**INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

# "CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE UN *CIBEREJÉRCITO* EN MÉXICO"

SOLUCIÓN ESTRATÉGICA
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

**Presenta:**

Héctor Maximiliano Segura Cantú

**Asesor:**

Mtra. Evelyn Téllez Carvajal

**Ciudad de México, diciembre de 2019**

## Autorización de Impresión

**AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA**

**MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN**

Ciudad de México, 17 de febrero de 2020
*INFOTEC-DAIC-GCH-SE-0142/2020.*

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

***CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE UN CIBEREJÉRCITO EN MÉXICO***

Desarrollado por el alumno **Héctor Maximiliano Segura Cantú** y bajo la asesoría de la **Mtra. Evelyn Téllez Carvajal**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

**Mtra. Julieta Alcibar Hermosillo**
Coordinadora de Biblioteca

**Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.**

*C.p.p Servicios Escolares*

## Agradecimientos

Agradezco profundamente a mi familia, mi esposa, mis padres, especialmente a mis hijas Jimena y María por el aguante de tenerme todos los fines de semana durante dos años fuera de casa, quienes me dieron la oportunidad de estudiar esta Maestría que cambió de manera tajante mi vida profesional.

También, quiero agradecer a la Institución INFOTEC por pensar no solamente en los ingenieros especialistas en las TIC, sino también en nosotros los abogados.

De igual forma quiero agradecer a mi asesora de tesis la Maestra Evelyn Téllez Carvajal, quien con mucha paciencia me guío para la conclusión de este estudio.

# Tabla de contenido

# Índice de figuras

## Índice de cuadros

# Introducción

Año con año la ciberdelincuencia va en aumento.[1] Ya no solo se realizan delitos con la finalidad de afectar económicamente haciendo uso de los tipos más comunes como son el robo de identidad, el fraude cibernético, el *phishing*, entre otros, sino que los delitos informáticos cada vez son más sofisticados.[2]

Dese el año 2007 se han suscitado ataques que han utilizado a la red como medio comisivo para perpetrar ilícitos, sin embargo, la red también ha sido objetivo de ataques que se presumen han sido orquestados por naciones independientes tales como Estados Unidos, Rusia, China e Israel.[3]

También se han realizado ataques perpetrados por particulares tal como sucedió con dos hackers rusos, Alexsey Belan y Karim Baratov, quienes en 2014 robaron datos de 500 millones de usuarios de la empresa Yahoo para espiar a

---

[1] McKinsey & Company, Perspectiva de ciberseguridad en México, México, Consejo Mexicano de Asuntos Internacionales, junio, 2018, pp. 16 y 17.
"En el año 2017, 33 millones de mexicanos (50% más que en 2016) fueron víctimas del cibercrimen – uno de cada cuatro habitantes del país".

[2] Piña Libien, Hiram Raúl, "Los delitos informáticos previstos y sancionados en el ordenamiento jurídico mexicano", Segundo Congreso Nacional, "Cultura de la Legalidad e Informática Jurídica, México, Secretaría de Gobernación, 2012, pp. 3-5. "…destacan: *hacking*, *cracking*, *phishing*, *evil twins*, *pharming* y *spamming*, robo de identidad, *cyberterrorismo*, propagación de *Malware* a través de redes de datos, el empleo de tecnologías *Pop-UP Ads* y *Adware*, la instalación de *sniffers*, *spyware*, o programas espía en las computadoras personales para conocer los hábitos y actividades de familiares o empleados; así como la vigilancia internacional de las comunicaciones electrónicas a través de programas gubernamentales como *ECHELON* o los de control fronterizo como el *US-VISIT*, son tan solo algunas de las tantas expresiones de tan variada fenomenología que han hecho de la seguridad jurídica de las personas y de las transacciones comerciales electrónicas, dependan de las medidas de seguridad de los sistemas informáticos de información y comunicación". Algunas citas fueron omitidas.

[3] Calderín, Juanafer F. y Jiménez, María, "Estados Unidos, Rusia o China presentan ventajas para el cibercrimen", *Observatorio Internacional de Estudios sobre Terrorismo*, 7 de julio de 2016, disponible en https://observatorioterrorismo.com/entrevistas/eeuu-rusia-y-china-son-paraisos-del-ciberterrorismo/, consultado el 21 de mayo de 2019.

periodistas rusos, empleados de servicios financieros y funcionarios del gobierno estadounidense y del propio Ejecutivo ruso.[4]

Es precisamente por el aumento de las vulneraciones y ataques en el *ciberespacio* que países como los Estados Unidos hacen inversiones cada vez mayores en la materia de seguridad informática.

Estados como Rusia, Inglaterra, España y otros Estados[5] han invertido en ciberseguridad en el ámbito público pero también los agentes privados invierten cada vez más en seguridad informática pues han tomado conciencia de su relevancia.

En este aspecto los Estados responden a las necesidades de seguridad informática y surge la propuesta e inclusive puesta en marcha de los llamados *ciberejércitos*, que tienen como misión salvaguardar la soberanía de un país por medio de la protección de los sistemas de información y bases de datos que pudieran contener información sensible de una nación, así como del manejo de infraestructura crítica que se vería comprometida en caso de ataques informáticos, lo cual podría causar caos de manera casi inmediata debido a la dependencia que se tiene en este mundo hiperconectado.

Es pertinente hacer la distinción de que en estos casos ya no estamos frente a un tema de ciberseguridad en general sino específicamente a un tema de defensa de la soberanía de un Estado por lo que hay que separar con cautela el tema militar

---

[4] EFE, "EU acusa a dos espías rusos y dos 'hackers' de robar datos de Yahoo.", *El Universal*, 15 de marzo de 2017, disponible en *http://www.eluniversal.com.mx/articulo/techbit/2017/03/15/eu-acusa-dos-espias-rusos-y-dos-hackers-de-robar-datos-de-yahoo*, consultado el seis de diciembre de 2018.

[5] "Israel, Finlandia y Suecia son vistos como los más avanzados en "ciberdefensa", de acuerdo a un nuevo informa de seguridad, El estudio sobre ciber preparación impulsado por McAfee, empresa líder en antivirus y seguridad informática consideró que China, Brasil y México están entre los menos capaces de defenderse contra potenciales ataques".
Lee, Dave, "Los países mejor preparados para resistir un ciber ataque… y los peores", *BBC News Mundo*, 31 de enero de 2012, disponible en *https://www.bbc.com/mundo/noticias/2012/01/120131_ciberataques_paises_mejor_peor_preparados_adz*, consultado el 21 de mayo de 2019.

de otros temas en los que se ven inmiscuídos otros agentes del orden como en el caso mexicano pudo ser la Policía Federal y sus distintas divisiones que como órgano desconcentrado de la Secretaría de Gobernación contó con un marco jurídico distinto al que tienen las fuerzas armadas a cargo de la Secretaría de la Defensa Nacional que es hacia donde se orienta la presente investigación dejando de lado otros temas de ciberseguridad y concentrándose únicamente en los ciberejércitos que ya cuentan con experiencia en la materia y en sus actuaciones en la actualidad para hacer frente a lo que se ha denominado como "ciberguerra" a fin de que los incipientes intentos en México puedan tomar en cuenta la experiencia compartida por dichos ciberejércitos.

Antes de referir a los *ciberejércitos* es necesario recordar que los ejércitos son la institución Estatal dentro de la legalidad encargados de proteger la soberanía; cuentan con personal especializado en combate en diversos escenarios, así como armamento especial para llevar a cabo enfrentamientos tanto en el espacio aéreo, marítimo y terrestre.

Los ejércitos tienen la necesidad de actualizar sus sistemas de defensa, ataque y **resilencia**, no solo en los ámbitos antes mencionados sino también en este nuevo lugar de conflicto que es el *ciberespacio*, motivo por el cual se desarrolla el presente estudio, a efecto de proponer la creación de un *ciberejército* con los elementos y las tecnologías necesarias para hacer frente a estos nuevos retos.

No puede pasar desapercibido que en el cierre del año 2016 así como en el transcurso del año 2017, en el ámbito internacional se supo de diversos casos relacionados al tema de *ciberespionaje*, es decir intervenciones no autorizadas cometidas por parte del gobierno de un Estado a otro con fines de obtener información secreta, sensible o clasificada, que pudiera poner en riesgo a toda una nación de ser revelada. Algunos de estos casos incluso fueron ventilados por los medios de comunicación, como el famoso caso de Wikileaks revelado por el ya célebre Edward Snowden.[6]

[6] EFE, "Cronología del 'caso Snowden', el joven que reveló el espionaje masivo de Estados Unidos", 20 minutos, 7 de julio de 2013, disponible en

Hoy, derivado de los ataques en el *ciberespacio* como son los espionaje, las tensiones se generan entre los distintos Estados y en particular entre los Estados Unidos y Rusia, lo cual nos hace recordar la época de la Guerra Fría en la que los Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas (URSS) con sus tácticas de espionaje ponían a todo el planeta en tensión.[7]

Hoy son precisamente estos dos actores internacionales quienes nuevamente nos llevan a reflexionar sobre los temas de espionaje pero en el contexto cibernético. Lo cual nos hace cuestionar si estamos ante el origen silencioso de la primera *ciberguerra*.

Como alumno del INFOTEC, he detectado la relevancia de la tendencia de los Estados en la creación de ciberejércitos y lo poco que se ha escrito en Latinoamérica al respecto, por ello se elaborará una investigación en materia de *ciberdefensa* y *ciberseguidad* aplicada, ya que se elaborarán los lineamientos que se deben seguir para la implementación de un *ciberejército* en el Estado Mexicano.

Nuestra hipótesis se basa en que el ejército mexicano no se encuentra preparado para enfrentar una ciberguerra ya que no se cuenta con los medios suficientes, ni tecnológicos o humanos para ello. La propuesta de esta investigación es precisamente dotar de los lineamientos que deben seguirse para la conformación del mismo.

El presente estudio expondrá los lineamientos sobre la implementación de un *Ciberejército* en el Estado Mexicano, brindando la información necesaria desde el punto de vista jurídico sobre los elementos necesarios para una debida funcionalidad y operación del mismo. Se expondrán cuáles son los métodos de

---

*https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/,* última fecha de consulta el 23 de mayo de 2019.

[7] "Las últimas revelaciones de Wikileaks sobre los métodos de la CIA constatan que las agencias de espionaje han adaptado sus métodos y herramientas al nuevo ecosistema digital. La vigilancia masiva a través de los móviles, los ordenadores e incluso los televisores se realiza a escala mundial".
García Campos, Juan Manuel, "El ciberejército de Putin", *Magazine digital*, disponible en *http://www.magazinedigital.com/historias/reportajes/ciberejercito-putin* fecha de consulta el 21 de mayo de 2019.

creación de los *ciberejércitos*, los sistemas de prevención, sistemas de ataques y sistemas de resiliencia, además de los métodos utilizados para la *ciberinteligencia* y el *ciberespionaje* dentro de los parámetros para ejercer estas actividades.

Veremos también los lineamientos jurídicos que justifican el uso de la tecnología aplicada en la materia, además de los estatutos internacionales que regulan y promueven la creación u la actividad de un *ciberejército*.

En el presente estudio se utilizará una metodología de investigación documental para escribir con base a la literatura internacional en el tema, se elaborarán cuadros comparativos sobre los documentos expedidos por organizaciones civiles y militares, además de hacer un análisis de información relacionada con la guerra y ciberguerra, y las herramientas relacionadas con la informática jurídica para la implementación de *ciberejércitos*.

# Capítulo 1

# Conceptos generales para comprender la ciberguerra y el concepto ciberejército

# Capítulo 1: Conceptos generales para comprender la ciberguerra y el concepto de *ciberejército*

El presente capítulo tiene por objetivo acercar al lector a los conceptos generales que se utilizan a lo largo del presente trabajo de investigación para profundizar más adelante sobre los mismos.

El análisis doctrinal será fundamental para comprender el concepto de ejército que, si bien ya habían sido tradicionalmente definidos, estos conceptos se han transformado en la actualidad a partir de la incorporación del uso de herramientas tecnológicas que permiten hoy hablar de la necesidad de crear *ciberejércitos* que protejan la soberanía nacional de los Estados dentro del llamado *ciberespacio*.

Antes de profundizar en el concepto base de la investigación será necesario también ahondar en conceptos propios que se circunscriben a los conflictos armados, tal es el caso de la guerra en sí misma así como también explicar la relevancia del armamento que se utiliza durante estas actividades, ya que mucho del tema en torno a los *ciberejércitos* tiene relación directa precisamente con las denominadas *ciberarmas*, en un conflicto denominado *ciberguerra* que pudiera ser considerado como un espacio independiente de conflicto entre naciones.

Una vez aclarando el uso de estos conceptos básicos en el estudio, se procederá a abordar el tema del uso de los denominados *ciberejércitos* como parte de la *ciberseguridad* y la *ciberdefensa*, haciendo hincapié de que algunos Estados soberanos ya tienen implementados *ciberejércitos*, pues forman parte de las estrategias nacionales para hacer frente a posibles ataques a sus sistemas informáticos, en esta parte centramos la atención en el marco normativo que rige el *ciberespacio* ya que por su propia naturaleza no pertenece a ningún Estado ni tiene fronteras delimitadas.

Finalmente, en este capítulo se estudian las armas que son implementadas por los Estados en sus estrategias defensivas, a fin de explicar si él es correcto el uso del concepto de ciberguerra, ciberejército y armas cibernéticas (*cyberweapons*)

pues con ello se permite el estudio de quiénes son o pueden ser los combatientes en el *ciberespacio*.

Todos estos conceptos analizados son herramientas que serán de utilidad para poder en el segundo capítulo comparar cuáles son los elementos comunes a todos los ciberejercitos que están en funciones actualmente. También nos permitirá tomar pautas para diseñar los lineamientos para la creación y puesta en marcha de un ciberejército en el Estado mexicano.

Sin embargo, no debe olvidarse que los lineamientos que plantearemos son estándares generalizados obtenidos del estudio de ciberejércitos de otros Estados y que es necesario tomar en cuenta el contexto de las fuerzas armadas nacionales, es decir que los lineamientos no son elementos que deban aplicarse a rajatabla en el caso mexicano sino sirvan para impulsar el desarrollo de las capacidades del personal, instrumentos y tecnología con la que contamos en el país.

Ahora bien, en el tema análisis de los enfrentamientos bélicos podemos observar que estos surgen desde tiempos remotos incluso antes del nacimiento de los Estados – nación. Sin embargo, nosotros centraremos precisamente el arranque de este estudio desde la concepción de la soberanía del Estado por ser actualmente el único actor que el derecho internacional contempla como facultado para llevar a cabo una guerra contra otro Estado igualmente soberano. Por ello a continuación se explica la soberanía en el contexto de la defensa nacional de los Estados.

