La Armada de México y las Operaciones en el Ciberespacio
The Mexican Navy and Cyber Space Operations

Resumen

¿Qué es el Ciberespacio? ¿Qué son las Operaciones en el Ciberespacio? y con base en esto ¿La Institución puede realizar Operaciones en el Ciberespacio?, son las preguntas que se pretender responder con el presente ensayo, dentro de un marco conceptual con base jurídica.

Para tal efecto, explica que las Fuerzas Armadas operan en la dimensión física, mundo real en donde los humanos y máquinas se mueven y pelean, cuyos límites son definidos por las restricciones de las capacidades de los sentidos humanos; y que la información recolectada en esa dimensión física a través del espectro electromagnético, es usada para localizar fuerzas militares enmascaradas en espacio y tiempo, usando tecnologías furtivas. Posteriormente, expone que varios autores, manifiestan la necesidad de redefinir el espacio de batalla, ya que el concepto tradicional de guerra de maniobra puede ser obsoleto, dado que las fuerzas que la conducen operan en el espacio humano y éste representa la zona de muerte de la guerra futura.

Concluye señalando que la Armada de México:

1. Realiza algunas actividades relacionadas con las Operaciones en el Ciberespacio.
2. Que el marco jurídico vigente le permite a la Institución realizar actividades de monitoreo de sus redes de datos, comunicaciones e infraestructura que las soporta, a fin de evitar que se materialicen amenazas y,
3. Puede hacer uso de la información que fluye en el Ciberespacio incluida la anónima.

P: 47-71

Abstract

What is cyberspace? What are cyberspace operations? and based on this, is the Institution able to carry out cyberspace operations? These are the questions to be answered in this essay within a juridical conceptual framework.

For such a purpose, it is explained that the Armed Forces operate in the physical dimension, the real world where human beings and machines move around and struggle and whose limits are defined by the restrains in human senses capabilities; and that the information collected in that physical dimension through the electromagnetic range is used to locate military forces masked in space and time, using fortuitous technologies. Subsequently, it is explained that several authors express the need to redefine the battle space, since the traditional maneuvering war concept can be obsolete because the forces that conduct it operate in the human space and it represents the death zone of war in the future.

The essay concludes by pointing out that the Mexican Navy:

1. Carries out some activities related to Cyberspace Operations.
2. Within the current juridical framework, can carry out monitoring activities on its data, communications and infrastructure networks that support it to prevent threats from materializing, and
3. Can make use of the information that flows in the cyberspace, including the anonymous one.

Cap. Frag. CG. DEM. ECI. MSI. Carlos Lira Flores

Ingeniero en Ciencias Navales, egresado de la Heroica Escuela Naval Militar, cuenta con Diplomados en Computación y Electrónica por el Insittuto Nacional de Astrofísica Óptica y Electrónica; las especialidades en Comunicaciones e Informática y de Mando Naval, así como las maestrías en Seguridad de la Información y en Administración Naval por el CESNAV.

Se ha desempeñado como Oficial de cargo en diferentes buques; como jefe de la Subsección de Información de la Fuerza Naval del Pacífico; vocal de análisis de riesgos y planes de continuidad y de capacitación y concientización de la Comisión de Seguridad de la Información. ContrIbuyó a la creación y desarrollo de la Subdirección de Internet y redes sociales de la Dirección de Difusión y Atención a Medios de Comunicación de la Unidad de Comunicación Social donde también fue Director de Estrategia de Imagen Pública y Análisis de Opinión, y actualmente es Director de Difusión y Atención a Medios de Comunicación.

(Correo electrónico: carlos.flrlira@gmail.com)

Artículo recibido el 23de septiembre de 2016. Aprobado 05 de enero de 2017.

Los errores remanentes son responsabilidad de los autores.

Introducción

Historia y desarrollo tecnológico. Estado del Arte

Después de la guerra fría y la lucha armamentista, el entorno internacional advierte la aparición de amenazas a la seguridad nacional de todos los países, igual de silenciosas y quizá aún más letales: las Ciberamenazas; por ello, la tendencia en los ejércitos modernos es generar doctrina y procedimientos que les permitan realizar actividades y operaciones para mantener el control en el Ciberespacio, para lograrlo, se apoyan en estudios e investigaciones llevadas a la práctica mediante ejercicios y pruebas; los resultados han sido variados; sin embargo, ahora se habla de conceptos tales como: Ciberguerra (del inglés Cyberwarfare), Ciberseguridad (del inglés Cybersecurity), Ciberdefensa (del inglés Cyberdefense) y Ciberengaño (del inglés Cyber deception); los cuales se aplican empleando otros conceptos, ya ampliamente usados por los ejércitos modernos, como guerra de información, guerra centrada en redes y operaciones de información.

Por su parte, (Haeni, 1997) expone en su artículo *"information warfare an introduction"*, que la humanidad pasó por tres oleadas para llegar a madurar esos conceptos; la primera, la agraria que le permitió el desarrollo de la sociedad como se conoce actualmente, habilitando las comunicaciones que le ayudaron a generar productos y con ellos la economía; en esta ola, los soldados tenían una paga irregular y baja. La segunda fue la industrial, que cambio la forma en que se realizaban las guerras -cita por ejemplo, la forma en cómo se condujo la Segunda Guerra Mundial,- introduciendo además las armas de destrucción masiva. La tercera ocurrió a finales de los setentas y principios de los ochentas, ya que la tecnología e ideas empezaron a cambiar a la sociedad industrializada, a una sociedad basada en las comunicaciones e información; y con estos cambios, la doctrina militar también sufrió modificaciones para adaptarse a las nuevas realidades y amenazas.

Para ejemplificar mejor lo anterior (Kramer, Starr, & Wentz, 2013), editores del libro *"Cyberpower and National Security"*, crean una línea de tiempo de eventos clave en el Ciberespacio, que permite observar su evolución, la cual puede ser vista desde dos perspectivas: la militar y la económica. La creación del internet, la evolución de los nombres de dominio, la fundación de Google en 1998, el lanzamiento de Wikipedia en el 2001; estos momentos clave y otros, han venido ocasionando que la sociedad tenga un rol cada vez más importante en el Ciberespacio, y que aspectos de la vida personal, la sociedad, el gobierno y hasta el comercio sean ahora en gran parte trasladados a la dimensión virtual. Desde la perspectiva militar, la línea inicia en 1983 cuando

la red MILNET[1] se separa de ARPANET, ya para el 2010 el Ciberespacio es redefinido por el desarrollo de sistemas de información avanzados que apoyan al campo de batalla, siendo la base para aplicar los conceptos de operaciones en redes de computadora y guerra centrada en redes, operaciones en el Ciberespacio, etcétera.

Actualmente, las ciberamenazas afectan sectores como el financiero, médico o de medios y los pueden colapsar, tal y como lo demuestran los ataques en Estonia (2007)[2] ; que afectaron las industrias de esa nación, otra prueba de ello es el virus Stuxnet (2010)[3] y algunos gusanos informáticos que han venido transformando desde los años ochenta a la sociedad, ahora ya más integrada al Ciberespacio; su impacto, ha provocado que las tecnologías de información y sistemas que las soportan, -sistemas operativos, programas de cómputo, ruteadores y switches,- sufran los embates de los ataques.

