desarrollo. Observatorio de la Ciberseguridad en América Latina y el Caribe. Recuperado de https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

OEA. (2018). *Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe*. Recuperado de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

ONU. (1945). *Carta de las Naciones Unidas*. Recuperada de http://www.un.org/es/documents/charter/

Pádinger, G. (2018). *Ciberataques a bancos latinoamericanos y el fantasma norcoreano: los afectados en 2018 y las amenazas para 2019*. Infobae, España. Recuperado de https://www.infobae.com/america/tecno/2018/12/22/ciber-ataques-a-bancos-latinoamericanos-y-el-fantasma-norcoreano-los-afectados-en-2018-y-las-amenazas-para-2019/

UIT-T X.1205. (2008). *Seguridad en el ciberespacio – Ciberseguridad, aspectos generales de la ciberseguridad, Sector de Normalización de las Telecomunicaciones de la UIT*. Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad Recomendación UIT-T X.1205. Recuperado de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-S&type=items

UIT–T X.1205. (2010). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. Actualidades de la UIT. Decisiones de Guadalajara*. Recuperado de https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Vicioso, H. J. (2015). La sanidad se prepara para un ataque terrorista. *Revista Médica, 60*. Recuperado de http://www.rmedica.es/edicion/260/la-sanidad-se-prepara-para-un-ataque-terrorista