### 1.1. Soberanía de los Estados y defensa nacional

La soberanía concebida como el poder que no está sujeto a otro poder[8] o el poder absoluto sobre un territorio determinado por unas fronteras fijas,[9] se ve cuestionado a la luz de la globalización debido a la "desterritorialización, occidentaliozación, modernización, liberalización o unversalización [que] ha modificado los patrones de referencia entre los Estados, las sociedades y las instituciones del sistema

[8] Seara Vázquez, Modesto, *Derecho internacional público*, 15a. ed., México, Porrúa, 1994, p. 91
[9] Perieira Menaut, Antonio – Carlos, "Después de la soberanía", *Revista de derecho político*, núm. 50, 2001, p. 64.

internacional. La soberanía como concepto de rígida defensa contra el otro se ha flexibilizado relativamente,…".[10]

> La soberanía nacional, fundada primordialmente para efectuar la defensa del territorio ante cualquier amenaza de intervención y para la legitimación de una forma de gobernar, adquirió dos dimensiones: la externa, representaba a un Estado entre los otros, y la interna, que se sujetó al reconocimiento de la primera para ser ejercida...[11]

Por medio del poder soberano los Estados deciden las políticas que habrán de implementar para protegerse de peligros provenientes del exterior pues la soberanía fue "una construcción cultural y política fabricada para fortalecer el poder de los reyes absolutistas en la Europa de las guerras de religión [y] estaba ligada a un tipo de armamento, una cultura, unos intereses políticos y unas circunstancias sociales y económicas".[12]

La soberanía se encuentra íntimamente relacionada a la defensa, es decir al mecanismo para proteger su integridad territorial por un lado y a la prevención de cualquier situación que pudiera provenir del exterior en detrimento del orden público del Estado. Es así que los Estados tradicionalmente han contado con una institución encargada de la protección de su seguridad nacional, nos referimos a las fuerzas armadas.

Son a las fuerzas armadas precisamente a quienes se encarga la tarea de diseñar estrategias para la defensa e integridad del Estado. Luis Felieu Ortega, define la defensa como "aquella que se basa fundamentalmente en la disuasión, es decir, en la capacidad de respuesta de forma que el potencial atacante renuncia a materializar su amenaza, por los perjuicios que a cambio pudiera recibir".[13] Por esta

---

[10] Valdés Ugalde, José Luis, "Globalización vs. Soberanía: gobernanza, guerra o progreso y orden mundial, *Norteamérica*, año 2010, núm. 2, julio – diciembre de 2015, p. 8.
[11] *Ibidem*, p. 9.
[12] Perieira Menaut, Antonio – Carlos, *op. cit*., nota 9, p. 66.
[13] Feliu Ortega, Luis, "La ciberseguridad y la ciberdefensa", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN*,* Consejo Superior de Estudios de la Defensa Nacional, núm. 126, España, Ministerio de Defensa, 2012, p. 41.

razón los Estados invierten gran parte de sus recursos para el reclutamiento, adiestramiento y armamento de sus fuerzas armadas.

La lista de los países con mayores gastos en armamento es encabezada por Bahréin, seguido por Rusia, Líbano, Israel, Jordania, Argelia, Kuwait, Congo Arabia Saudita y Omán.[14]

De acuerdo a datos del Banco Mundial hay Estados que destinan un mayor porcentaje de su Producto Interno Bruto (PIB) en gasto militar, Estados Unidos por ejemplo que es una potencia militar invierte el 3,1% de su PIB en este rubro, sin embargo Eritrea destina el 20,9%, Arabia Saudita el 10,3%, Rusia el 4,3%, en comparación con México que destina el 0,5%.[15] Estos datos son relevantes porque en el tema de la implementación de los *ciberejércitos* el gasto que se destina para su funcionamiento es fundamental para su desempeño que se traduce en la disminución de riesgos y capacidad de reacción tras ataques a sistemas informáticos que pudieran comprometer la seguridad nacional.

Por su parte la seguridad nacional, fue un concepto que se comenzó a utilizar durante la Guerra Fría para hacer referencia a la defensa militar y la seguridad interna.[16]

Hoy entenderemos a la "Seguridad Nacional como el estado deseado por una sociedad en el que pueda desarrollarse y prosperar libre de amenazas".[17] Así, podemos concluir que la defensa es la adopción práctica de medidas conducentes

---

[14] BBC, Mundo, Cuáles son los 10 países del mundo que gastan una mayor parte de su riqueza en armamento, 3 de mayo de 2018, disponible en *https://www.bbc.com/mundo/noticias-internacional-43984570*, última fecha de consulta el 24 de mayo de 2019.

[15] Banco Mundial, "Gasto Militar (% del PIB), Instituto Internacional de Investigación para la Paz de Estocolmo (SPIRI), Yearbook: Armaments, Disarmament and International Security, disponible en *https://datos.bancomundial.org/indicador/ms.mil.xpnd.gd.zs*, última fecha de consulta el 24 de mayo de 2019.

[16] Leal Buitrago, Francisco, "La doctrina de seguridad nacional: materialización de la Guerra Fría en América del Sur*", Revista de Estudios Sociales*, núm. 15, junio de 2003, p. 74.

[17] Doctrina del Ejército de Tierra (español) D01-001, año 2003.

a mantener la seguridad deseada y que los Estados atendiendo a la necesidad de garantizar su integridad territorial y prevenir las amenazas provenientes del exterior, invierten en personal especializado y capacitado para diseñar políticas y estrategias que mantengan el orden público y puedan reaccionar ante posibles ataques y conflictos entre Estados y actualmente también se deben considerar ataques de particulares.

### 1.2. Conflictos entre Estados y medios pacíficos de solución de controversias

En derecho internacional existe el principio de no intervención que se refiere a la no injerencia en los asuntos internos de otro Estado para el mantenimiento de la paz y seguridad internacionales. Es precisamente en la violación a este principio que se pueden derivar asuntos controvertidos entre Estados.

La Asamblea General de las Naciones Unidas en su resolución 2.625 del 24 de octubre de 1970 señala que:

> Ningún Estado o grupo de Estados tienen derecho a intervenir directa o indirectamente ya sea cual fuere el motivo, en los asuntos internos o externos de cualquier otro. Por lo tanto, no solamente la intervención armada, sino cualquier otra forma de inferencia o amenaza atentatoria a la personalidad del Estado, o de los elementos políticos, económicos y culturales que lo constituyen, son violaciones al Derechos Internacional.

Sin embargo, las relaciones entre los Estados no siempre son amigables y pueden surgir controversias de diversa índole. “En el campo de las relaciones internacionales, la manera idónea de resolver los conflictos es mediante las negociaciones internacionales”[18] aunque no siempre sucede.

Cuando los Estados se encontrar ante un conflicto se sugiere el uso de medios pacíficos de solución de controversias como pueden ser los buenos oficios, la mediación, la conciliación, la investigación o el arbitraje, pero, el mismo derecho internacional no descarta la posibilidad de que los Estados puedan llegar a la lucha

[18] Murguia Rosete, José Antonio, “Actualidades del derecho internacional convencional: la negociación y los tratados internacionales”, en Velázquez Elizarrarás, Juan Carlos, *El derecho internacional público en la agenda política de las relaciones internacionales*, México, UNAM, 2005, p. 377.

armada. Una situación que se antoja contradictoria en un mundo en el que se pugna por la paz mundial.

El derecho humanitario es el conjunto de normas jurídicas que regula precisamente los efectos de los enfrentamientos entre ejércitos y que a su vez protege a aquellas personas que no son combatientes.

El derecho internacional humanitario (DIH) también llamado derecho de guerra o derecho de los conflictos armados se encuentran regulados por los Convenios de Ginebra y los Convenios de la Haya.

> El derecho internacional humanitario forma parte del cuerpo de derecho internacional que rige las relaciones entre los Estados. El DIH tiene por objeto limitar los efectos de los conflictos armados por razones humanitarias. Su finalidad es proteger a las personas que no participan o han dejado de participar en las hostilidades, a los enfermos y heridos y a los prisioneros y las personas civiles, y definir los derechos y las obligaciones de las partes en un conflicto en relación con la conducción de las hostilidades.[19]

Si bien los conflictos armados se encuentran regulados por los Convenios de Ginebra y de la Haya es relevante preguntar si estas normas contemplan la posibilidad de enfrentamientos en el *ciberespacio*. La respuesta no es definitiva.

### 1. 3. Guerra, *ciberespacio* y *ciberguerra*

En la actualidad, la guerra es entendida en el lenguaje corriente como un combate entre Estados destinada a imponer la voluntad de uno de los bandos en el conflicto y cuyo evento se desenvuelve en el espacio aéreo, el espacio terrestre y el espacio marítimo de los Estados combatientes.

> la guerra como concepto legal tiene características y efectos propios que se extienden a muy diversas ramas del Derecho Internacional, no limitándose a los obvios *Ius ad Bellum et Ius in Bello*. Aún cuando esta figura tiene una serie de consecuencias jurídicas de alcance bastante importante, es interesante observar que hasta el día de hoy, no existe una definición universalmente aceptada sobre lo que es la misma, y aunque podemos encontrar un buen número de académicos que a lo

[19] Bugnion, François, "El derecho de Ginebra y el derecho de la Haya", *Revista Internacional de la Cruz Roja*, Comité Internacional de la Cruz Roja, 31 de diciembre de 2001, disponible en *https://www.icrc.org/es/doc/resources/documents/misc/5tdqeh.htm*, última fecha de consulta el 24 de mayo de 2019.

> largo del tiempo han intentado precisarla, lo que no encontraremos será una convención multilateral que nos ilustre sobre su significado a través de una dentición específica.[20]

Esta situación ocasiona que, si no existe una definición unívoca del concepto de guerra, será prácticamente un ejercicio infructuoso tratar de dar una definición de lo que debe entenderse por el concepto de *ciberguerra* sin embargo es común escuchar referir al concepto y considerar que los Estados tienen injerencia en un cuarto espacio aparte del aéreo, marítimo y terrestre y es el escenario de conflicto materia del presente estudio, el *ciberespacio*.

> … los conflictos armados que se manifiestan por medio de combates o luchas que tienen lugar, en principio, en espacios terrestres. Más tarde y al percatarse que desde el mar también es posible imponer esta voluntad surgen los combates navales y las acciones del mar sobre la costa, después aparecen de forma similar los combates en el aire y en el espacio. Cada vez que aparece una nueva dimensión real o virtual que el ser humano va a utilizar, los contendientes tratarán de dominarlo con objeto de poder emplearlo en su beneficio e impedir o dificultar su uso al adversario. Éste ha sido el caso últimamente del espacio electromagnético o éter y más recientemente aún, del espacio cibernético o *ciberespacio*…"[21]

El *ciberespacio* puede entenderse como una construcción digital desarrollada con computadoras, podría decirse que es "realidad virtual" sin embargo, para que esto se cumpla, debería ser desarrollada "por" computadoras y no "con" computadoras. El escritor William Gibson es quien acuñó el término en 1961, ayudando a popularizarse a través del Neuromante una novela publicada en 1964.[22] Así el *ciberespacio* es entendido como

> Un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores.[23]

---

[20] Ramírez García de León, Xavier Jared, *Conflicto armado no internacional en el México actual y cuasibeligerancia de los cárteles narcotraficantes*, Tesis, México, UNAM, Facultad de Derecho, 2012. p. 10.
[21] Feliu Ortega, Luis, *op. cit*., nota 13, pp. 37 y 38.
[22] Defínción de *ciberespacio*, Definicion.de, disponible en *https://definicion.de/ciberespacio/*, última fecha de consulta el 24 de mayo de 2019.
[23] Consejo Superior de Estudios de la Defensa Nacional, *op. cit*., nota 13, p. 171.

La interrogante aquí se desprende respecto a cómo un Estado puede ejercer control y actos de defensa sobre un espacio que es virtual y que no tiene fronteras delimitadas. Para responder a esta situación existen espacios que sin estar sujetos a la soberanía de ningún país tienen un tratamiento jurídico "internacional" tal es el caso de las aguas internacionales, el espacio exterior o los cuerpos celestes.

El *ciberespacio* está compuesto por tres capas: la capa sintáctica, la capa semántica y la capa física y es en cada una de estas capas que se reciben distintos tipos de ataques que se han venido defendiendo como ciberataques y debido a su intensidad y daño incluso como *ciberguerr*a.

Juan Pablo Salazar es de la opinión que hoy estamos ante la configuración de un nuevo espacio de poder que requiere revalorar las fronteras, la interdependencia de las economías ante la globalización así como la transformación de los mercados y los medios de comunicación, es el espacio digital que si bien no pertenece a ningún Estado cuenta con sus propias reglas, protocolos y relaciones de poder.[24]

> En junio de 2012, el fundador y CEO de Kaspersky Lab, Eugne Kaspersky, propuso un pacto internacional que regule las ciberarmas. Entonces, Kaspersky declaró: "La amenaza de la guerra cibernética ha sido uno de los temas más graves en el área de la seguridad de la información desde hace varios años", agregando que "La ciberguerra ha dejado entonces de ser un tema de ficción. Pero al contrario que las armas atómicas, biológicas y químicas, no existen reglas internacionales ni tratados sobre tal variante bélica. Las consecuencias de un ataque cibernético podrían ser igual de devastadoras que un ataque con armas tradicionales. Ejemplo de tales escenarios son el sabotaje de una central nuclear, en el peor de los caos podría resultar en una catastrófica fusión nuclear. Otros ejemplos son vertidos de sustancias químicas, o suspensión del suministro eléctrico en regiones completas".[25]

Tal es la relevancia de los ataques que se pueden realizar a los sistemas informáticos y las consecuencias que pueden derivarse que los países que

---

[24] Véase, Salazar, Juan Pablo, "La migración de la guerra al espacio digital", disponible en *https://www.sites.oas.org/cyber/Documents/2016%20-%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf*, última fecha de consulta el 24 de mayo de 2019.
[25] S/a, "LA OTAN publica manual de ciberguerra", *Diario TI*, 21 de marzo de 2013, disponible en *https://diarioti.com/la-otan-publica-manual-de-ciberguerra/62351*, última fecha de consulta el 24 de mayo de 2019.

conforman el Tratado del Atlántico Norte realizaron el estudio no vinculante sobre "*cyber conflicts and cyber warfare*", (los conflictos cibernéticos y la ciberguerra), nos referimos a el *Tallinn Manual of the International Law Applicable to Cyber Warfare*, mejor conocido como Manual de Tallinn que ha sido publicado por la editorial de la Universidad de Cambridge.