Para tener una mejor convivencia en internet y el ciberespacio, se han realizado esfuerzos por parte de organizaciones e instituciones, lo que se hace patente al ver la creación de la Internet Engineering Task Force en 1992, o el Consorcio de la World Wide Web; para combatir las amenazas, se han realizado esfuerzos creando equipos de respuesta a incidentes en cómputo, el primero se creó en 1998.

Por su parte, las fuerzas armadas han identificado la importancia del Ciberespacio, especialmente los Estados Unidos de Norteamérica, que actualmente cuentan con los cibercomandos, –USCYBERCOM, US Army Cyber Command, US Strategic Command, US Fleet Cyber Command, entre otros- que realizan Operaciones en el Ciberespacio, basadas en los conceptos de guerra de la información, guerra centrada en redes y operaciones de información empleando tácticas y técnicas de enmascaramiento y distracción (engaño); y en sus misiones se contempla la defensa de sus infraestructuras críticas de información y comunicaciones ante ataques de otros países o de organizaciones criminales, la OTAN es otro referente.

La doctrina de la Armada de México ya cuenta con el concepto de operaciones de información, y las capacidades requeridas para implementarlas se encuentran distribuidas entre la Unidad de Inteligencia Naval (con un área de Ciberinteligencia), la Subsección de Protección a las Infraestructuras

1 Del inglés Military Network, red de comunicación militar de los Estados Unidos, creada en 1983 a partir de Arpanet que fue un proyecto común de varios establecimientos civiles y militares, que fue dividida posteriormente por motivos de seguridad.

2 Las computadoras que atacaron los sistemas de Estonia, el 25% eran de Estados Unidos, pero fueron controladas desde Rusia, -lo que indica que no hubo límites geográficos- y, los dueños de los equipos atacantes no tuvieron ni idea de que estaban siendo controladas de forma remota para propósitos dañinos, en esos momentos no se podía hacer un análisis sofisticado, siendo difícil rastrear el origen del ataque y casi imposible determinar el equipo controlador remoto. (Kramer, Starr, & Wentz, 2013).

3 En el 2010 miles de computadoras habían sido infectadas en India y Estados Unidos, pero el grueso de la infecciones se ubicaba en Irán, al hacer investigaciones sobre el virus Stuxnet, se descubrió que tenía cuatro vulnerabilidades del tipo "día cero", que usaba dos firmas digitales de certificados robados a dos compañías y que trabaja en todos los sistemas operativos Windows; su objetivo era acceder al kernel para insertar código que podía interactuar (vía drivers de dispositivos) con el hardware, el código malicioso buscaba un programa usado por Siemens para controlar sistemas SCADA –específicamente de las centrifugadoras nucleares- (si no lo encontraba el gusano se volvía inerte). (Kramer, Starr, & Wentz, 2013).

Críticas de Información (perteneciente a la Sección Segunda del Estado Mayor General), y la Unidad de Comunicación Social. Pero a juicio del suscrito, el nivel de madurez en su aplicación no es suficiente; no obstante, algunas actividades relativas a esas operaciones se materializan de forma aislada.

Sin embargo, la necesidad de proteger los flujos de información de las redes de datos, la interacción entre individuos e instituciones, las comunicaciones y las infraestructuras críticas de información y comunicaciones que las soportan, permanece y se acentúa aún más con el avance tecnológico. Por lo tanto, ahora es conveniente establecer estrategias, metodologías de planeamiento y procedimientos operativos que usen tácticas y coordinación de actividades, que ayuden a la Armada de México a proteger y defender sus infraestructuras críticas, mediante operaciones en el ciberespacio, de forma similar a cómo lo hacen otros ejércitos modernos.

¿Qué es el Ciberespacio?

En la actualidad existen varias definiciones de ciberespacio, la Real Academia Española de la Lengua lo define como: *"El ámbito virtual creado por medios informáticos"*; el Ministerio de Defensa Español lo expresa como: *"Dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de la información y telecomunicaciones interdependientes, que incluye el internet, los sistemas de información y controladores, y procesadores integrados, junto con sus usuarios y operadores";* el concepto también se encuentra en la Estrategia de Ciberseguridad del Reino Unido de 2011, mencionándolo de la siguiente forma: *"El Ciberespacio es un dominio interactivo conformado por redes digitales que son usadas para almacenar, modificar y comunicar información. Esto incluye el internet, pero también cualquier otro sistema de información que soporta nuestros negocios, infraestructura y servicios"*.

Organizaciones internacionales también han desarrollado el concepto, el que se presenta a continuación es de la Alianza de Seguridad Informática que al respecto dice *"El Ciberespacio es la vasta red de servidores, computadoras y demás aparatos, conectados entre sí, que nos permiten transmitir y recibir información de todo tipo"*.

En México, durante el presente sexenio se ha elaborado un glosario de términos unificados entre la Secretaría de Marina y la Secretaría de la Defensa Nacional, en él se define como: *"Ámbito intangible, de naturaleza global, soportado por las tecnologías de la información y comunicaciones (TIC´s), que es utilizado para la interacción entre individuos y entidades públicas y privadas"*.

Las definiciones anteriores permiten apreciar sus características:

1. El ciberespacio es ubicuo, dado que no hay fronteras físicas ni de tiempo.

2. En él existe también una alta interacción con las Tecnologías de Información y Comunicaciones, las cuales son su medio de acceso.
3. La interdependencia de redes, sistemas de información, sistemas de comunicación y espacio electromagnético, se basan en su infraestructura que no necesariamente es la propia.
4. El dominio físico se extiende al ámbito virtual, ya que la persona traslada su esencia a ese entorno, y una foto, sus comentarios, su información se constituyen como una prolongación de su propio ser.
5. El manejo de información es a todos los niveles personal, privado, industrial y gubernamental.

La siguiente información tiene la finalidad de mostrar que estas características permiten la interacción y flujo de información entre usuarios. El Internet por ser una de las infraestructuras más importantes que soportan el ciberespacio, crece constantemente.

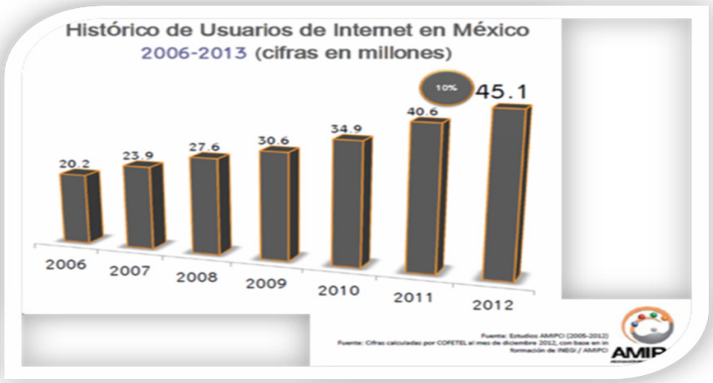

Fig. 1 Histórico de usuarios de internet

En la figura se aprecia el histórico de usuarios de Internet en México de 2006 al 2013; en tan solo seis años el número de usuarios se duplicó, iniciando con 20.2 millones de usuarios en 2006, al 2013 cuenta con 45.1 millones de usuarios.

Otro estudio, elaborado por la AMIPCI en el año 2013, muestra las principales actividades en línea; en ese contexto se observa que el envío y recepción de correos electrónicos, la búsqueda de información y la interacción social en Internet son las principales actividades.

Fig. 2 Principales actividades en línea

En la figura se observa que el mundo real ha o está migrando al digital, llevando a cabo actividades en el ciberespacio que van desde el entretenimiento, hasta actividades académicas, laborales y personales; en este tenor destacan las redes sociales, entes del Ciberespacio, creadoras de un poder moral que puede sobrepasar las capacidades de disuasión de un gobierno.

Pero también es conveniente describir el uso contrario que se le puede dar al Ciberespacio, lo cual se relaciona con el Cibercrimen, que se define *"como aquellas conductas contrarias a derecho que tienen como objetivo o medio de comisión a las Tecnologías de la Información"*, estas conductas son por citar algunas: Pornografía infantil, fraude, extorsión, espionaje, intervención de medios de comunicación, terrorismo. ¿Pero a quién afecta más el Cibercrimen? Datos del (Reporte, 2013) Norton muestran que:

1. El costo anual por Cibercrimen aumentó un 40% de un año a otro, en el 2012 fue de $2, 200 MDD contra $3,000 MDD del 2013.
2. El costo promedio por víctima fue de $4,381 pesos, cifra que prácticamente se duplicó ya que en el 2012 fue de $151 dólares y para el 2013 $337 dólares.
3. El porcentaje de personas que alguna vez han sido víctimas de ciberdelitos en México es del 71%, estando sólo debajo de China y Rusia que alcanza un 85%.

Ejemplos de este tipo de actos contrarios son los hechos ocurridos la mañana del 15 de septiembre del 2011, cuando las páginas Web de las Secretaría de la Defensa Nacional y de Seguridad Pública fueron atacadas

por un grupo de hackers denominado "Anonymous" catalogado por muchos gobiernos como terrorista; el mismo día, pero en la tarde el grupo y sus simpatizantes atacaron la página web de la presidencia, dado que fueron activadas las medidas de seguridad en poco tiempo se restableció el servicio.

La importancia de la seguridad en el Ciberespacio

Ya se ha definido el ciberespacio y su contexto en México, por lo que ahora se precisará el mecanismo que permite interactuar y fluir la información entre usuarios, de forma "normal"; esto es, la "seguridad". Pero ¿qué se entiende por seguridad?

Desde el ámbito de Seguridad de la Información, se define como:

> *"La sensación, estado o condición que permite operar los procesos, infraestructuras y personas dentro de los parámetros normales".*

Desde el ámbito de la Seguridad Nacional, se relaciona con:

> *"Las acciones destinadas a mantener la integridad, estabilidad y permanencia del Estado Mexicano,… que conlleven al mantenimiento del orden constitucional y fortalecimiento de las Instituciones democráticas del Gobierno;… la defensa legítima respecto a otros Estados,… todo ellos basado en el desarrollo económico, social y político del País y sus habitantes" (SEMAR S, 2013).*

Se entiende por ciberdefensa "al conjunto de acciones, recursos y mecanismos del Estado en materia de Seguridad Nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica Nacional" (SEMAR 2, DOF: 16/12/2013).

Por ciberseguridad se concibe "al 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".

Ahora se observa que todas las acciones emprendidas por el Estado para apoyar y soportar la interacción y flujo de información entre los usuarios se le denomina "ciberdefensa", y las mismas acciones, pero emprendidas por las "organizaciones" se le llama Ciberseguridad.

A continuación, se verá por qué son necesarias la ciberseguridad y la ciberdefensa y el uso de tácticas adecuadas para proteger la información e infraestructuras críticas. Frente a las oportunidades que trae el ciberespacio se vislumbran también amenazas y riesgos asociados con el cibercrimen, por ejemplo:

El acceso a la información, implica que fluya la información fuera del control de las autoridades del Estado (un ejemplo es el de España, donde se realizó un experimento a través de un recorrido por los principales sitios, en búsqueda de información acerca de drogas, se encontró entre los primeros enlaces mostrados por buscadores como Google, Bing y Yahoo!, que la mayoría de los sitios manifiestan que las drogas NO afectan la salud, que tienen propiedades curativas, que no causan adicciones ni daños físicos y que es la sociedad la que les ha impuesto la etiqueta de tabú.

Las redes sociales apoyan las posturas anteriores, y no se encontraron páginas de organismos gubernamentales que figuren en los primeros lugares (en el page ranking para refutar toda la información vertida). También se tiene el polo opuesto; es decir, el férreo control al flujo de información aplicado en China.

Otro ejemplo se observa en los ingresos por ciberdelitos que desde 2007, por primera vez fueron superiores a $100,000 millones de dólares y superaron las ganancias obtenidas por el tráfico ilegal de drogas; entre 2007 y 2009, el 60% de las compañías en Estados Unidos de Norteamérica, consideraron más costoso el ciberdelito que el delito físico. (ITU, 2009)

Escenarios que afectan la seguridad en el ciberespacio

En la coordinación de los ataques del 11 de septiembre de 2011 en New York, se utilizaron métodos de ocultamiento de información, para transmitirla a través de la red de datos más vigilada del mundo. (BLANCO, 2008).

Como ejemplos más actuales están el caso de Julián Assange, fundador de WikiLeaks, que recibió del soldado Bradley Manning "analista de inteligencia", 250 mil cables diplomáticos estadounidenses confidenciales. Esos documentos ponen en evidencia a la diplomacia estadounidense en una serie de temas, muchos de ellos sensibles.

Los sistemas SCADA acrónimo de (Software de Adquisición de Datos y Control de Supervisión), desarrollados por SIEMENS han sido blancos de ataques informáticos, evidencia de ellos es la aparición de Stuxnet, un gusano informático descubierto en junio de 2010, caracterizado por espiar y reprogramar sistemas industriales y con el potencial de afectar infraestructuras críticas como las centrales nucleares de generación de energía. Stuxnet tiene la capacidad de reprogramar Controladores Lógicos Programables (PLC, por sus siglas en inglés) y ocultar los cambios realizados; el primer blanco de este gusano, fueron los sistemas de las plantas nucleares en Irán y, por ciertas peculiaridades de su código, se ha especulado que los autores pudieran ser los Estados Unidos e Israel.

Escenarios como estos ya se habían vislumbrado internacionalmente, y por ello la Unión Internacional de Telecomunicaciones (UIT), lanzó en 2009 la Agenda sobre Ciberseguridad Global (GCA), la OCDE mediante un comité

planteó las directrices de la seguridad de los sistemas y redes de información, más tarde la Comunidad Europea sienta las bases del Convenio sobre Criminalidad.

Mejorar la ciberseguridad y proteger las infraestructuras de información que son críticas, es importante para lograr la seguridad y bienestar económico de un país, esto incluye, la adopción de medidas jurídicas adecuadas por el mal el uso de las TICs, específicamente las que tienen que ver con el sector comunicaciones, transportes, agua, electricidad y petróleo. La mejoría y cuidado, son responsabilidad de los sectores gubernamental, académico y privado.