Ahora bien, entenderemos por *ciberguerra* como "un ataque sistemático al más alto nivel, incluyendo ataques de denegación de servicios críticos con el empleo de bornets, la mutilación de sitios web, el daño de los sistemas, a intrusión en infraestructuras críticas, etc.".[26] La *ciberguerra*, son todas aquellas acciones que se efectúan por parte de un agente estatal con el propósito de vulnerar los sistemas informáticos y redes de computadoras de otro Estado con la finalidad de causar distintas afectaciones. Como menciona el Consejo Superior de Estudios de la Defensa Nacional de España son diversas manifestaciones las que se dan como la denegación de servicio, el robo electrónico, el control indebido de instalaciones como de energía o transporte, y por supuesto el espionaje.

Los criterios para la determinación de un acto como *ciberguerra* según Juan Pablo Salazar son los siguientes:

> -Intensidad de hostilidades. Duración de la fuerza.
>
> -La hostilidad debe ser suficiente, necesaria y proporcional.
>
> -Incidentes esporádicos no son tratados por el derecho de los conflictos armados.
>
> -El hecho de ser armado no significa involucrar a las fuerzas armadas.
>
> -Un acto de espionaje a otro Estado no significa por sí mismo el resultado de un conflicto armado.[27]

El mismo autor señala que para estar frente a un acto de *ciberguerra*, se debe comprometer la seguridad nacional, muchas veces es a través de propaganda o espionaje, por la manipulación no autorizada de infraestructuras y sistemas

[26] Feliu Ortega, Luis, *op. cit*., nota 13, p. 32.
[27] Véase Salazar, Juan Pablo, *op. cit*. nota 23.

estratégicos con el objeto de poner en riesgo el funcionamiento económico o social de un Estado con fines políticos.[28]

> Con frecuencia se identifica el espionaje con la inteligencia. Sin embargo, ambos términos no son estrictamente sinónimos ya que el segundo engloba al primero. Los servicios de inteligencia generan un conocimiento especializado que es el resultado de un proceso sistemático y normalizado como consecuencia de la transformación de informaciones obtenidas por medios y recursos muy dispares, con métodos también muy diferentes, tanto de carácter abierto como secreto. Con independencia de que la inteligencia se estudie como proceso o como organización, su principal misión se orienta a minimizar los riesgos derivados de las amenazas y a potenciar las fortalezas para convertirlas en oportunidades. En toda época, pero especialmente en la actualidad, la definición de un buen sistema de inteligencia es una capacidad inestimable para afrontar satisfactoriamente el múltiple espectro de amenazas a la seguridad: desde la soberanía de la nación y su integridad jurídica y territorial hasta la defensa de los intereses comerciales, industriales y económicos mediante un sistema de inteligencia competitiva y económica.
>
> En última instancia, invertir en inteligencia para garantizar los objetivos de una agenda de seguridad y defensa resulta rentable y ningún otro medio tiene la enorme capacidad anticipatoria, preventiva y prospectiva. En todo caso, no se puede entender la actividad de inteligencia sin su reverso ineludible: la contrainteligencia. Penetrar en el secreto del adversario obliga a desplegar las capacidades para impedir que el adversario haga lo mismo con los secretos propios: incremento de la producción armamentística, situación de las bases militares, firmas de convenios económicos y acuerdos políticos, desarrollos tecnológicos y científicos punteros, etc., figuran entre los numerosos objetivos que deben ser protegidos de las acciones de un servicio extranjero. Inteligencia activa, y contrainteligencia defensiva, son por tanto, dimensiones de una misma realidad.[29]

El espionaje es una actividad que se realiza de manera cotidiana y más por los países con capacidades tecnológicas superiores que utilizan esta ventaja para recolectar, evaluar y analizar la información obtenida para así diseñar operaciones

---

[28] *Idem*.

[29] Navarro Bonilla, Diego, "Espionaje, seguridad nacional y relaciones internacionales", *Colección de estados internacionales*, núm. 14, 2013-2014, pp. 9 y 10, disponible en *https://web-argitalpena.adm.ehu.es/pdf/USPDF170933.pdf*, última fecha de consulta el 24 de mayo de 2019.

y tácticas de inteligencia[30] para la toma de decisiones e incluso para medir riesgos que afecten su seguridad nacional.

La capacidad de obtener información privilegiada sobre las actividades de aquella nación que se encuentra bajo el espionaje, proporciona ventajas para el Estado que obtiene estas informaciones lo que lo pone en una posición privilegiada y de ventaja frente a aquellos que no poseen dichas informaciones.

Las oficinas de inteligencia de los Estados recolectan información sobre seguridad para diseñar medidas de prevención de riesgo, disminución de daños y para prevenir o neutralizar las actividades que se consideren perjudiciales a los intereses nacionales.

Precisamente en las actividades de inteligencia se suelen utilizar medidas de espionaje que pueden vulnerar o comprometer la seguridad de otras naciones.

En poco tiempo se

> ha visto incrementar la tensión en la relación entre Estados, como consecuencia de una masiva y sistemática filtración de información clasificada que marca un punto de inflexión en las relaciones internacionales. Nunca antes la acción de un *whistleblower* como Edward Snowden había llegado a socavar de manera tan profunda los principios y fundamentos que habían definido el contexto de interacción entre países, tanto aliados como manifiestamente adversarios. Frente a otras filtraciones contemporáneas, especialmente las orquestadas por Julian Assange y el movimiento Anonymous, este caso ha marcado una notable diferencia.[31]

Así los actos realizados en nombre de operaciones de inteligencia han dejado de manifiesto que el espionaje que se realiza por medios tecnológicos han superado las medidas de seguridad estatales y por otra parte que ya no son únicamente los

---

[30] La ley de Seguridad Nacional, en su artículo 29 define a la inteligencia como “el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotaicón de información, para la toma de decisiones en materia de Seguridad Nacional”.
Ley de Seguridad Nacional Diario Oficial de la Federación 31 de enero de 2005, última reforma publicada el 8 de noviembre de 2019. Disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac_081119.pdf*, última fecha de consulta el 23 de diciembre de 2019.

[31] *Idem*.

Estados y sus agencias de inteligencia quienes pueden realizar estas tareas sino que hoy por hoy agentes no estatales también pueden vulnerar la seguridad informática de los Estados, razón por la cual urgen mecanismos internacionales vinculantes para paliar estas realidades de sabotaje y espionaje que se suceden en el *ciberespacio*.

El Manual de Tallinn, establece que las partes involucradas para poder determinar una *ciberguerra* deben ser agentes Estatales o bien actores no estatales que toman el control de uno de los Estados involucrados en las hostilidades. (privados al servicio del Estado).[32]

Ahora bien, una vez establecida la relación entre el concepto de guerra, el *ciberespacio* y la *ciberguerra* consideramos necesario profundizar sobre el concepto de *ciberespacio* y así proporcionar los elementos que permiten entenderlo como espacio en el que se puede desarrollar un conflicto "bélico" para así poder entender cuál es el escenario en el que actualmente se "enfrentan" los denominados ciberejércitos.

### 1.4. Breve análisis del *Ciberespacio* como escenario de guerra

Como se explicó al inicio del capítulo, el concepto de soberanía ha permitido que cada Estado pueda ejercer ese poder dentro de su jurisdicción. Sin embargo, en el contexto internacional, existen determinados espacios denominados *Common Grounds* sobre los cuales los Estados no pueden ejercer plena soberanía por lo que ha sido fundamental determinar una situación jurídica distinta sobre ellos.

Los *Common Grounds* "[p]odemos definirlos como aquellos espacios del orbe que no están bajo jurisdicción o control de Estado alguno, están abiertos al acceso y uso de actores estatales y no estatales".[33]

---

[32] Véase Manual de Tallinn, Regla 32 sobre el ciberespionaje en tiempo de paz y Regla 33 sobre los actores no estatales.

[33] Grünschläger, Gustavo Ricardo, "Global Commons", *Revista de la Escuela de Guerra Naval*, Armada de Argentina, núm. 61, diciembre 2015, p. 46. Disponible en *http://www.cefadigital.edu.ar/bitstream/123456789/334/1/4_Revista_61_Global_Commons_w4.pdf,* última fecha de consulta el 25 de mayo de 2019.

Los bienes comunes "son formas específicas de acuerdos sociales para el uso colectivo, sostenible y justo de los recursos comunes. Se les entiende también como régimenes autorregulados, cuyo acceso, uso y derechos de participación de ellos están regidos por reglas determinadas por la comunidad misma…".[34]

María Cecilia Añaños Meza explica que para asegurar el éxito y efectividad de la regulación sobre los bienes comunes o *Common Grounds*, deben fundarse en:

> una acción colectiva autoorganizada, autoregulada y autoadministrada por los actores o usuarios mismos, estipulada mediante un acuerdo contractual y vinculante de cooperación. La misma debe contener reglas coherentes y claramente definidas por los participantes que determinen la apropiación, las formas de uso y cooperación, la restricción, el aprovisionamiento, la distribución, etcétera, las decisiones deben ser tomadas colectivamente y con la participación de sus miembros en su modificación; debe existir un mecanismo de supervisión y control recíproco del cumplimiento de las reglas, de sanciones graduales o proporcionadas contra el incumplimiento, y un mecanismo de resolución de conflictos, así como de un reconocimiento exterior del derecho de autoorganizarse; por último, deben existir múltiples niveles de organización interna y coordinación de recursos que son parte de sistemas más grandes.[35]

El *ciberespacio* como es sabido contiene reglas definidas, sin embargo, no puede ser controlado por sus propias características de interoperabilidad, flexibilidad y anonimato lo que hacen que su control sea prácticamente imposible.

La información que está contenida en cada una de las computadoras alrededor del mundo hoy permiten conocer inclusive un perfil humano y psicológico de quien utiliza esa herramienta.

López de Turiso y Sánchez explica que:

> en la década de los años ochenta se produjeron tres grandes hitos que marcarían definitivamente el futuro de la informática, sus comunicaciones y la seguridad: la aparición del PC, el despegue de Internet y surgimiento del malware. Hoy día, treinta años después, la utilización del *ciberespacio* para la comisión de delitos o actividades ilícitas se ha extendido

---

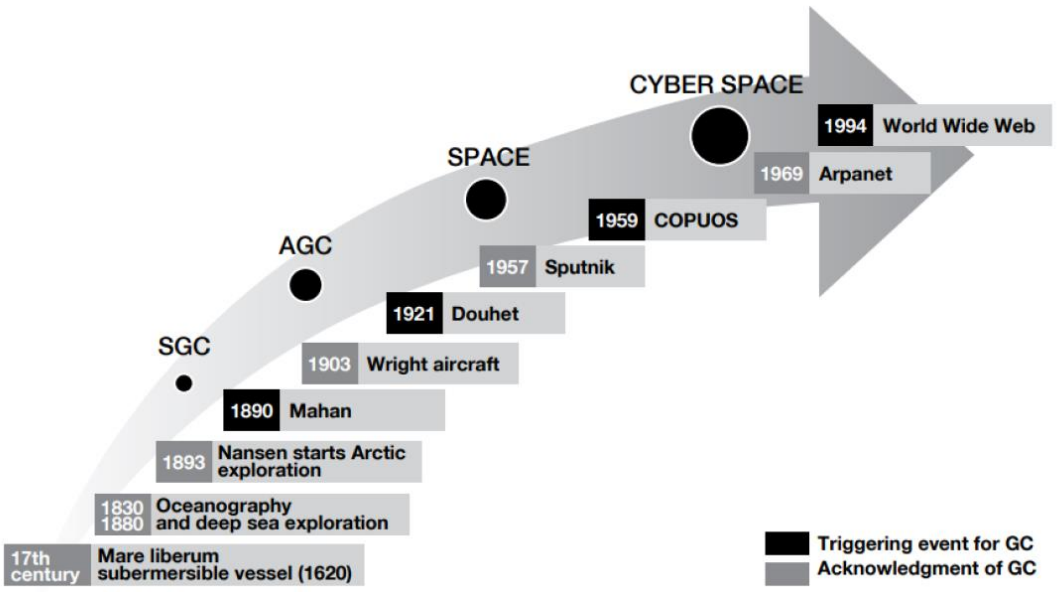
[34] Añaños Meza, María Cecilia, "La idea de los bienes comunes en el sistema internacional: ¿renacimiento o extinción?, *Anuario Mexicano de Derecho Internacional*, vol. 14, diciembre 2014, disponible en *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542014000100005*, última fecha de consulta el 25 de mayo de 2019. Una cita fue omitida.

[35] *Idem*.

> profusamente, lo que está originando una gran alarma social por lo novedoso del escenario utilizado.[36]

Sería importante considerar si el *ciberespacio* cuenta con estos estándares pues siguiendo el pensamiento de Gustavo Ricardo Grünschläger los bienes comunes han evolucionado siendo el primero de ellos el *Mare Liberum*, seguido del espacio aéreo, luego el espacio ultraterrestre hasta llegar al ciberespacio.37

Figura 1. Evolución de los bienes o Common Grounds




Fuente: Tomado del artículo de Gustavo Ricardo Grünschläger "Global Commons".[38]

De esta manera el *ciberespacio* como cualquiera de los otros bienes comunes puede ser considerado como un espacio en el cual pudieran realizarse actos violentos ya que su característica de virtual no es una limitante sino más bien una particularidad. José Ramón Casar Corredera, define al:

> *ciberespacio*, como un escenario de conflicto mayor, en el que las actuales escaramuzas, mayoritariamente aún de baja intensidad, pudieran evolucionar a enfrentamientos de mayores dimensiones, que posiblemente combinados con otras actuaciones de fuerza,

[36] López de Tursio y Sánchez, Javier, "La evolución del conflicto hacia un nuevo escenario bélico", en *El ciberespacio. Nuevo escenario de confrontación*, *op. cit*., nota 13, p. 120.
[37] Grünschläger, Gustavo Ricardo, *op. cit*., nota 31, p. 46.
[38] *Idem*.

> quizás en otros Commons, constituyan una verdadera guerra, la que ha dado en llamarse ciberguerra.[39]

Así, el *ciberespacio* es considerado como el nuevo espacio de confrontación entre naciones, en el que entres de naturaleza privada al servicio de naciones también pueden participar. Ahora, es pertinente reflexionar sobre el objeto estudio de esta investigación que son las condiciones y elementos sobre los cuáles se conforma y regula un *ciberejército*.