En concreto en México, el establecimiento de la Estrategia Digital Nacional, el Plan Nacional de Desarrollo y los Planes Sectoriales de Marina y Defensa reconocen la importancia de la Ciberseguridad y se preparan en el área de ciberdefensa, y ejemplos están los siguientes:

1. La creación de equipos de respuesta a incidentes de seguridad en cómputo,
2. El fortalecimiento de la coordinación interinstitucional e internacional en el tema de la Ciberdefensa.
3. El impulso de la Estrategia Nacional de Seguridad de la Información.
4. El apoyo en la elaboración de proyectos de ley relacionados con el tema.

Importancia de operar en el ciberespacio

Como se explicó anteriormente, la seguridad es un estado deseado por una sociedad, en el que pueda desarrollarse y prosperar libre de amenazas. Pero ***¿Qué sucede cuando esa sociedad proyecta su concepto de Estado fuera del territorio, su espacio aéreo y marítimo hacia el ciberespacio?*** Un país en vías de desarrollo, que basa mucho de su crecimiento en las TIC´s, debe reconocer este espacio como estratégico y definir medidas de prevención, disuasión, protección y reacción, por lo que la ciberseguridad y ciberdefensa juegan un rol importante, y el ciberespacio plantea características únicas que se deben considerar:

1. *Es un espacio único en el que el atacante puede* disfrutar del anonimato, encontrarse en cualquier lugar y usar la infraestructura tecnológica que incluso puede no ser propia, por lo tanto las medidas de protección son diferentes a las emprendidas para proteger el territorio o el espacio marítimo.
2. Tiene una diversidad de factores, pues en ella convergen intereses personales, empresariales, nacionales e internacionales, por lo que se requiere una cuidadosa integración, coordinación y sincronización de acciones.
3. Es un área de conflicto asimétrico, donde las naciones están obligadas a utilizar la fuerza del Estado bajo principios éticos y leyes nacionales e internacionales, mientras el enemigo, se oculta en el anonimato y ubicuidad

del ciberespacio, pudiendo hacer uso de cualquier estrategia de ataque, sin necesidad de que exista una guerra declarada.

4. En este entorno prevalece el dominio de la información y el uso de la inteligencia, en el sentido de que puede pasar mucho tiempo obteniendo información de un gobierno, sin que éste se entere de ello. En este ambiente, es fácil escalar las ciberamenazas desde los ámbitos de ciberseguridad a los de ciberdefensa.

En este nuevo escenario se requiere el conocimiento y manejo de tácticas que se apliquen en conjunto con conceptos de "Operaciones de información", "Seguridad de la información", "Guerra Centrada en Redes" y, "Operaciones de Redes de Computadoras" las cuales apoyen a los futuros Ciberejércitos y Ciberpolicías.

¿Cuáles son las operaciones que se pueden realizar en el Ciberespacio?

Estas operaciones se definen en la (Publicación Conjunta JP 3-12 (R) "USA", 2015) como:

> ***"El empleo de capacidades en el Ciberespacio, cuyo propósito principal es lograr objetivos o efectos en o a través del mismo."***

Fig. 3. Premisas espaciales del espacio de batalla avanzado
Fuente: Elaboración propia con imágenes obtenidas de diferentes sitios de internet.

Para entender mejor la definición, es necesario conocer el concepto de éste tipo de operaciones, Robert J. Bunker, 2014, menciona que el pensamiento del ejército americano argumenta que el *espacio de batalla* está compuesto de

dimensiones electromagnéticas y físicas discretas pero separadas, y cada una de ellas debe ser controlada, si se desea que las operaciones amigas sean exitosas.

También expone que las fuerzas militares operan en la dimensión física, personificada por el mundo en donde los humanos y sus máquinas se mueven y pelean, sus límites pueden ser vistos en forma tridimensional, ya que están definidos por las limitaciones de las capacidades de los sentidos humanos; estas premisas se incluyen en el concepto del *espacio de batalla avanzado*, que puede ser visto como un volumen tridimensional dividido en dos por una cuarta barrera dimensional -un cubo-, es decir, los sentidos humanos; en él, se incluye al tiempo que representa el atributo de la quinta dimensión.

Igualmente define el concepto de *espacio humano*, que representa la dimensión física tradicional de los sentidos humanos en donde las fuerzas militares operan, y menciona que el *ciberespacio es dominante sobre este espacio;* que los medios para entrar en éste ámbito, se basan en la aplicación de *procesos y tecnologías furtivas*[4]; y que las contramedidas para las fuerzas que usan éstas tecnologías, se centran en lo que llaman *la fusión de datos que trascienden a lo espacial;* esto se debe a que las tecnologías furtivas, permiten a las fuerzas militares dejar el espacio humano y entrar al ciberespacio, y la fusión de datos niega la protección que brindan esas tecnologías. Además menciona que la *fusión de datos* es un concepto que se refiere a usar la información recolectada a través del espectro electromagnético, para localizar en espacio y tiempo a fuerzas militares enmascaradas usando la tecnología furtiva.

Más adelante en su libro se indica, que la base teórica antes descrita, fue aportada en un artículo del diario BlueFor del Colegio de Guerra[5], y que esa teoría ha evolucionado, ya que ahora en el tradicional cubo de batalla tridimensional, se fusiona el espacio humano con el tiempo, además, se superpone un quinto espacio de batalla dimensional, que existe más allá de la gama de los sentidos humanos, el ciberespacio.

La utilidad de ésta forma avanzada de espacio de batalla, es que permite superar las limitaciones físicas de los cuatro espacios dimensiónales, descritos anteriormente y que se deben superar para cumplir con los fines de guerra; esa ciberdimensión permite entonces, literalmente disolver las barreras de tiempo y espacio, permitiendo sacar ventaja en combate, pudiendo realizar operaciones defensivas y ofensivas en ese nuevo ámbito de batalla, empleando una filosofía donde operan fuerzas pequeñas bien entrenadas muy especializadas y tecnificadas, que usan nuevas tecnologías existentes en el mercado común, que les permiten enmascarar sus movimientos y sacar ventaja de sus adversarios.

Para lograr la superioridad en la quinta dimensión ciberespacio, se deben conocer sus limitaciones, mismas que a continuación se enuncian:

4 Del inglés Stealth, que en determinados contextos se le denomina también de disimulo o enmascaramiento.

5 Al pasar el tiempo, el término cuarta dimensión de guerra, se consideró un atributo de la quinta dimensión, y con el objetivo de evitar conflictos con escritos científicos, el tiempo fue reordenado como el cuarto atributo dimensional y el ciberespacio como el quinto atributo dimensional.

1. Distancia física y orientación,
2. El tiempo {t} que se tarda en recorrer la ruta entre dos objetos militares y
3. La dimensionalidad, es decir, la estructura física de un objeto.

Bunker et al. (2014) expresan que el viejo término de "campo de batalla", ha sido reemplazado en el discurso militar moderno por un término más exacto, *"espacio de batalla"*, incluso lo definen como el dominio o reino donde un adversario puede ser encontrado y enganchado; aseveran además que la cuarta dimensión; es decir, el tiempo es "continuo sin espacio" donde se producen eventos en una sucesión irreversible, desde el pasado hasta el presente y hacia el futuro; no obstante, el tiempo no es una dimensión distinta y separada, sino un componente crítico del espacio de batalla.

Mencionan que en tiempos recientes, estas cuatro dimensiones describieron satisfactoriamente el espacio de batalla; lo suficiente como para permitir planear, encontrar y enganchar adversarios en apoyo a fuerzas militares y de aplicación de la ley, sin importar que los adversarios sean criminales, terroristas o soldados enemigos. Sin embargo, conforme el tiempo pasa, este entendimiento del espacio de batalla se está volviendo inadecuado, ya que está adquiriendo una nueva dimensión; es decir, la quinta dimensión, el ciberespacio; y afirman que mientras la mayoría de la gente piensa en él, como un mundo de redes de computadoras en línea, es de hecho un ambiente mucho más rico y profundo, que se puede entender mejor como un nocional de "espacio de información"; en este reino, las personas interactúan con el espacio humano, a través del uso de gran variedad de dispositivos, como lo son computadoras, teléfonos celulares, sistemas GPS, tablas etcétera; donde cada momento, una persona interactúa con otra persona o máquina a través de uno de estos dispositivos, moviéndose en efecto a través del Ciberespacio.

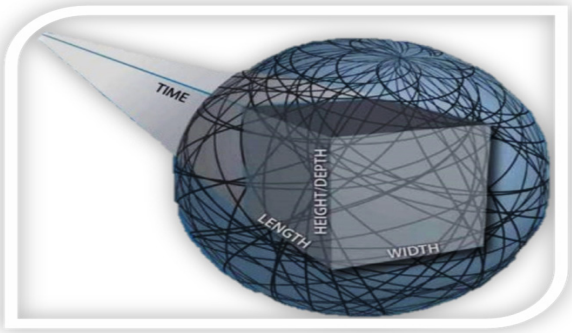

Fig. 4. Dimensiones tradicionales del campo batalla
Fuente: Extraída de la portada del libro de Bunker et al. (2014) y adaptada al presente trabajo.

Si fuera posible ver el espacio de batalla, podría verse como algo así, longitud, ancho y profundidad/altura, comprenden la dimensión del espacio, la cuarta dimensión es el tiempo, juntos espacio y tiempo comprenden el espacio humano, y la quinta dimensión es el ciberespacio; las cinco dimensiones interactúan entre sí, con los seres humanos siendo el "enlace o elemento" común. -Véase la figura cuatro -.

Los mismos autores Bunker et al. (2014) mencionan que el *espacio de batalla es igual al espacio humano más el ciberespacio;* y que en conjunto, las dimensiones de espacio y tiempo forman la porción del espacio de batalla ocupado por seres humanos, que como tal, se llama espacio humano; mencionan que hasta hace poco, el espacio humano, fue el dominio exclusivo donde los combatientes se encontraban y luchaban, sin embargo, cuando se añade la quinta dimensión "ciberespacio", los combatientes que permanecen en el espacio humano pueden ser atacados con impunidad desde éste ámbito ciberespacial y lo que separa al espacio humano de éste, es una barrera de sensaciones humanas, que dependiendo de las circunstancias dicha barrera puede tomar diferentes formas, las necesarias para que el adversario no pueda ser encontrado o enganchado con las capacidades de detección humana.

Es comprensible que el Ciberespacio ofrezca un refugio donde los adversarios más débiles pueden escapar usando la clandestinidad, convirtiéndose en indistinguibles, o incluso sólo oscurecidos para que los esfuerzos para identificarlos y engancharlos excedan el valor de búsqueda. Esa barrera es una frontera dinámica y competida entre fuerzas oponentes; pero lo que es necesario para tener éxito en el Ciberespacio, es tener herramientas para recolectar, privar o manipular información. La redefinición del espacio de batalla sugiere que nuestro concepto tradicional de guerra de maniobra puede ser obsoleto, ya que las fuerzas que la conducen operan en el espacio humano, y éste representa la zona de la muerte en las guerras futuras; también indica, que la guerra de la información es conducida dentro del ámbito electromagnético donde no hay fuerzas militares físicas.

Operaciones ofensivas y defensivas en el ciberespacio

Kevin (O´Shea, 2003) en su libro "Cyber attack investigative tools and technologies" define al ciberataque como:

> *"""Intento malicioso premeditado para interrumpir la confidencialidad, integridad o disponibilidad de información residente en computadoras o redes de computadoras."""*

Asimismo, Alexander Klimburg, y Jason Healey en su Manual Marco de Ciberseguridad Nacional les asignan una prelación conforme a su orden

de gravedad: espionaje, negación de servicio (DoS) y modificación de información; indican que esa segmentación, es útil para realizar estudios, ya que es muy aceptada en el ámbito militar; porque permite distinguir "tres niveles de severidad que provocan conforme a su impacto":

1. **Ruido de fondo de la seguridad de la información**
   También llamado "guerra de redes", que incluye la lógica maliciosa móvil, ataques de troyanos, intentos básicos de phishing, explotación de vulnerabilidades comunes. Algunos gobiernos lo han definido, como "explotación a nivel de redes de computadoras" (CNE), lo que implica cometer ciberdelitos convencionales, el ciberespionaje está limitado a este nivel, a menos que se modifiquen o destruyan datos.
2. **Ciberataque adjunto (Kinetic Combat)**
   Donde la intención es lograr un "efecto cinético" a través de un Ciberataque, para facilitar un ataque convencional en un objetivo secundario; un ejemplo de esto, es el uso de lógica maliciosa para desactivar una red de defensa aérea, dentro de un contexto de ataque aéreo, más amplio.
3. **Manipulación de datos maliciosa**
   Se refiere a manejos invisibles de sistemas a gran escala con el objetivo de degradarla con el tiempo, en el más grave de los casos, es posible que este tipo de ataques puedan elevarse a un "ataque armado".

Por su parte (Wong, Diciembre 2011) en su tesis Active Cyber Defense: Enhancing national cyber defense, define a los tipos de ciberataques como: Web defacement[6], Dos y DoS distribuido (DDoS), ataques con malware, ataques de día cero, y canales encubiertos sofisticados (http tunnel) mismos que coinciden con los descrito el manual marco antes citado.

Asimismo, a continuación se presenta la tabla uno que propone los tipos de operaciones ofensivas que se pueden realizar en el Ciberespacio.

6 Web defacement es un ataque que cambia el aspecto visual de una página o sitio web. DDoS es un ataque que mediante inundación de paquetes impide que un sitio web brinde un servicio, la diferencia con un DoS es que el primero es distribuido lo cual quiere decir que desde diferentes direcciones de internet se envían miles de paquetes por segundo a fin de negar el servicio.