El ciberespacio fue defiido en la Estrategia Nacional de Ciberseguridad de 2017 como "… un entorno digital constitutido por redes informaáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como hacen en el mundo físico".[40]

### 1.5. La evolución del concepto ejército a *ciberejército*

Un ejército, es el conjunto de fuerzas armadas, hombres y mujeres, que están a cargo de las acciones bélicas de un Estado. Normalmente se encuentra conformado por distintas unidades, cuerpos y servicios.

Krepinevich[41] plantea diez revoluciones en los ejércitos desde que se hacían los enfrentamientos de milicia contra milicia en el siglo XIV y evolucionando con las revoluciones de infantería, las artillerías, las fortalezas, las fuerzas navales hasta llegar a la mecanización, la aviación y la información que trajo la Primera Guerra Mundial.

Las revoluciones militares consideran cuatro elementos de acuerdo a Andrew F. Krepinevich, el cambio tecnológico, el desarrollo de sistemas, la innovación operacional y la adaptación organizacional. Los avances en los entrenamientos militares son de gran importancia que incluso se han desarrollado simuladores de

---

[39] Casar Corredera, José Ramón, "Introducción", *El Ciberespacio, nuevo escenario de confrontación*, *op. cit*., nota 13, p. 11.
[40] Gobierno de México, "Estrategía Nacional de Ciberseguridad", México, 2017, p. 27, disponible en *https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf*, última fecha de consulta 16 de diciembre del 2019.
[41] Véase Krepinevich, Andrew F., "Calvary to Computer. The Pattern of Military Revolutions", *The National Interest*, Fall 1994.

operaciones militares que incluyen altos niveles de sistemas e integración de arquitecturas.

Un *ciberejército* va más allá de entrenamientos de los soldados con simuladores. El *ciberjercito* se entiende como aquel grupo de personas encargado de defender la soberanía de una Nación dentro de su espacio de protección en el *ciberespacio.*

Las actividades de un *ciberejército* en concreto son:

> Dirigir las operaciones y la defensa de las redes de información específicas del Departamento de Defensa.
>
> Preparar y, cuando así se indique, llevar a cabo todo el espectro de las posibles operaciones militares en el *ciberespacio*, con el objetivo de facilitar las acciones en todos los ámbitos.
>
> Garantizar libertad de acción […] en el *ciberespacio*, y negar la misma a sus adversarios.[42]

Como es evidente las estrategias que se realizan por parte de un *ciberejército* serán distintas a las de un ejército convencional pues el tipo de elementos y recursos disponibles sin distintos.

A continuación, se profundizará sobre este tipo de estrategias y las armas que son utilizadas en el *ciberespacio*.

### 1.6. Estrategia bélica en el *ciberespacio*

Clausewits define a la estrategia como un acto sostenido de voluntad necesaria con la finalidad de dominar las terribles incertidumbres de la guerra. La estrategia comienza con el establecimiento de una meta o un objetivo con claridad.[43]

---

[42] Pastor Acosta, Oscar "Capacidades para la defensa en el *ciberespacio*", *op. cit*., nota 13, p. 241.

[43] Véase McMaster, H. R., "Continuity and Change. The Army Operating Concept and Clear Thinking about future War, Military review, March – April 2015, p. 10. La traducción es libre. Disponible en *https://www.queensu.ca/kcis/sites/webpublish.queensu.ca.kciswww/files/files/2015/MilitaryReview_20150430_art005.pdf*, última fecha de consulta el 26 de mayo de 2019.

Las estrategias desplegadas por los *ciberejércitos* que se realizan en el *ciberespacio* están relacionados con las medidas de *ciberdefensa* y *ciberseguridad*. En este espacio de grandes volúmenes de información, el espionaje es la actividad preponderante que despliegan los miembros de un ciberejército pues se busca la obtención de:

> 1. Información secreta militar (orden de batalla de un ejército extranjero, tecnología de defensa, información sobre armamento, renovación y actualización de capacidades, etc.
>
> 2. Información secreta industrial para alcanzar ventaja competitiva frente a rivales económicos (planes estratégicos, proyectos de innovación de productos y servicios, invenciones y modelos en áreas sensibles, etc.).
>
> 3. Información secreta de naturaleza política (decisiones de gobierno, planes estratégicos, negociaciones internas y exteriores, desarrollo económico, acuerdos internaciones sectoriales, etc.,).[44]

La *ciberseguridad* y *ciberdefensa* alegadas por los Estados para desplegar actividades en el *ciberespacio* se explican a continuación.

### *1.6.1 Ciberseguridad*

El concepto de seguridad ha cambiado menciona Feliu Ortega "desde su categoría jurídica que desde el concepto clásico de orden público y paz pública, seguridad interior y exterior del Estado, ha ido evolucionando hasta uno más amplio y multidimensional como es el de Seguridad Nacional que se define hoy como 'el estado deseado por una sociedad en el que pueda ésta desarrollarse y prosperar libre de amenazas'".[45]

La ciberseguridad de acuerdo a Feliu Ortega es:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgo, 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

---

En original se lee "Clausewitz defined strategy as a sustained act of will necessary to master war's terrible uncertainties. Strategy begins with establishing a clearly defined objective or goal".

[44] Navarro Bonilla, Diego, *op. cit*., nota 28, p. 13.

[45] Feliu Ortega, Luis, *op. cit*., nota 13, p. 39.

> organización y los usuarios son los dispositivos informáticos conectados, los usuarios, lo servicios-aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluye una o más de las siguientes: disponibilidad, integridad, la autenticidad y el no repudio y la confidencialidad.[46]

El autor continúa en la reflexión sobre los espacios en donde se llevan a cabo las confrontaciones y concluye que en lugar de referirse a conceptos como guerra naval o guerra aérea, guerra económica o guerra psicológica, deberían utilizarse específicamente los contextos en donde se desarrollan las actividades bélicas para así poder referir a la guerra en el mar, la guerra en el aire o bien la guerra en el *ciberespacio*.[47]

La ciberseguridad entendida como aquellas herramientas para la protección y defensa del espacio electromagnético forman parte hoy en día de las estrategias de Seguridad Nacional de los Estados en las cuales se debe de incluir las medidas de prevención, protección, respuesta, mitigación y recuperación ante posibles ataques.

La *ciberseguridad* según la OTAN "en su MC0571 (NATO *Cyberdefense*) la define como 'la aplicación de medidas de seguridad para proteger las infraestructura de los sistemas de información y comunicaciones frente a los ciberataques'"[48], lo que podríamos incluir las llamadas Infraestructura de Información Crítica (IIC)[49] o

[46] *Ibidem*, p. 46.
[47] *Ibidem*, p. 47.
[48] *Ibidem*, p. 42.
[49] El Manual Administativo de Aplicación General en Materia de tecnologías de la Información define a las infraestructuras críticas de información como: "Las infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de biens y preatción de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia".
El Manual distingue a las infraestructuras Críticas de Información de las Infraestructuras de Informaicón esenciales, entendiendo por estas ´últimas a "Las redes, servicios, equipos e instalaciones asociados o vinculados con los activos de

infraestructuras estratégicas entendiendo por estas a todos los sistemas y activos tanto virtuales como físicos que resultan vitales para la seguridad nacional de los Estados tanto en materia económica, financiera, abastecimiento, de seguridad, de salud pública, de comunicaciones por mencionar algunas.

Ahora bien, la ciberseguridad de acuerdo a lo establecido en el documento Estrategía Nacional de Ciberseguridad de México, la cual se dictó en el año 2017, la define como "conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección e la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación".[50]

Las infraestructuras estratégicas como se puede advertir son fundamentales para el funcionamiento regular indispensable de alguna área en específico cuya destrucción o intervención puede causar un grave impacto o afectación para el Estado y su población.

Por todo lo anterior será importante para los Estados considerar cuáles son sus vulnerabilidades y dependencias en las infraestructuras estratégicas para poder diseñar y planear una adecuada estrategia de ciberseguridad que garantice su Seguridad Nacional.

### *1.6.2 Ciberdefensa*

Como se mencionó al inicio de este capítulo, los Estados protegen su soberanía nacional de cualquier amenaza que pudiera poner en peligro la seguridad de su territorio, su infraestructura o su nación. Las maneras en que puede garantizarse esta seguridad va desde las negociaciones con otros Estados, el estrechamiento de

---

información, TIC y TO [Tecnologías de Operación], cuya afectación, interrupción o destrucción tendría unimpacto mayor en la operación de las instituciones".
Acuerdo por el que se modifican las políticas y disposicions para la Estategia Digial Nacioal, en materia de tecnologías de la Infomración, así como el Manual Administativo de Aplicación General en dichas materias, disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016*, última fecha de consulta el 23 de diciembre de 2019.

[50] Gobierno de México, *op. cit*. nota 39, p. 27.

relaciones diplomáticas y consulares, así como establecimiento de relaciones comerciales, económicas, políticas, educativas, culturales, deportivas, etcétera.

Sin embargo, como también se adelantaba al inicio de este capítulo, el uso de la fuerza es una herramienta para garantizar la seguridad nacional o bien utilizarse como un medio de defensa. En palabras de Feliu Ortega la defensa es básicamente disuasiva y "comprende […] todas las acciones y medidas necesarias para garantizar la ciberseguridad […]".[51]

Para la Estrategía Nacional de Ciberseguridad, la ciberdefensa se define como "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".[52]

La defensa llevada en el espacio electromagnético o también llamado cibernético o *ciberespacio* presenta características que lo distinguen del tipo de defensa que puede orquestarse en medios tradicionales como es el espacio terrestre, marítimo, aéreo o espacial.

Las características específicas del *ciberespacio* que deben tomarse en cuenta para planear una adecuada defensa son las siguientes:

> El *ciberespacio* es un ambiente único sin fronteras geográficas. El atacante puede estar en cualquier parte del globo y es difícil localizarlo.
>
> La defensa es muy compleja pues intervienen muchos factores. Entre otros hay que considerar que intervienen no solo elementos estatales si no también privados. Exige pues una estrecha coordinación entre todos ellos.
>
> La confrontación en el *ciberespacio* representa frecuentemente las características de un conflicto asimétrico. El atacante puede ser muy inferior al atacado en medios técnicos y con relativamente pocos medios y baratos puede causar tremendos perjuicios. Además, es frecuentemente anónimo y clandestino. Así pues, atrae, no solo a los gobiernos sino también a otros diferentes actores que incluyen los terroristas y las mafias del crimen organizado.

[51] Feliu Ortega, Luis, *op. cit*., nota 13, p. 39.
[52] Gobierno de México, *op. cit*. nota 39, p. 27.

> El *ciberespacio* no debe considerarse aisladamente a efectos de la defensa puesto que esta interrelacionado estrechamente con los demás espacios.
>
> La utilización del *ciberespacio* permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema y a menudo sin delatarse Una de sus facetas es el espionaje militar, político o industrial como se mencionó.
>
> Permite fácilmente también ejercer el chantaje, pero al mismo tiempo, la defensa puede utilizar el *ciberespacio* para la disuasión.
>
> Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC.[53]

La *ciberdefensa* como el conjunto de herramientas, sistemas, personas, infraestructuras, capacidades, etcétera, permitirán a los Estados llevar a cabo las medidas y acciones necesarias para poder contener, defender, prever, mitigar y reparar los ataques que se realicen en el *ciberespacio* en contra de sus sistemas permitiendo así que las afectaciones y consecuencias que se pudieran derivar tengan las menores consecuencias o repercusiones.

Sin embargo, una consideración que debe tenerse en cuenta en las estrategias para la *ciberdefensa* es que en el *ciberespacio* no solo se realizan amenazas de *ciberguerra* sino que también pueden sucederse eventos de ciberespionaje y ciberterrorismo realizados por particulares, situación que no resulta fácil para los Estados como ya lo advertíamos al principio.

### 1.7. El concepto de arma en el *ciberespacio*

Como hemos expuesto arriba, a pesar de no existir un concepto definitivo sobre *ciberguerra*, se suele utilizar para refiere a los actos que se llevan a cabo contra un Estado por parte de otro Estado para afectar o desestabilizar su infraestructura estratégica, pero que sin embargo estos ataques no es fácil distinguirlos de un ataque ciberterrorista o un acto de ciberespionaje efectuado por un particular.

Ahora es preciso aclarar que tampoco existe un consenso sobre el concepto de *ciberarma*. Margarita Robles Carillo hace un estudio de las diferentes aproximaciones doctrinales al respecto y encuentra lo siguiente:

---

[53] Feliu Ortega, Luis, *op. cit*., nota 13, pp. pp. 44 y 45.

Cuadro 1 Aproximaciones al concepto de ciberama

| Aproximación | Definición de arma cibernética |
|---|---|
| Informe EastWeast Institute Critical Terminology Foundations | software, firmware or hardware designed or applied to cause damage through the cyber domine |
| Manual de Tallinn | Cyber means of warfare that are by design, use, or intended use capable of causing either injury to, or death of, persons; or damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack. |
| Simobet y Brown | Hay que distinguir tres armas: el código, el sistema informático y el operador. |
| Tesis negacionistas | No existe como tal una acción armada |
| Kolb, tesis relativista | Se puede utilizar cualquier objeto como un arma como incluso puede ser la contaminación ambiental o radioactiva. |

Cuadro elaborado con información tomada del artículo de Margarita Robles Castillo. El concepto de arma cibernética en el marco internacional.[54]

Podemos concluir que por ahora no existe una definición de arma cibernética o ciberarma. Sin embargo, se hace referencia a estas como el tipo de herramientas utilizadas para llevar a cabo las agresiones en el *ciberespacio* son los conocidos virus informáticos, los trolls, los botnet, las intrusiones a sistemas informáticos en general, el espionaje y también se consideran como una arma a la propaganda digital por ejemplo.

### 1.8. Ciberguerra realidad o ficción

Para finalizar el presente capítulo consideramos que era necesario brindar al lector dos ejemplos para que sea el quien juzgue si en realidad el concepto de *ciberguerra*, *ciberarmas* y *ciberejércitos* son válidas ya que como se ha expuesto hasta ahora si bien es cierto la comunidad internacional expresa su interés en mantener al *ciberespacio* libre de peligros y agresiones y refiere la importancia de tener estándares como los expuestos en el Manual de Tallinn, la realidad es que existen

[54] Robles Castillo, Margarita, "El concepto de arma cibernética en el marco internacional: una aproximación funcional", *Documento de Opinión, Instituto Español de Estudios Estratégicos, Boletín Electrónico*, 3 de octubre de 2016, pp. 10 -12. Disponible en *http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf*, última fecha de consulta el 26 de mayo de 2019.

opiniones diversas respecto no a los actos y ataques sino más bien al mal uso de los conceptos.