Tabla 1
Tipos de Operaciones en el Ciberespacio ofensivas

Operaciones ofensivas	Nivel de severidad			Nivel de Impacto
	Guerra de redes o explotación a nivel de redes de computadora	Ciberata que con efecto cinético	Manipulación de datos maliciosa	
Espionaje	X			Alto
		X		Medio
			X	Bajo
DoS	X			Alto
		X		Medio
			X	Bajo
Modificación de Información	X			Alto
		X		Medio
			X	Bajo

Fuente: Elaboración propia

Si se permite en el presente trabajo considerar a los tipos de Ciberataques propuestos por Wong en su tesis cómo métodos de ciberataque, entonces la matriz anterior incluiría algunos métodos de ataque que se usan en las Operaciones en el Ciberespacio ofensivas pudiendo posicionarlos conforme a su nivel de impacto, dentro de éstas. Quedaría para una investigación posterior perfeccionar citada matriz, dado que es necesario evaluar el nivel de impacto. La Tabla dos presenta la matriz propuesta de Operaciones en el Ciberespacio ofensivas que incluye métodos de ataque.

En referencia a la ciberdefensa, Alexander Klimburg y Jason Healey, también expresan que a menudo se divide en cuatro tipos de acciones: **protección, detección, respuesta y recuperación.**

Para la protección consideran acciones tales como tener actualizados los antivirus, bien configurados los muros de fuego y en general realizar las acciones consideradas como "garantía de la información".

En el caso de la **detección**, explican, busca encontrar las pruebas de lo que está mal, en combinación con acciones pertinentes para cazar a los responsables de las acciones, dado que ya se sabe que algo anda mal, siendo necesario hacer uso de herramientas como los Sistemas de Detección de Intrusos (IDS), Sistemas de Prevención de Intrusos (IPS), así como la inspección profunda de paquetes de red (DPI).

Respecto a la **respuesta**, destacan que es toda acción necesaria para dar una respuesta efectiva, a fin de evitar que impacten de forma negativa en la organización, incluye en estas acciones a los equipos de respuesta a incidentes de seguridad en cómputo.

Tabla 2
Tipos de Operaciones en el Ciberespacio ofensivas con métodos de ataque incluidos

	Nivel de severidad			Métodos	
	Guerra de redes o explotación a nivel de redes de computadora	Ciberata que con efecto cinético	Manipulación de datos maliciosa	Ataques	Nivel de Impacto
Espionaje	X			Con malware Día cero	Alto
		X		Canales encubiertos	Medio
			X		Bajo
DoS	X			DDoS DoS	Alto
		X			Medio
			X		Bajo
Modificación de Información	X			Web defacement	Alto
		X			Medio
			X		Bajo

Fuente: Elaboración propia

Finalmente, de la *recuperación,* dicen que tiene que ver con garantizar que los usuarios finales sufran las interrupciones el menor tiempo posible, para lo cual hay planes de continuidad de las operaciones, de respuesta a incidentes, programas de respaldo y otras tecnologías que ayudan a que la recuperación sea en el menor tiempo posible y aun costo "bajo."

La tabla tres con una matriz muestra los tipos de operaciones defensivas que se pueden realizar en el ciberespacio, incluye algunos métodos de defensa que se usan en las Operaciones en el ciberespacio posicionados conforme al tipo de operación en el cual actúan.

Los autores del Manual Marco de la Ciberseguridad Nacional, Alexander Klimburg y Jason Healey, también mencionan que más recientemente, la naturaleza de la defensa ha estado cambianda; ya que mientras la defensa "pasiva" es todavía considerada una prioridad, voces muy influyentes han puesto su mirada en lo que denominan **"defensa activa"**, que usa algunos tipos de ataques para interrumpir los ataques entrantes, la cual se ha visto cristalizada mediante políticas en el Departamento de Defensa de los Estados Unidos de América.

Tabla 3
Tipos de Operaciones en el Ciberespacio defensivas

Operaciones Defensivas	Métodos o acciones de defensa
Protección	1. Actualización de antivirus 2. buena configuración de los muros de fuego 3. Parcheo de vulnerabilidades
Detección	1. Uso de IDS, IPS, DPI 2. Monitoreo de red 3. Auditorías
Respuesta	1. Uso de equipos de respuesta a incidentes 2. Monitoreo de red silencioso
Recuperación	1. Planes de continuidad 2. Programas de respaldo 3. Planes de recuperación

Fuente: Elaboración propia

Por su parte (Wong, diciembre 2011) en su tesis define los conceptos de Defensa pasiva, activa y ciberdefensa; al respecto explica que la defensa pasiva:

> *""Se refiere a las medidas tomadas para minimizar los efectos de daño causados por actos hostiles, sin la intención de tomar la iniciativa.""*

Para lo cual usa los siguientes activos de defensa: muros de fuego, IDS/IPS, parches y auditorias, y abarca desde la prevención y respuesta hasta la disuasión e investigación.

Con respecto a la defensa activa explica que:

> *""Se relaciona con el uso de acciones ofensivas limitadas y contra ataques[7], a fin de negar una posición o área disputada con el enemigo.""*

Tiene varias tipologías, tales como: recolección de información por medios no cooperativos, contra ataque, defensa preventiva, técnicas de engaño en el ciberespacio.

Respecto a los tipos de ciberdefensa activa, menciona que incluye a la ciberexplotación, contraataque, ataques anticipados y preventivos. Además que las ciberdefensas activas y pasivas no operan solas sino en conjunto, por lo que para emplear a ambas efectivamente, el defensor debe tener la capacidad de lanzar ciberataques, así como ciberexplotar dispositivos.

En la tabla cuatro se muestra en una matriz los tipos de defensas activas,

7 Tales como, ataques preventivos y anticipados del inglés preemptive.

pasivas y de ciberfedensa activa, en ella se observa que la defensa pasiva tiene los mismos elementos propuestos por Alexander Klimburg, y Jason Healey, pero Wong agrega la disuasión e investigación; asimismo profundiza más en el tema de la defensa activa proponiendo sus elementos.

Tabla 4
Tipos de Operaciones en el Ciberespacio de defensa pasiva, activa y de Ciberdefensa activa

Operaciones		Tipologías
De Defensa	Pasiva	Protección
		Detección
		Respuesta
		Recuperación
		Disuasión
		Investigación
	Activa	Acciones ofensivas limitadas
		Contra ataques preventivos
		Contra ataques anticipados
Ciber defensa activa	Explotación	N/A
	Contraataque	N/A
	Ataque preventivo	N/A
	Ataque anticipado	N/A

Fuente: Elaboración propia

Wong También explica que se debe considerar que las mejores vulnerabilidades son las de día cero; sin embargo, emplearlas requiere un programa de investigación interno o acceder a investigaciones para contar con información y herramientas para usarlas.

Finalmente, Wong escribe que para limitar el impacto de un ciberataque, es crucial detenerlo tan rápido como sea posible, lo cual significa que el defensor debe contar con herramientas para la defensa activa, incluyendo artefactos que explotan vulnerabilidades de día cero, junto con el conocimiento de cómo emplearlas.

Es posible apreciar que las Operaciones en el Ciberespacio utilizan las capacidades existentes en el mismo Ciberespacio, para lograr objetivos en o a través del mismo, para lo cual se pueden diseñar e implementar Operaciones defensivas y ofensivas, las primeras tienen que ver con la protección de las infraestructuras críticas de información y comunicaciones, para minimizar los efectos de daño causados por actos hostiles, sin la intención de tomar la iniciativa y las segundas con acciones llevadas a cabo para negar una posición o área disputada con el enemigo.

Asimismo, la Institución puede realizar este tipo de operaciones para

proteger sus infraestructuras críticas de información y comunicaciones, sus operaciones o para evitar afectaciones a la seguridad nacional, dado que la ley se lo permite; para tal efecto, se puede valer de los medios disponibles como las Operaciones en el Ciberespacio defensivas y de defensa pasiva.

¿Es legal efectuar operaciones en el Ciberespacio?

Para analizar el marco jurídico es necesario estructurar la búsqueda de información y dividir el cúmulo de información para enfocarse solamente en los temas jurídicos que se relacionan con el "engaño militar y su aplicación en las Operaciones en el Ciberespacio", esto se logra al usar la división empleada por (Alexander Klimburg, 2012) en su Manual Marco de Ciberseguridad Nacional, ya que mediante su división de tres dimensiones y cinco mandatos[8] permite enfocar el esfuerzo de búsqueda y su correspondiente análisis facilitando el trabajo, pudiéndose identificar las áreas que se relacionan con el trabajo: 1. Cibermilitar, 2. Inteligencia y contra-inteligencia y 3. Protección a las infraestructuras críticas de información y comunicaciones y administración de crisis. Lo anterior se debe a que la carrera de producción de armas virtuales que ocurre en el ciberespacio, se puede interpretar como algo similar al poder aéreo, marítimo o terrestre, que puede ser usada únicamente dentro de una misión militar claramente definida, abarcando cuatro tareas diferentes:

1. Habilitar la protección de sus redes militares,
2. Habilitar sus capacidades de Guerra Centrada en Redes,
3. Ciberguerra a nivel del campo de batalla (táctica),
4. Ciberguerra a niveles estratégicos.

Esas tareas tienen que ver con el ciberespacio y, por lo tanto, con las operaciones que en éste se realicen. Asimismo, el autor deja claro, que todavía es controversial la distinción del ciberespionaje, del cibercrimen y actividades cibermilitares, ya que los vectores de ataque y tecnología usada son similares, haciendo muy difícil identificar a un atacante y saber si es un estado o grupo criminal operando en su nombre o en el de un país.

Además, explica que el ciberespionaje, cuando se dirige a un estado, hace necesario desarrollar mecanismos de respuesta políticos capaces de tratar con la ambigüedad existente en el ciberespacio. Ocurre lo mismo con las actividades de contra-inteligencia, ya que a menudo dependen de los tipos de actividades de inteligencia que incluyen a la inteligencia humana, electrónica y de señales, análisis forense de datos etcétera, así como una vasta compartición de información entre socios internacionales; involucrando a

8 Tres dimensiones de actividad: gubernamental, internacional y nacional o social. Cinco mandatos de CiberseguridacNacional: 1. Cibermilitar, 2. Contra-Cibercrimen, 3. Inteligencia y contra-inteligencia, 4. Protección a Infraestructuras Críticas de Información y Comunicaciones y administración de crisis nacionales y 5. Ciberdiplomacia y gobernanza de Internet.

proveedores de servicios esenciales en un país; la mayoría están en el sector privado, por lo que es necesario extender algún tipo de apoyo por parte del gobierno para ayudar a proteger las infraestructuras críticas de información y comunicaciones y los servicios que brinda; por obvias razones también se implica a la Ciberseguridad Nacional.

Para reducir la ambigüedad existente en el ciberespacio fue necesario buscar más referentes, encontrando que el (Manual de Tallin, April, 2013) de Michael N. Schimtt, es importante ya que sienta las reglas generales de naturaleza legal, que rigen las relaciones entre estados, las infraestructuras críticas de información y comunicaciones y las Operaciones en el Ciberespacio, especificando que un *estado puede ejercer soberanía sobre infraestructuras críticas de información y comunicaciones y sus actividades dentro de su territorio,* lo que a su vez le da el derecho de controlarlas al igual que sus ciberactividades, provocando dos consecuencias, que:

1. La infraestructura crítica de información y comunicaciones está sujeta a un control legal y regulatorio.
2. La soberanía estatal la protege, sin importar si pertenece al Estado o una entidad privada o individuo.

Por lo que una Operación en el Ciberespacio, dirigida por un estado contra una infraestructura crítica de información y comunicaciones localizada en otro Estado, puede violar la soberanía del último Estado.

El grupo de expertos que elaboró el manual, no llegó a un consenso en el caso de que un *malware*[9] que ocasione un daño no físico como lo puede ser el monitoreo de actividades, constituya una violación a la soberanía de un estado.

Del manual también importa lo relacionado con los conflictos militares en el ciberespacio también llamados "ciberamados", las conductas hostiles, uso impropio de la perfidia y espionaje, y al respecto menciona que en el desarrollo de las hostilidades de una Operación en el Ciberespacio, está prohibido matar o lesionar a un adversario valiéndose de medios pérfidos, actos de invitación particular para ganar la confianza del adversario y la intención de traicionar esa confianza.

El manual también menciona que no hay obligación para marcar sitios web, direcciones IP u otras infraestructuras críticas de información y comunicaciones que tengan fines militares, a fin de distinguirlos de los bienes de carácter civil; sin embargo, puede ser pérfido hacer que dichos sitios web -u otras TIC's- parezcan tener un estado civil con el fin de engañar al enemigo, para matar o herir. Por lo tanto, no es pérfido llevar a cabo una Operación en el Ciberespacio que no revelen al creador de la operación.

9 Software destinado a dañar una computadora, dispositivo móvil, sistema informático o red informática, o tomar control parcial sobre su funcionamiento. Fuente: http://dictionary.reference.com/browse/malware. Obtenido el 01 de enero 2016. 22:40 hrs.

Cabe hacer mención que el manual no refleja la doctrina de la Organización del Tratado del Atlántico Norte ni de sus Estados miembro; sin embargo, fue elaborado por el Centro de Excelencia para la Ciberdefensa Cooperativa de esa organización militar, por lo que es referente mundial en la materia, asimismo, base de estudios pues todavía no existe otro documento similar que relacione al ciberespacio, derecho internacional aplicable a la ciberguerra, temas de soberanía, responsabilidad de Estados y otros temas igual de importantes.

Es importante citar que el Estado mexicano tiene firmados acuerdos y convenios con múltiples organizaciones internacionales como la UIT, ONU, OEA, etcétera, que requieren su cumplimiento, incluso tiene compromisos como el ASPAN que exige el intercambio de información en materia de seguridad; pero dado que la comunidad internacional en general, pide cooperación en temas de seguridad, no es posible voltear la cara o dejar de realizar acciones para proteger los flujos de información e infraestructuras críticas de información y comunicaciones, por lo que documentos como el Manual de Tallin, o Convenio de Budapest son referentes obligados que el Estado mexicano debe cumplir como actor con responsabilidad global [10].