Por ello a continuación se exponen de forma sucinta dos de los casos que han sido considerados como actos de ciberguerra. El primero de ellos es conocido como el caso “The Angency” y el otro como el caso Stuntext.

### *1.8.1 El caso “The Agency”, The New York Times Magazine, Adrian Chen*

El caso “The Agency” se trata de una investigación realizada por el periodista Adrain Chen, quien viajó en el año 2015 a San Petersburgo para corroborar la existencia de la utilización de una granja rusa de trolles, o también conocidos como bots, que son robots que se encargan de retuitear mensajes específicos, falsos o ficticios con un propósito en común. En esta ocasión la granja en Rusia llamada “Internaitoal Resesarch Agency”, se dedicó a apoyar la campaña del presidente Trump.

El caso de uso de bots con tendencias a la desinformaicón, a generar alarma social o para dirigir o persuadir la opinión pública se considera como una intrusión en la libertad de opinión y en la desinformación que genera. Sin embargo, no existen elementos suficientes desde nuestro punto de vista para señalar que nos encontramos con elementos que puedan específicamente calificar esta acción como un acto de *ciberguerra*. El lector podrá juzgar por sí mismo.

### *1.8.2 El caso Stuxnet, Natanz, Irán*

El caso Stuxnet, se refiere a un virus malicioso conocido, que en el año 2010 tomó control de máquinas que enriquecían uranio en una central nuclear en Irán. El virus informático conocido como “worm”, realizó lo siguiente:

> **1- Stuxnet penetró en la red**
>
> Según la firma de seguridad cibernética Symantec, Stuxnet probablemente llegó al programa nuclear de Natanz de Irán en una memoria USB infectada.
>
> Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red. El gusano penetró así en el sistema informático de la planta.
>
> **2- El gusano se propagó a través de las computadoras**

Una vez dentro del sistema informático, Stuxnet buscó el software que controla las máquinas llamadas centrifugadoras.

Las centrífugas giran a altas velocidades para separar componentes. En la planta de Natanz, las centrifugadoras estaban separando los diferentes tipos de uranio, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares.

**3- Stuxnet reprogramó las centrifugadoras**

El gusano encontró el software que controla las centrifugadoras y se insertó en él, tomando el control de las máquinas.

Stuxnet llevó a cabo dos ataques diferentes. En primer lugar, hizo que las centrifugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después, desaceleró las centrifugadoras durante unos 50 minutos. Esto se repitió en distintas ocasiones durante varios meses.

**4- Destrucción de las máquinas**

Con el tiempo, la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas 1000, se desintegraran.

Durante el ataque cibernético, alrededor del 20 por ciento de las centrifugadoras en la planta de Natanz quedaron fuera de servicio.[55]

Hasta la fecha no se ha podido saber la procedencia del ataque, aunque se ha llegado a presumir que fue perpetrado por los Estados Unidos e Israel quienes pudieran estar interesados en sabotear el programa nuclear iraní.

Después de este virus se han detectado otros ataques, uno de los más conocidos es el troyano Havex, y el Insudtroyer, que pueden acceder a los sistemas de control industrial. Con este caso se deja al descubierto que los ataques *cibernéticos* pueden ser desplegados por los mismos Estados o bien por entes privados que pretenden causar afectaciones a los sistemas industriales. Así es necesario repensar los conceptos que a lo largo de este capítulo presentamos. Invitamos al lector a que sea él quien haga las reflexiones finales.

[55] BBC, iWonder, "El virus que tomó control de mil máquinas y les ordenó autodestruirse", *BBC News Mundo*, 11 de octubre de 2015, disponible en *https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet*, última fecha de consulta el 26 de mayo de 2019.

A continuación, en el siguiente capítulo dejaremos las consideraciones teóricas respecto a los ciberejércitos, y nos adentraremos en el análisis de los mismos en cuanto a los Estados que ya cuentan con ellos en la práctica.

.

# Capítulo 2

# Los *Ciberejércitos* en la experiencia de algunos Estados

# Capítulo 2 *Ciberejércitos* en la experiencia de algunos Estados

En el presente capítulo se brinda información respecto al estado del arte en el que se encuentra el tema de los *ciberejércitos* a nivel internacional, se presentan reflexiones respecto a las consideraciones que la comunidad internacional ha vertido al respecto de justificar la ciberguerra, el uso de las armas cibernéticas, la inteligencia artificial en las operaciones ofensivas y defensivas así como sobre las instituciones militares en el ámbito digital.[56]

En una segunda parte se analizan los fundamentos jurídicos respecto al tema de la *ciberguerra*, el uso de *ciberejercitos* y de *ciberarmas* detectado hasta el momento en documentos internacionales para finalmente identificar la experiencia de algunos Estados que ya han desarrollado *ciberejércitos* tal es el caso de Alemania, España, China, India, Inglaterra y Corea del Norte, para que con base en su estudio se puedan identificar cuáles son los lineamientos que deben privar en la conformación, reglamentación y operación de un ciberejército en genera

## 2.1. Política internacional y consideraciones de la comunidad internacional respecto al despliegue de ciberataques alrededor del mundo

Los ataques en contra de los medios informáticos se dan desde los años cincuenta con los virus y caballos de Troya en un inicio que permitían a los hackers apoderarse, eliminar o alterar determinada información almacenada en una computadora. Con el paso del tiempo los ataques se han ido haciendo más sofisticados con el uso de gusanos, denegaciones de servicios o bonets. Fue hasta los años ochenta que el Departamento de Estado de los Estados Unidos comenzó a considerar los ataques de este tipo como una nueva amenaza.[57]

---

[56] Véase Salazar, Juan Pablo, "La migración de la guerra al espacio digital", disponible en *https://www.sites.oas.org/cyber/Documents/2016%20-%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf*, última fecha de consulta el 21 de mayo de 2019.

[57] Véase Remus, Titiriga, "Cyber-attacks and international law of armed conflicts; a 'jus ad bellum' perspective", en *Journal of International Commercial Law and Technoloogy*, vol. 8, no. 3, 2013, p. 179.

Andrea Bendovschi en su artículo Cyber-Attacks-Trends, Patterns and Security Counter measures, explica que existe una correlación entre el sector que recibe los ataques y el tipo de ataque que se ejecuta; por ejemplo establece que en el caso del espionaje cibernético es más probable que éste apunte a los sectores de gobierno y los medios de comunicación, mientras que si se trata de realizar un cibercrimen, la guerra cibernética y las técnicas de hacktivismo se dirigirán en contra de los sectores empresariales.[58]

Entonces podemos presumir que dependiendo del tipo de ataque que se prepare son las medidas y contramedidas que se pueden llevar a cabo para hacer frente a estos ataques. Por lo que no será lo mismo reforzar las medidas de seguridad de una empresa para mitigar los ataques que realizar una estrategia de *ciberdefensa* en la que incluso se haga uso del espionaje cibernético. En cuyo caso se entiende que son los Estados quienes deben de diseñar dichas estrategias.

Por su parte Christian Czosseck y Kenneth Geers en su obra *The Virtual Battlefield: Perspectives on Cyber Warefare* señalan que en el mundo contemporáneo actual en general y en los países desarrollados en particular la confianza en los avances tecnológicos es tal que no se les considerada un lujo sino por el contrario como una necesidad donde existen tres elementos que son dependientes entre sí en caso de una estrategia de guerra en el *ciberespacio*: el gobierno, el ejército, y las personas.[59]

> El secretario general de la ONU, António Guterres, ha abogado por establecer reglas globales para minimizar el impacto de la ciberguerra en los civiles. 'Ya que existen episodios de guerra cibernética entre Estados. Y lo peor es que no hay un esquema reglamentario para este tipo de guerra, no está claro si ahí se aplica la Convención de Ginebra o el

[58] Véase Bendovschi, Andreea, "Cyber-Attacks – Trends, Patterns and Security Countermeasures", en *Procedia Economics and Finance*, núm. 28, 2015, p. 26.
[59] Czosseck, Christian y Geers, Keneth, (eds.), *The virtual battlefield: Perspectives on Cyber Warfare*, Amsterdam-Berlín-Tokyo-Washington, D.C., IOS Press, 2009, p. 6.

> Derecho Internacional pueden aplicase en estos casos', ha reconocido el máximo responsable de la ONU.[60]

Sin embargo, es en realidad poco lo que por parte de las Naciones Unidas se ha avanzado con respecto a la regulación de las actividades relacionadas la ciberguerra en el *ciberespacio*. Algunas de las resoluciones han sido:

> - Resoluciones de la Asamblea General 55/63 (2000) y 56/121 (2001). A través de estas resoluciones se invita a los Estados Miembros a que tomen en cuenta las medidas propuestas, al elaborar leyes y políticas nacionales, para combatir la utilización de la tecnología de la información con fines delictivos.
> - Resoluciones de la Asamblea General 57/239 (2002) para la creación de una cultura global de ciberseguridad. A través de esta resolución se exhorta a crear la citada cultura teniendo en cuenta los principios de: conciencia, responsabilidad, respuesta ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación.
> - Resolución de la Asamblea General 58/199 (2004) para la protección de las infraestructuras de información. Se persigue estimular el desarrollo de normas de conducta en el *ciberespacio* que sirvan para la promoción del desarrollo socioeconómico y el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información.[61]

Como se observa, las resoluciones en comento invitan, exhortan y promueven ciertas conductas de los Estados en el *ciberespacio* y aún no son normas específicas vinculantes al respecto. Tampoco se discute sobre una costumbre internacional instantánea que pudiera abonar en la temática sino más bien son pocos los ejercicios que en este tenor se desarrollan respecto a la ciberseguridad y *ciberdefensa* en el contexto internacional.

---

[60] Martín del Barrio, Javier, "El secretario general de la ONU dice que hay 'ciberguerra entre los Estados'", *El País*, publicado el 19 de febrero de 2018, disponible en *https://elpais.com/internacional/2018/02/19/actualidad/1519058033_483850.html*, última fecha de consulta el 3 de junio de 2019.

[61] Reguera Sánchez, Jesús, "Aspectos legales en el *ciberespacio*. La ciberguerra y el Derecho Internacional Humanitario", *Análisis del Grupo de Estudios en Seguridad Internacional*, Universidad de Granada, 14 de junio de 2015, pp. 11 y 12.

Como ejemplos respecto al actual de la comunidad internacional e materia de ciberseguridad y *ciberdefensa* a continuación se detallen dos instrumentos internacionales el Manual de Tallinn y el Convenio de Budapest.

### 2.2. Ciberseguridad y *ciberdefensa* en el contexto internacional

En el capítulo anterior se explicó la relación que existe entre la ciberseguridad y la defensa que despliegan los Estados como parte de su estrategia nacional. Ahora bien, estos dos conceptos en el contexto internacional son relevantes ya que como también se apuntó al inicio de esta investigación los Estados como entes soberanos tienen como una de sus primicias garantizar su integridad territorial así como salvaguardad la integridad de su nación.

De esta manera los Estados conscientes de que los avances tecnológicos hoy día también representan amenazas a su seguridad nacional, deben de recurrir a las estrategias de ciberseguridad, así como medias de *ciberdefensa* ante los eventuales ataques de los que pudieran ser objeto siempre y cuando se encuentren de conformidad con las normas que dicta el derecho internacional. Es decir que en general los ataques militares se encuentran prohibidos en materia internacional a menos que sean el resultado de una defensa propia o cuando estos ataques son avalados por el Consejo de Seguridad de Naciones Unidas.[62]

> Desde el punto de vista de la regulación de los conflictos, los gobernantes que recurran a la ciberguerra lo tendrán que hacer desde el respeto al *ius ad bellum* (el Derecho Internacional que rige la autorización del empleo de la fuerza por los Estados soberanos y del ius in bello (el de la conducción de las hostilidades), mientras no se tenga ninguna regulación acorde a la regulación de estos nuevos conflictos (nueva o aclaratoria del DIH aplicado en la ciberguerra).[63]

A pesar de esta realidad respecto a los ataques en el *ciberespacio* hasta el año 2017 solo la mitad de los países contaban con una estrategia de seguridad o

---

[62] Véase Pasman, Matthew C., "Cyber Attacks as "Force" Under UN Charter Article, vol. 2, núm. 4, Columbia Law School, 2011, disponible en *https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1882&context=faculty_scholarship*, última fecha de consulta el 4 de junio de 2019.
[63] Reguera Sánchez, Jesús, *op. cit*., p. 5.

se encontraban en proceso de crearla,[64] pese a que desde el año 2001 ya se había celebrado la Convención sobre Ciberciminalidad en Budapest que diera paso posterior al Convenio con el mismo nombre que entrara en vigor el año 2004.

También como se adelantaba en líneas anteriores un documento relevante en el tema de la ciberguerra es precisamente el Manual de Tallinn respecto a la defensa cibernética en virtud de la educación, la investigación y el desarrollo. Este Manual si bien no resulta ser un documento vinculante para los Estados, sí es referente para interpretar las normas existentes en torno a los ciberataques y para invitar a un análisis jurídico plural que incluya a los Estados respecto a determinados valores tanto jurídicos, pero también éticos en el *ciberespacio*.

Debido a la relevancia que tienen estos dos instrumentos es que se profundizará al respecto en los siguientes puntos.

### *2.2.1. Convenio de Budapest, 2001*

Con la aparición de las tecnologías de la información y la comunicación los actos ilícitos haciendo uso de estos dispositivos puso en tela de juicio si estas conductas podían ser sancionadas por medio de las normas de cada Estado pues dichas conductas que se desplegaban a través de esta nueva herramienta informática puso de manifiesto que podrían fácilmente trascender fronteras nacionales; así el *ciberespacio* se convirtió en el escenario perfecto para llevar a cabo delitos como el hacking o el esparcimiento de software malicioso, o los ataques por medio de la denegación de servicios, todos estos si bien son constitutivos de actos ilícitos en el *ciberespacio*, no hay elementos que determinen que específicamente estas actividades sean o deban ser considerados como actos de ciberguerra.