En la Tesis "Evaluación del uso de programas de cómputo de tipo malicioso, con el fin de obtener información de valor específico para la producción de inteligencia naval" (Carlos Lira, 2008), se hace un análisis del marco jurídico mexicano, y como resultado menciona que la Ley de Seguridad Nacional faculta a las instituciones relacionadas con la Seguridad Nacional para monitorear sus redes de datos, de comunicaciones e infraestructuras críticas de información y comunicaciones que las soportan, para evitar se materialicen ataques, para lo cual les permite realizar actividades de inteligencia y contrainteligencia apoyándose de métodos, técnicas, sistemas de información y programas de cómputo para obtener información, evitando en todo momento lesionar las garantías individuales y los derechos humanos, tomando en consideración que las actividades de inteligencia que se lleven a cabo bajo esta óptica, deberán estar encaminadas a combatir las amenazas descritas en la Agenda Nacional de Riesgos. Por lo que está claro que pueden realizar Operaciones en el Ciberespacio a fin de proteger sus infraestructuras críticas de información y comunicaciones, sus operaciones o para evitar afectaciones a la Seguridad Nacional, valiéndose para ello de los medios disponibles los cuales incluyen las tácticas enmascaramiento y distracción aplicables a las Operaciones en el Ciberespacio.

10 Plan Nacional de Desarrollo 2013-2018 p.18 "Proyección internacional para un México con Responsabilidad Global." p.22 Cinco metas nacionales "Un México con Responsabilidad Global" la actuación del Estado Mexicano debe ser con responsabilidad atendiendo nuestra prioridades enmarcadas en las otras cuatro metas definiendo así la política exterior, fortaleciendo nuestra voz y presencia en la comunidad internacional.

Conclusiones

1. Se puede afirmar que la Armada de México ejecuta algunas actividades relacionadas con las Operaciones en el Ciberespacio, por lo que es factible que las realice de manera formal.

2. El marco jurídico permite aseverar que la institución naval en mención puede realizar actividades de monitoreo de sus redes de datos, comunicaciones e infraestructura que las soporta, a fin de evitar que se materialicen amenazas; además puede usar la información que fluye en el ciberespacio incluida la anónima, tomando en consideración que las actividades que realice, se lleven a cabo bajo la óptica, de estar encaminadas a combatir las amenazas descritas en la Agenda Nacional de Riesgos.

3. La Institución tiene necesidad de proteger los flujos de información en las redes de datos, las comunicaciones e infraestructura que las soporta, y está en continua exploración y búsqueda de métodos, procedimientos, técnicas y tácticas que le auxilien a realizar de forma efectiva citada labor.

4. El Manual de Tallin permite sentar las reglas que rigen las relaciones entre Estados, sus infraestructuras críticas de información y comunicaciones, y las Operaciones en el Ciberespacio, especificando cómo ejerce la soberanía, qué tanta jurisdicción y control tiene sobre las infraestructuras críticas de información y comunicaciones, y cuál es su responsabilidad al efectuar una operación de éste tipo.

5. El Manual de Tallin estudia las conductas hostiles en las Operaciones en el Ciberespacio y perfidia expresando al respecto que un Estado no tiene obligación de marcar sus infraestructuras críticas de información y comunicaciones como civiles o militares, por lo que no es desleal llevar a cabo una Operación en el Ciberespacio que no revele al creador de la misma.

Fuentes consultadas

1. Alexander Klimburg. (2012). National Cyber Security Framework Manual. En N. C. Excellence, National Cyber Security Framework Manual. Tallin, Estonia: Nato CCD COE Publication.

2. BLANCO, J. V. (30 de Abril de 2008). El funambulista, las torres y el bodrio gore. Recuperado el 14 de septiembre de 2014, de www.elmundo.es: http://www.elmundo.es/elmundo/2008/04/30/cultura/1209540817.html

3. campodocs.com. (2015). Mando y Control términos. Recuperado el 08 de febrero de 2015, de www.campodocs.com: http://campodocs.com/articulos-educativos/article_18491.html

4. DAM México, A. d. (2013). DAM 1.0 Mando y Control. En A. d. México, DAM 1.0Mando y Control. México: Armada de México.

5. DAM México, A. d. (2013). DAM 1.2 Inteligencia Naval. En A. d. México, DAM 1.2 Inteligencia Naval. México: Armada de México.

6. Denning, D. E. (1999). Information Warefare & Security. En D. E. Denning, Information Warefare & Security. Addison Wesley.

7. Haeni, R. E. (january de 1997). Information warefare, an introduction. Recuperado el 16 de septiembre de 2014, de Trinity University: http://www.trinity.edu/rjensen/infowar.pdf

8. ITU. (2009). Guía para los países en desarrollo. Recuperado el 14 de Septiembre de 2014, de Unión Internacional de Telecomunicaciones: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

9. Kramer, F. D., Starr, S. H., & Wentz, L. K. (2013). Cyberpower and National Security. Washington D.C.: National Defense University Press and Potomac Books, Inc.

10. Manual de Tallin, T. N. (April, 2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. En T. N. Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare (pág. 302). Estonia: Cambridge University Press; Edición: Reprint (7 de marzo de 2013).

11. O´Shea, K. (2003). En K. O´Shea, Cyber attack investigative tools and technologies. Hanover, NH: Dartmouth College.

12. Pangea. (2015). Conceptos de Guerra. Recuperado el 08 de febrero de 2015, de ruben.pangea.org: http://ruben.pangea.org/psiclib/cptos_guerra.pdf

13. Programa Sectorial de Marina, 2. (DOF: 16/12/2013). Programa Sectorial de Marina. México D.F.: Secretaría de Marina.

14. Publicación Conjunta JP 3-12 (R) "USA", D. (2015). Cyberspace Operations. En D. (. Joint Chiefs of Staff, Joint Publication 3-12(R) Cyberspace Operations (págs. I-1). Washington D.C.: DoD.

15. Reporte, N. 2. (2013). Reporte Norton 2013 en México. México: Symantec Norton.

16. Robert J. Bunker, C." (2014). Sección 1: Conceptos de espacio de batalla avanzado y cibermaniobra: Implicaciones para la fuerza XXI. En C. "Robert J. Bunker, Operaciones de la quinta dimensión: Espacio-Tiempo- Ciber dimensionalidad en conflictos y guerra. Ed Universe LLC.

17. SEMAR, 2. (DOF: 16/12/2013). Programa Sectorial de Marina. México D.F.: Secretaría de Marina.

18. SEMAR, S. (2013). Glosario de términos unificados entre la Secretaría de Marina y la Secretaría de la Defensa Nacional. México D.F.: CESNAV, CODENA.

19. Tte. Nav. CG. ECI. MSI. Carlos Lira Flores. (2008). Aspectos legales y bases técnicas para

explotar sistemas. En T. N. Flores, Evaluación del uso de programas de cómputo de tipo malicioso, con el fin de obtener información de valor específico para la producción de inteligencia naval (págs. 8-11). México D.F.: CESNAV.

20. Tutor. (2014). Documentos generados por la Sección Segunda. En Tutor, Documentos generados por la Sección Segunda. México: DEM.

21. Tutor. (diciembre de 2014). Organización y Funciones de Estado Mayor. Recuperado el 08 de febrero de 2015, de Maestría en Administración Naval 2014: http://201.116.62.25/man2014/pluginfile.php/663/mod_resource/content/7/tema7/intro.html

22. Wong, T. P. (diciembre 2011). Thesis. Active Cyber Defense: Enhancing national cyber defense. Naval Posgraduate School.