El gran avance de este instrumento sin lugar a dudas es el que coloca en el escenario internacional la necesidad de regular conductas ilícitas que se realizan

[64] ITU, “Half of all countries aware but lacking national plan on cybersecurity, UN agency reports”, *UN News, Global perspectives stories*, 5 July 2017. Disponible en *https://news.un.org/en/tags/cyber*, última fecha de consulta el 4 de junio de 2019.

haciendo uso de las tecnologías de la información y la comunicación. En palabras de Danya Centeno:

> El Convenio sobre la Ciberdelincuencia, popularmente conocido como Convenio de Budapest, fue elaborado durante el 2001 por el Consejo de Europa, con la activa participación de los Estados involucrados, con el fin de combatir la comisión de delitos informáticos. Se trata del único tratado internacional vinculante en la materia y constituye una especie de guía, "ley modelo" o "acuerdo marco" para que los Estados Parte: i) implementen dentro de su ordenamiento jurídico nacional la legislación pertinente para investigar y perseguir penalmente aquellos delitos cometidos en contra de sistemas o medios informáticos o mediante el uso de los mismos y ii) faciliten la cooperación internacional en este sentido.
>
> El Convenio está abierto a ratificación para Estados no parte del Consejo de Europa. En función de que durante los últimos años se ha incrementado considerablemente la "ciberdelincuencia" tanto a nivel nacional como internacional, también ha aumentado considerablemente la presión internacional para que más países, sobre todo aquellos que no pertenecen al Consejo, se adhieran al tratado. Sin embargo, no todos los Estados parten de los mismos contextos ni enfrentan los mismos problemas en materia de delitos relacionados con las tecnologías de la información y las comunicaciones así como de respeto al Estado de Derecho y a los derechos humanos.[65]

El Convenio contempla la tipificación de los siguientes delitos: delitos contra la confidencialidad, integridad y disponibilidad de sistemas y datos informáticos; los delitos cometidos haciendo uso de las tecnologías de la información y telecomunicaciones, los delitos por el contenido que se difunde por medio de ellos y los delitos en el área de derechos de autor.

43 países en Europa han ratificado el Convenio frente a tan solo 8 países del continente americano (entre ellos Argentina y Paraguay en el año 2018, Chile y Costa Rica en el 2017, Canadá en 2015, Panamá en 2014, República Dominicana en 2013 y los Estados Unidos en 2006), 4 en el continente africano (Cabo Verde y Marruecos en al año 2018, Senegal en el 2016 y Mauricio en 2013), al igual que el

[65] Centeno, Danya, *México y el Convenio de Budapest. Posibles incompatibilidades*, Red en Defensa de los Derechos Digitales (R3D) y Derechos Digitales. América Latina, 2018, p. 3, disponible en *https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf*, última fecha de consulta el 3 de junio de 2019.

continente asiático (Filipinas en 2018, Israel en 2016, Sri Lanka en 2015 y Japón en 2012) y solo dos en Oceanía Australia y Toga ambos en el año 2012.

Como se puede observar, son realmente pocos los Estados que han ratificado el Convenio y esto se debe en gran medida a:

> que el cibercrimen constituye una forma de delincuencia, pero puede ser caracterizado con precisión como algo más que eso; tiene las características básicas propias de la delincuencia tradicional (un actor, una víctima y la comisión de un daño socialmente intolerable), pero no tiene base territorial. A diferencia de los delitos tradicionales, el cibercrimen puede trascender fácilmente las fronteras nacionales. En cambio, la respuesta de la Convención para tal circunstancia es tradicional: tal como los tratados de asistencia legal recíproca, ella solicita a los países brindarse asistencia unos a otros a través de investigaciones y procedimientos en los respectivos países. Esto implica continuar con el sistema de cumplimiento local y descentralizado de que hemos dispuesto por siglos.[66]

Así teniendo los Estados un amplio margen para poder adaptarse a lo establecido por el Convenio hace de lo que podría ser una de sus fortalezas se convierta en una complicación para su ratificación por parte de varios Estados que no pueden cumplir estos estándares.

### *2.2.2. Manual de Tallinn, 2013*

Por su parte el Manual de Tallinn, es un documento resultado de la investigación y formación en temas de ciberguerra a cargo de personal experto del centro de Excelencia de la OTAN que se ubica en Tallinn, Estonia.

Derivado del incremento en los ciberataques fue necesario establecer las bases sobre la *ciberdefensa*.

[66] Brenner, Susan W., “La Convención sobre Cibercrimen del Consejo de Europa”, Revista Chilena de Derecho y Tecnología, Centro de Estudios en Derecho Informático, Universidad de Chile, vol. 1, núm. 1, 2012, p. 236.

Es menester recordar que precisamente el Manual es un documento generado por expertos en el tema de la *ciberdefensa* pero que sin embargo no es un documento que resulte vinculante para los Estados.

Algunos de los Estados que participan en este Centro se encuentran Alemania, España, Italia y Turquía. Algunas de sus funciones es mejorar las estrategias de *ciberdefensa* mediante el desarrollo de programas para la misma OTAN y los estados miembros.

El Manual en comento tenía como finalidad establecer si el derecho internacional aplicaba en los casos suscitados en el *ciberespacio*. Lamentablemente las respuestas no son terminantes al respecto pues es complejo tener una respuesta única si se hace referencia al concepto por ejemplo del uso de la fuerza, en cuyo caso para algunos expertos el hecho de que con los ataques perpetrados por medios digitales pueda ocasionar afectaciones en los oponentes como puede ser los daños físicos, entonces estos actos sí deben ser considerados como uso de la fuerza.[67]

El manual se divide en secciones y dentro de los temas que se tratan son el conflicto armado, las hostilidades, la responsabilidad estatal, el uso de la fuerza, la soberanía, las acciones de organismos internacionales gubernamentales, la conducción de las hostilidades entre otros.

En lo que interesa a la presente investigación sobre el tema de los miembros de las fuerzas armadas en el curso de operaciones en el ciber espacio el grupo de expertos consideró la importancia de establecer la relación que existe entre los individuos que llevan a cabo las operaciones durante un conflicto en el *ciberespacio* para así determinar a qué grupo de los combatientes pertenece. Sin embargo, la situación es compleja debido a que las organizaciones que se encuentran únicamente en un entorno virtual es difícil que se les reconozca como combatientes

[67] Véase, Schmitt, Michael N., *International Law in ciberespace: The Koh Speech and Tallinn Manual Juxtaposed*, Harvard International Law Journal, vol. 54, 2012.

ya que para tener ese estatus una de las características es que los individuos deben tener un distintivo que claramente los identifique de individuos que no son parte de las fuerzas armadas o que no son combatientes, esto en el mundo no virtual supone por ejemplo el uso de uniformes militares.

Otro de los temas sobre el cual los expertos han reflexionado es referente a los objetivos militares ya que en teoría al llevarse una operación militar en el *ciberespacio* el objetivo que se ataca debiera ser específicamente del Estado combatiente dejando de lado a cualquier otro objetivo civil. Sin embargo, un ataque en el *ciberespacio* resulta complicado identificar si la operación es perpetrada por un combatiente y si el objetivo en específico que se ataca pertenece al Estado o si solo se trata de un ataque criminal en el *ciberespacio*.

El tipo de incidentes que se han perpetrado a lo largo de los últimos años han evolucionado y se han ido perfeccionando para así causar las mayores afectaciones. En un principio los ataques se enfocaban en tiempos de conflicto en contra de los medios de comunicación y conectividad de que disponían los combatientes. Poco a poco los ataques también se usaron como censura propaganda en la red, y posteriormente evolucionaron al punto de que se centraron en las infraestructuras críticas como se explicaba en el capítulo anterior, la denegación de servicios, el robo de información estratégica e información confidencial, por citar algunos.

Es evidente que los países que han sido objeto de los ataques en el *ciberespacio* también resultan ser los Estados que han desarrollado mayores estrategias en el espacio digital, los principales Estados que se encuentran en la arena de lo que se conoce como la ciberguerra son: Israel, Estados Unidos, Kosovo, Palestina, China, Reino Unido, Rusia, Georgia, Irán, Canadá Japón, Corea del Norte, India, Ucrania, Alemania, Francia.

Varios de estos Estados cuentan con la conformación de ciberejércitos que dan cuenta de que los enfrentamientos en el *ciberespacio* son cada vez más frecuentes. A continuación, se expondrá sobre estos ciberejércitos.

## 2.3. Experiencias nacionales en torno al tema de ciberejércitos

La implementación de ciberejercitos ha sido una actividad que se comenzó a gestar desde los años noventa debido a la evolución de las tecnologías. Diversos actores en el escenario internacional comenzaron a opinar sobre la nueva era de la información y sus impactos nocivos en cuanto a la vulneración de la seguridad y soberanía de los Estados. Ejemplo de ello son los comentarios del Departamento de Defensa de los Estaos Unidos haciendo referencia a los ciberataques perpetrados supuestamente por China o bien las declaraciones del Ministerio de Defensa del Reino Unido sobre la necesidad de implementar ciberfuerzas de un cuarto Ejército.

El uso del *ciberespacio* con fines de atacar a un deterinado Estado incluye desde prácticas de desinformación o propagandistas, la minería de datos, el fraude electrónico, pasando por el espionaje industrial, sistemas informáticos maliciosos, interferencias ilegales o apropiación ilegal de datos.

Pero cada Estado ha comenzado a desarrollar sus propias estrategias en materia de seguridad a través del *ciberespacio*. Algunos de los más representativos son los siguientes:

### *2.3.1. Alemania*

En el año 2017 Alemania anunció la creación de un equipo conformado en un inicio por 260 personas con la intensión de alcanzar 13,500 miembros entre personal militar y civiles para conformar oficialmente un ciberejército. La fecha programada para comenzar las operaciones de esta unidad está programada para el año 2021 y tiene como principales finalidades proteger las infraestructuras críticas que incluye las estructuras militares y sistemas de armamento.[68]

> Ni siquiera el Ejército alemán ha quedado exento de agresiones digitales: el Bundeswehr dice haber identificado y repelido alrededor de dos millones de incursiones no autorizadas en sus sistemas en 2017; de ellas,

[68] Véase Euronews, “Alemania lanza su ciber-ejército”, abril 2017, disponible en *https://es.euronews.com/2017/04/06/alemania-lanza-su-ciber-ejercito*, última fecha de consulta el 5 de junio de 2019.

> 8.000 habrían conseguido acceder a sus redes y causado daños enormes si las medidas defensivas habituales no hubieran funcionado. Fue con ese telón de fondo que la ministra de Defensa de Alemania, Ursula von der Leyen, inauguró el Cyber- und Informationsraum (CIR) en Bonn en abril de 2017.
>
> Sus miembros –260 expertos, civiles y uniformados– se esmeran en proteger la seguridad nacional desde barricadas tan disímiles como la inteligencia militar, las telecomunicaciones, la tecnología de la información y los sistemas de información geográfica. El teniente coronel Marco Kempel y su equipo se ocupan de todo tipo de tareas, desde la conducción de entrenamientos mediante juegos de guerra virtuales hasta la optimización de escudos digitales, como los que impiden la reprogramación no autorizada o el hackeo de los drones.[69]

Una de las problemáticas que enfrenta este país en la conformación de un ciberejército es que no cuentan con el suficiente capital humano que puedan contratar para incluirlos en sus filas y que también el espacio para contratar nuevo personal tiene que pasar por una serie de pasos en los cuales no se había contemplado el perfil de personas expertas en temas tecnológicos específicos para prevenir, contener o repeler los ataques en el *ciberespacio*.

El Estado alemán ha creado dos instituciones para estos efectos, el primero es el Centro Nacional de *Ciberdefensa* (Nationales Cyber-Abwehrzentrum) encargado de detectar las potenciales amenazas así como analizar dichas amenazas y coordinar las medidas necesarias para hacer frente a dichas amenazas.[70]

Por otra parte se encuentra el Consejo Nacional de Ciberseguridad (National Cyber Security Council) bajo el mando de la Oficina Federal para la Seguridad de la Información, que trabaja en conjunto con otras oficinas como la Oficina Federal de Protección Civil y Asistencia en Desastres, la Oficina Federal de Policía Criminal y la Policía Federal así como el Servicio Federal Alemán de Inteligencia todo esto

---

[69] Véase DW, "Ciberdefensa: el Bundeswehr y sus desafíos", Actualidad, Política, Disponible en *https://www.dw.com/es/ciberdefensa-el-bundeswehr-y-sus-desaf%C3%ADos/a-44989489*, última fecha de consulta el 5 de junio de 2019.

[70] Véase Stackelberg, Filippa von, "Germany prepares for cyber war", New security learning. Technology-Assisted Training for Security, Defence and Emergency Services, disponible en *http://www.newsecuritylearning.com/index.php/feature/88-germany-prepares-for-a-cyber-war*, última fecha de consulta el 5 de junio de 2019.

necesario para analizar y prever los posibles ataques pues Alemania es un país que controla y maneja desde sistemas computacionales el abastecimiento de agua, electricidad, energía nuclear así como también el sistema bancario y de transporte ferroviario por lo que los ciberataques que no fueran detectados pudieran causar serios problemas en la estabilidad y seguridad del país.[71]

Alemania recibe aproximadamente de cuatro a cinco ataques por medio de los conocidos trojanos al día, que tratan de penetrar los sistemas de seguridad para realizar espionaje y sabotaje principalmente.[72]

> La seguridad cibernética en Alemania debe garantizarse a un nivel acorde con la importancia y protección que exigen las infraestructuras de información interconectadas, sin obstaculizar las oportunidades y la utilización del *ciberespacio*. En este contexto, el nivel de ciberseguridad alcanzado es la suma de todas las medidas nacionales e internacionales tomadas para proteger la disponibilidad de información y comunicaciones, la tecnología y la integridad, autenticidad y confidencialidad de los datos en el *ciberespacio*.
> La ciberseguridad debe basarse en un enfoque integral. Esto requiere intercambio de información y coordinación más intensivos. La estrategia de ciberseguridad se centra principalmente en los enfoques y medidas civiles. Se complementan con medidas tomadas por la Bundeswehrp para proteger sus capacidades y medidas basadas sobre los mandatos para hacer de la seguridad cibernética una parte de la seguridad preventiva de la estrategia alemana. Dada la naturaleza global de la tecnología de la información y las comunicaciones, coordinación internacional y redes apropiadas centradas en el extranjero y la seguridad los aspectos de política son indispensables. Esto incluye la cooperación no solo en los Estados Unidos, Naciones Unidas, pero también en la UE, el Consejo de Europa, la OTAN, el G8, la OSCE y otras organizaciones multinacionales. El objetivo es garantizar la coherencia y las capacidades de la comunidad internacional para proteger el *ciberespacio*. [73]

La estrategia del gobierno alemán en materia de ciberseguridad y *ciberdefensa* se resumen en los siguientes puntos:

1. Protección de las infraestructuras críticas de información

---

[71] *Idem.*
[72] *Idem.*
[73] Véase European Union Agency for Network and Information Security, (UNISA), Europa, “Ciber Security Strategy for Germany”, Noticias, 2011, disponible en *https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1*, última fecha de consulta el 5 de junio de 2019.

2. Asegurar los sistemas de tecnología de la Información en Alemania.
3. Reforzar la tecnología en materia de seguridad de la administración pública alemana.
4. Optimizar el Centro Nacional de Ciberrespuesta.
5. Armonizar las distintas instituciones, oficinas y demás órganos necesarios para garantizar el adecuado funcionamiento del Consejo Nacional de Ciberseguirdad.
6. Tener un control efectivo sobre los crímenes cometidos en el *ciberespacio*.
7. Llevar a cabo acciones coordinadas en materia de ciberseguridad en Europa y alrededor del mundo.
8. Uso de tecnología de la información confiable.
9. Desarrollo del interés en la ciberseguridad del personal y autoridades federales.
10. Contar con las herramientas necesarias para responder a los ataques cibernéticos.
11. Implementación de estos objetivos estratégicos de manera sostenible.[74]

Definitivamente en el campo de la *ciberdefensa* el Estado Alemán es consciente de que uniendo su fuerza con otros actores importantes se logran más y mejores resultados.

### *2.3.2. España*

El gobierno español cuenta con distintas instituciones que funcionan de manera conjunta para contar con una adecuada protección y prevención en materia de ciberseguridad y *ciberdefensa*. Dentro de estas oficinas se encuentran el Consejo de Seguridad Nacional, Comité Especializado de Ciberseguridad, y el Comité Especializado de Situación.

En conjunto con estas instituciones el gobierno español tiene seis objetivos específicos en materia de ciberseguridad que se resumen en:

> 1) para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el

[74] *Ibidem*, pp. 3-7.

> adecuado nivel de seguridad y resiliencia; 2) para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular; 3) en el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el *ciberespacio*; 4) en materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del *ciberespacio*; 5) en capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad; y 6) en lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.[75]

El gobierno español cuenta también con distintas líneas de acción para alcanzar los seis objetivos antes señalados y son:

1) Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.
2) Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.
3) Seguridad en los sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.
4) Capacidad de investigación y persecución del ciberterrorismo y la ciberdelicnuencia.
5) Seguridad y resilencia de las TIC en el sector privado.
6) Conocimientos, competencias e I+D+i.
7) Cultura de ciberseguridad.
8) Compromiso internacional.[76]

---

[75] Gobierno de España, Presidencia del Gobierno, *Estrategia de ciberseguridad nacional*, s/f, disponible en European Union Agency for Network and Information Security, disponible en *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy*, última fecha de consulta el 5 de junio de 2019.
[76] *Ibidem*, pp. 31-38.

Al igual que el análisis que se realizó respecto a la experiencia del gobierno alemán se deja de manifiesto que en el tema de ciberseguridad y *ciberdefensa* ya no es suficiente que las fuerzas armadas sean las encargadas de armar las estrategias necesarias, sino que se involucran inclusive los actores privados para poder tener una política estatal más acorde a las amenazas que representa el inadecuado manejo del *ciberespacio* y el desconocimiento de los potenciales riesgos y vulnerabilidades.

Como se dejó de manifiesto, el Estado alemán y el Estado español refuerzan sus acciones en el *ciberespacio* por medio de la creación de organismos ex professo, así como fomentar la cooperación internacional.

### *2.3.3. China*

China siempre ha sido un impulsor de las Tecnologías de la Información y Comunicación, considerado uno de los principales creadores de nuevas formas de implementación en TIC, lo anterior aunado de que en diversas ocasiones ha sido acusado de que su gran crecimiento económico se debe a los constantes ataques relacionados al ciberespionaje económico para efectos de robo de patentes y secretos industriales que catapulta a esta Nación como una de las principales creadoras de piratería en cualquier industria empresarial.

De igual forma, la cercanía que tiene con Rusia, entendiendo que este país es el principal jugador en tópico de la ciberguerra, ha hecho que China se fortalezca en entrenamiento de oficiales de alto rango en la ciberguerra, incluso existen datos que hacen pensar que la Nación realiza constantes financiamientos en la comunidad hacker para obtener nuevos talentos que posteriormente se utilizarán como nuevos integrantes de sus ciber fuerzas armadas.

En julio de 2004, Juang Zemin, Presidente de la comisión militar Central hizo una llamada a las fuerzas militares para equiparse con tecnologías de la información para prepararse para una posible ciberguerra.[77]

[77] Pastor Acosta, Oscar; *et. al*, *Seguridad Nacional y Ciberdefensa*, Cuadernos Cátedra ISDEFE-UPM, Madrid, Imagen Gráfica, 2009, p. 127, disponible en

Además, Shen Weiguang reconocido estudioso de la ciberguerra, escribió:

> Aquellos que toman parte de un ciberataque no son soldados, Cualquiera que sepa informática puede convertirse en un luchador en la red. Hay que pensar en la posibilidad de carros de combate no gubernamentales que pueden tomar la decisión de entrar en el conflicto; no solo hay que buscar la movilización de la gente joven, también industrias relacionadas con las tecnologías de la información serán las primeras en ser movilizadas y formar parte de la guerra.[78]

Esto nos refleja el avance bélico que caracteriza a la nación oriental como una de las principales fuerzas militares no solo en el quinto elemento de conflicto, sino también en todos y cada uno de ellos, siempre motivados por la carrera militar frente a los Estados Unidos de América; no podemos dejar pasar por alto la gran característica nacionalista que tiene la nación, la cual lleva de la mano su poderío castrense.

En el mismo texto citado de los dos párrafos que anteceden, hace referencia a que China destina más de 65,000 millones de euros anuales, de los cuales el 9,6% se destina a la mejora en TIC. A este proceso de le bautizó como la “acupuntura militar” a efectos de paralizar al enemigo atacando la debilidad del enlace de su mando, control de comunicaciones e información.

China se enfoca en tres pilares de ataques, el primero consiste en el la vigilancia con la intención de recoger inteligencia enemiga para poder trazar rutas de ataque; la segunda basada en la ofensiva en donde se realizan “operaciones para interrumpir, sabotear y destruir información en los sistemas de red enemigos utilizando equipamiento especializado”[79] buscando como principal objetivo de ataque las infraestructuras críticas e infraestructuras críticas de la información; y por último la protección en donde evidentemente buscan no se objetivos substanciales de sus enemigos.

---

*http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf*, última fecha de consulta el 3 de junio de 2019.

[78] *Idem*.

[79] *Idem*.

Para contar con una alta eficacia en las operaciones asignadas, la PLA (Peoples Liberation Army), dentro de la Academia de Mando y Comunicaciones, en Wuhan, se encuentra la Universidad de Ingeniería en Información, en Zhegzhou, la Universidad de Ingeniería y Ciencias y la Universidad de Ciencia y Tecnología en defensa Nacional, en Changsa.[80]

En el entrenamiento de los soldados incluyen teoría básica de ordenadores y aplicaciones; tecnologías de redes de comunicaciones; unidades conectadas por TIC; contramedidas electrónicas; tecnologías RADAR; reglas y regulaciones en ciberguerra; tácticas y estrategias en ciberguerra; sistemas de información incluyendo el reunir, diseminar y usar la información; mando, monitorización, toma de decisiones, y sistemas de control. Otra parte del entrenamiento de los soldados del PLA incluye el uso de ciberarmas, simulación de ciberguerras, protección de sistemas de información, ataques con virus informáticos y defensa frente a los mismos, jamming y anti-jamming en redes de comunicaciones.[81]

### *2.3.4. India*

India, ha tenido un reconocimiento en la última década por el incremento de capacidad de capital humano en Tecnologías de la Información y Comunicación, esto ha llevado a que su connacionales estén presentes en la mayoría de países en Latinoamérica y Europa aportando creatividad tecnológica en áreas a de desarrollo de tecnología, por lo que la industria militar no se quedó atrás y a partir del año dos mil se empezaron a hacer aportaciones por parte no solo de la industria pública sino también por la industria militar.

Fue entonces en el año dos mil dos, cuando el gobierno de la India invitó a la industria privada, la cual antes no era tomada en cuenta por cuestiones de seguridad, en donde se invirtió principalmente en tres áreas principales: tecnologías

[80] *Idem*.
[81] *Idem*.

de la información y ciberguerra; infraestructuras de guerra electrónica y C4I; y movilidad [82]

En el mismo año se crea la *Defence Intelligence Agency* (DIA) quien es la encargada de la coordinación de inteligencia de las fuerzas de tierra, mar y aire, agencia de quien tiene una subdivisión denominada *Defence Information Warface Agency (DIWA)*, encargada de las operaciones psicológicas, ciberguerra y ondas electromagnéticas.

Dentro de la Estrategia de Seguridad Nacional del Estado indio de este año 2019, se establecen medias que toman en consideración a los Estados vecinos como China, Pakistán y Afganistán.

Se resaltan las medidas pacíficas de solución de controversias y por supuesto el reforzamiento de las capacidades en materia de fronteras marinas y terrestres, las capacidades militares, la transformación de la policía, la inteligencia y por supuesto la ciberguerra.

India reconoce que el aumento de los ciberataques lo colocan en el cuarto lugar de los países con problemas de ciberseguridad a nivel mundial lo que afecta a su población con los ciberdelitos como es el robo de datos, intrusiones y por supuesto los daños patrimoniales a sus nacionales haciendo uso de las tecnologías.

También los ataques a las infraestructuras críticas son un problema para los temas del funcionamiento de los medios de transporte, la energía y por supuesto el funcionamiento de las instituciones financieras.

El gobierno indio consciente de que no puede rastrear los ataques que recibe en el *ciberespacio* ni saber tampoco cuál es la capacidad del adversario pero sabe la necesidad de evaluar sus capacidades de llevar a cabo un contra ataque cibernético.

Por ello se decanta por una política que considera como un ataque hostil en contra de su soberanía nacional cualquier ataque cibernético malicioso y adelanta

[82] *Ibidem*, p. 132.

que responderá con todos los medios y recursos a su disociación sean cibernéticos, militares, diplomáticos o económicos.[83]

Dentro de las estrategias del gobierno indio está el desarrollo y fabricación de software y hardware elaborado por compañías privadas indias. Para hacer esto posible el gobierno debe brindar financiación y asistencia para la compra de equipos y priorizar las áreas sobre sistemas operativos, software, microelectrónica, equipo de red asó como sistemas de navegación y algoritmos criptográficos.[84]

### *2.3.5. Reino Unido*

El gobierno de Reino Unido, ha desarrollado su Seguridad Nacional teniendo muy en cuenta la protección a las infraestructuras críticas de ataques terroristas, criminales y naciones hostiles.

Las acciones que se desarrollan en general mencionados en su estrategia nacional son las siguientes:

> - Creación del Centro para la Protección de las Infraestructuras Nacionales (Centre for the Protection of National Infrastructure, CPNI) como resultado de la fusión de otros dos Centros:
>
>  - Uno de ellos encargado de aconsejar e informar sobre seguridad en redes y otros asuntos de seguridad de la información;
>  - Otro en materia de seguridad de las instalaciones y del personal.
>
> Con el asesoramiento del CPNI, se protege la seguridad de la nación reduciendo las vulnerabilidades de las infraestructuras.
>
> - Desarrollando una Estrategia Nacional de Seguridad de la Información e implementándola, en parte, mediante el Programa Técnico de Seguridad de la Información y la Lucha contra el Cibercrimen.
>
> Por otro lado, al igual que en el caso norteamericano, los esfuerzos a nivel civil se están viendo complementados por aquellos que el Ministerio de Defensa (MoD) está realizando a nivel de *Ciberdefensa*. Entre estos, destaca la prioridad de adquisición de ciertos medios tecnológicos para el nuevo campo de batalla, “el *ciberespacio*” como son:

---

[83] S/A, *India’s National Security Strategy*, 2019, p. 39, disponible en *https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf*, última fecha de consulta el 5 de junio de 2019.
[84] *Idem*.

- Dentro de la recolección de información (datos de fuentes reales y entrega de estos datos para labores de inteligencia) destaca la Ciber-recolección, determinando como tecnologías prioritarias aquellas para realizar:
    - Representación de diagramas de redes ("network mapping").
    - Monitorización de tráfico y sistemas. O Análisis de vulnerabilidades.
    - Análisis e integración de eventos de seguridad.
    - Fusión de información.

- Dentro de la seguridad de la información de las TIC, el MoD utiliza, al igual que el DoD en EE.UU., el concepto de la "Defensa de Redes de Ordenadores" en donde incluye: o Sistemas de Detección de Intrusos. O Sensores. O Protección de Intrusiones. O Análisis e Integración de Eventos de Seguridad. O Reacción y Respuesta. O Protección contra Virus, Gusanos y Malware. O Gestión de Parches de Seguridad. O Prevención de Denegaciones de Servicio.[85]

Dentro de la estrategia nacional de Reino Unido se incluye la responsabilidad de las personas en la sociedad pues se considera que solo actuando de manera conjunta se puede lograr un *ciberespacio* seguro así como también es necesario el involucramiento del sector privado pues mucho del *ciberespacio* se encuentra en manos de las compañías privadas.[86]

Otro de los puntos que se comparte con las consideraciones de los otros Estados es el tema de la cooperación internacional sobre la importancia de reglas de comportamiento en el *ciberespacio*, de acuerdo con las leyes tanto nacionales como internacionales.

El Estado cuenta con un Centro para la Protección de Infraestructuras Nacionales (CPNI), dentro de las varias actividades que desarrolla el centro existen las Sesiones InfoSec que son un conjunto de documentos de interés general, que

[85] Pastor Acosta, Oscar; *et. al*, *op. cit*., nota 72, p. 32.
[86] S/A, *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*, p. 22, disponible en *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf*, última fecha de consulta el 5 de junio de 2019.

destacan los riesgos a los que se expone la infraestructura nacional, las Notas Técnicas de Seguridad de la Información, la Identificación de Vulnerabilidades, la Guía de Buenas Prácticas y Puntos de Vista sobre los informes desarrollados.

Finalmente respecto a los esfuerzos en específico del Ministerio de la Defensa del Reino Unido y en particular en relación con la seguridad de la información y las Tecnologías de la Información y la Comunicación se tiene como tecnologías prioritarias, la criptografía y las operaciones de defensa en redes de computadoras dentro de los que se incluye: los sistemas de detección de intrusos, sensores, análisis e integración de eventos de seguridad, reacción respuesta, protección contra virus, malware y gusanos, gestión de parches de seguridad y prevención de denegaciones de servicios.[87]

Por supuesto que tampoco se dejan de lado los controles de acceso y gestión de identidades así como las técnicas de intercambio seguro de información.[88]

### *2.3.6 Corea del Norte*

Corea del Norte tiene la característica de ser una nación con una red de fibra óptica alrededor de toda su nación y estar a disposición de cualquier sector de la sociedad. El gobierno también ha invertido en brindar acceso a una red de telecomunicaciones y servicios de telefonía satelital a su población pero con un estricto control. Todas las redes están habilitadas para usos militares si fuese necesario.[89]

Una de las estrategias del gobierno de Corea del Norte es específicamente detectar las vulnerabilidades de sus posibles adversarios y atacarla

---

[87] *Ibidem*, p. 88.
[88] Idem.
[89] United States of America, Department of Defense, "Militaru and security developments involving the Democratic People's Republic of Korea", Anual Report Congress, 2013, disponible en *https://dod.defense.gov/Portals/1/Documents/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf*, última fecha de consulta el 5 de junio de 2019.

específicamente más que confrontar a sus adversarios lo que se conoce como una estrategia asimétrica.

Una de las oficinas con mayor injerencia en el tema de la Ciberseguridad del Estado norcoreano es la Oficina General de reconocimiento (RGB) que prácticamente es conocida por su actividad en el *ciberespacio* tendiente a las actividades de terrorismo, espionaje y actividades clandestinas en general.

La Oficina 121 conocida como *Electronic Reconnaissance Bureau's Cyber Warfare Guidance Bureau* o solo *Bureau* 121 es una unidad cibernética con misiones específicas en el *ciberespacio* que despliega operaciones tanto de defensa como de ataque. Dentro de sus actividades se encuentran operaciones en el *ciberespacio* como espionaje, y actividades criminales. Una situación que ha despertado el interés respecto al *ciberespacio* es que este grupo poco a poco se ha ido perfeccionando en la militarización de virus de computadora. Existen actualmente un gran número de reportes que señalan a la oficina RGB de Corea del Norte como los creadores de un sinfín de virus que permiten el espionaje.[90]

El Estado norcoreano también ha desarrollado políticas de Estado que promueven la educación en materia de tecnologías por ello incluso las Universidades están enfocándose en preparar a los estudiantes en el desarrollo de software tecnológico, así como tecnologías de control numérico que permite hacer pruebas en satélites. También estos esfuerzos se replican en el sector de la manufactura de hardware y en el desarrollo de tecnología militar.[91]

El gobierno norcoreano ha establecido desde los años ochenta y noventa diversos centros como es el Centro Coreano de Computación y el Centro de Informática de Pyongyang que data de 1986.

---

[90] Jun, Jenny, LaFoy, Scott y Sohn, Ethan, *North Korea's Cyber Operations, Strategy and Responses. A report of the CSIS Korea Chair*, Londres, Nueva York, Boulder, Lanham, Center for Strategic and International Studies, Roman & Littlefield, 2015, pp. 43 y 44, disponible en *https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf*, última fecha de consulta el 6 de junio de 2019.
[91] *Ibidem*, p. 52.

Dentro de sus principales objetivos en materia de ciberseguridad, el gobierno norcoreano ha planteado el preparar gradualmente a organizaciones relacionadas con la cibernética, identificar sus propias vulnerabilidades, relacionar operaciones sobre la libertad en el *ciberespacio* y la mitigación y resiliencia de las medidas para responder a los sistemas críticos y redes operacionales de mantenimiento continuado durante o posterior a recibir ataques.[92]

Al igual que otros Estados Corea del Norte promueve la cooperación internacional para por un lado implementar operaciones de forma conjunta pero también para implementar determinadas sanciones dependiendo de lo que se juzgue como una conducta ilícita en el ámbito del *ciberespacio*.[93]

*2.3.7. Irán*

Irán tiene varias características negativas en relación con las TIC, en el entendido que no cuenta con servicios de telecomunicaciones con tecnología de punta, tal como pudiera ser el uso de servicios telefónicos, que es a cuenta sabida rudimentario, sin dejar pasar por alto las consecuencias religiosas y su cuestionamiento respecto a la interacción de sus ciudadanos con la hiperinformación.

Desde principios del año dos mil, el Consejo Nacional de Inteligencia de los Estados Unidos, predijeron que tanto Irán e Irak eran ejemplos de naciones quienes "tenderán a explotar la utilidad de las tecnologías de la información en operaciones asimétricas. Para contrarrestar las capacidades militares de EE.UU, estos Estados buscarán formas de explotar nuestras vulnerabilidades, incluyendo el empleo de ciberguerras y ciberterrorismo".[94]

Por lo anterior, en el año 2004, la nación del norte incluyó a Irán dentro de la lista de países capaces de llevar a cabo ciberataques contra los intereses de los Estados Unidos. Desde la CIA se asegura que este país ya cuenta con el capital

[92] *Ibidem*, p. 64.
[93] *Ibidem*, p. 71.
[94] Pastor Acosta, Oscar; *et. al*, *Seguridad Nacional y Ciberdefensa*, Cuadernos, *op. cit*., nota 72, p. 135.

humano entrenado en los artes de ciberguerra, catalogándolo como poco probable que intentase atacar algún objetivo militar.

Aquí hay que puntualizar que la cercanía y alianzas que tiene la nación Iraní, con India y Rusia ha supuesto un incremento en la obtención de tecnología militar, incluso al tener intercambios universitarios entre la Universidad de Teherán y las universidades Rusas implícitas en conocimientos de software y hardware con inclinaciones militares.

### *2.3.8. Estados Unidos*

Posterior a los ataques perpetrados el 11 de septiembre, los Estados Unidos han despuntado en el diseño de sus estrategias de seguridad para la protección de sus infraestructuras críticas. Ha desarrollado Operaciones de Información con la finalidad de atacar e interrumpir o alterar las redes de computadoras de los atacantes o posibles atacantes, defender la información militar y recolectar información de inteligencia para poder afectar al atacante enemigo.[95]

> En Estados Unidos ha reunido un grupo de hackers de élite que se estaría preparado para luchar en caso de que se desencadenase una ciberguerra. Es lo que se conoce como JFCCNW (Joint Functional Component Command for Network Warfare), una unidad que se cree que está integrada por personal de la Agencia Central de Inteligencia (CIA), la ANS, el FBI, las cuatro ramas militares, algunos civiles expertos y representantes militares de naciones aliadas, y que tiene la responsabilidad total de defender la red de computadoras del Departamento de Defensa, destruir redes, entrar en los servidores de posibles enemigos para robar o manipular información y dañar las comunicaciones rivales hasta inutilizarlas. Un comando que tiene como contraparte en el Grupo Especial de Tareas para la Libertad de la Internet Global, GIFTF (Global Internet Freedom Task Force, EN sus siglas en inglés), una organización multiagencias (7) subordinada al Departamento de Estado.[96]

[95] *Ibidem*, p. 30.
[96] Sánchez Medero, Gema, “Los Estados y la ciberguerra”, Boletín de Información (Ministerio de Defensa), núm. 317, pp. 70 y 71, disponible en *https://dialnet.unirioja.es/servlet/autor?codigo=1005925*, última fecha de consulta el 3 de junio de 2019.

Además de lo anterior, los Estados Unidos de América cuentan con el cuerpo doctrinal más avanzado que existe en el planeta con el desarrollo del mando cibernético denominado USCYBERCOM, mismo que fue creado a partir de junio del año dos mil nueve, primeramente, bajo el mando del general Keith B. Alexander, quien previo a esa encomienda fue agente de la Agencia Nacional de Seguridad (NSA por sus siglas en inglés), el cual tenía la misión de llevar a cabo las siguientes actividades:

- Dirigir las operaciones y la defensa de las redes de información específicas del Departamento de Defensa.

- Preparar y, cuando así se indique, llevar a cabo todo el espectro de las posibles operaciones militares en *ciberespacio*, con el objetivo de facilitar las acciones en todos los ámbitos.

- Garantizar libertad de acción de Estados Unidos y sus aliados en el *ciberespacio*, y negar la misma a sus adversarios.[97]

Ahora bien el presupuesto que se destina para los ciberejércitos es incierto aunque se puede encontrar información que da datos aproximados como 7,000 mil millones de dólares aproximadamente.[98]

La inversión que se destina en las fuerzas armadas evidentemente es distinta en cada uno de los Estados y por ello es importante cuestionar cómo se encuentra este rubro en nuestro Estado.

---

[97] Pastor Acosta, Oscar, "Capacidades para la defensa en el *ciberespacio*", en *El ciberespacio. Nuevo escenario de confrontación*, *op. cit*., nota 13, p. 240.

[98] Botero, Juan David, Ciberejercito alemán: 5 cosas que deberías saber", en Enter.co, disponible en *https://www.enter.co/chips-bits/seguridad/ciberejercito-aleman-5-cosas-que-deberias-saber/*, última fecha de consulta el 5 de junio de 2019.

No se abundará mucho en el análisis del ciberejercito de los Estados Unidos de América, ya que se utilizará en el siguiente capítulo como base para el análisis de los elementos que el Estado mexicano debe de considerar para poder hacer frente a los posibles ataques en el *ciberespacio* en contra de sus infraestructuras críticas, *ciberdefensa*, y la materia importante del presente estudio, la ofensiva militar.

# Capítulo 3

# Consideraciones para la creación y funcionamiento de un ciberejército en México

# Capítulo 3 Consideraciones para la creación y funcionamiento de un ciberejército en México

En México, la Secretaría de la Defensa Nacional, SEDENA por sus siglas, es la encargada de velar por la seguridad de la nación Mexicana. La Ley Orgánica del Ejército y Fuerza Aérea Mexicanos señala expresamente en su artículo primero que el ejército y fuerza aérea tienen dentro de sus misiones "I. Defender la integridad, la independencia y la soberanía de la nación […]".

Como parte de su visión para el año 2030 la SEDENA señala:

> Contar con una Fuerza Armada polivalente, ligera, flexible, de gran movilidad táctica y estratégica, con capacidad de respuesta, sólida moral, espíritu de cuerpo, principios disciplinarios y arraigada vocación de servicio, dotada de recursos humanos, tecnológicos e informáticos de calidad, acordes a la potencialidad del país, que pueda hacer frente en diversos ambientes, a amenazas externas e internas, que pongan en riesgo la consecución y/o mantenimiento de los objetivos nacionales.[99]

Observemos que en estos momentos se gesta la formación de recursos tanto humanos, así como la obtención de herramientas tecnológicas para la conformación de un cuerpo de élite que pueda hacer frente a los riesgos en el *ciberespacio*. Razón por la cual trabajos de investigación como el que se presenta, pretende abonar en el tema.

Desde hace algunos años, se han hecho evidentes en la prensa escrita, las situaciones de vulnerabilidad de las infraestructuras críticas y la ciberseguridad en México, principalmente se pueden leer notas que hacen referencia a vulneraciones en instalaciones de PEMEX y las instituciones bancarias principalmente; por ello se anunció la creación de un Centro de Operaciones del *Ciberespacio* que empezaría sus funciones el año pasado, en 2018.

> El gobierno mexicano comenzó la construcción de un Centro de Operaciones del *Ciberespacio*, el cual, tiene el objetivo de enfrentar las

[99] Secretaría de la Defensa Nacional, ¿qué hacemos?, Gobierno de México, disponible en *https://www.gob.mx/sedena/que-hacemos*, última fecha de consulta el 8 de julio de 2019.

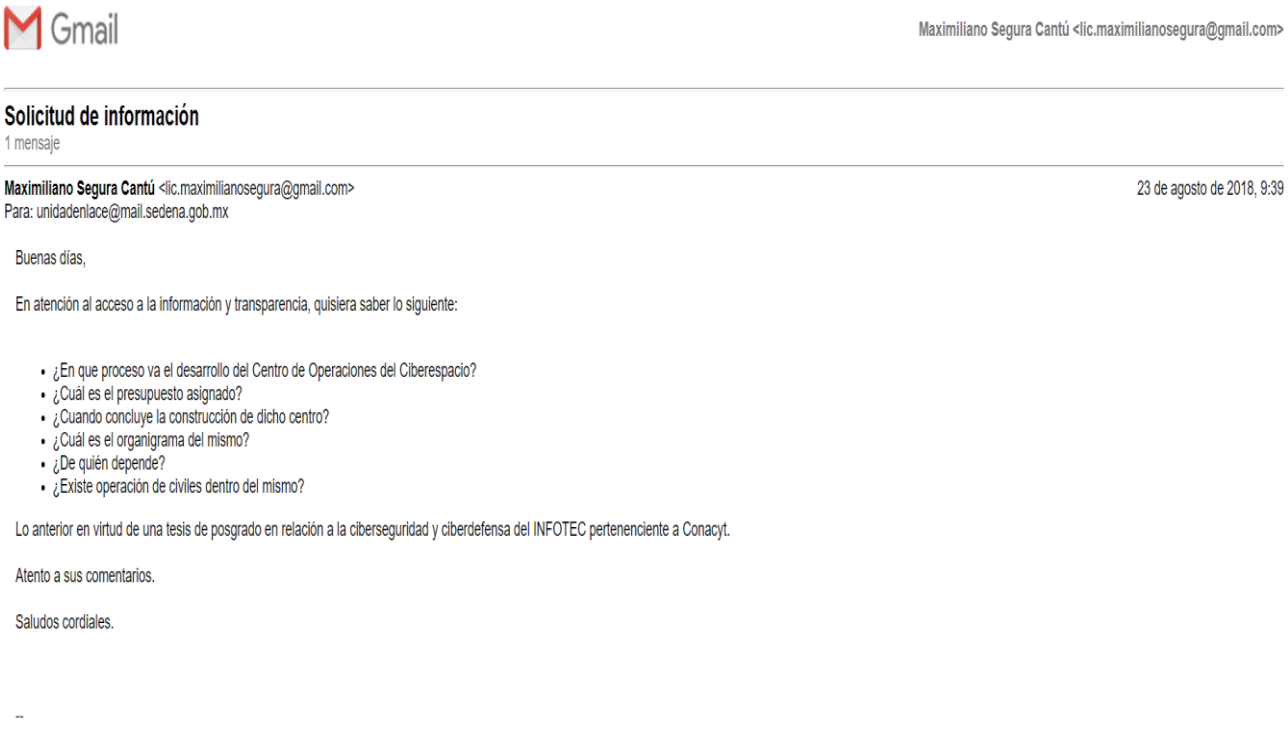
> amenazas a la seguridad nacional en internet, desde ataques en las redes sociales o hackeos a instituciones críticas, como el Banco de México, Pemex o aeropuertos, hasta la posibilidad de una ciberguerra con otro país.
>
> La versión pública del proyecto, […] identificada con la clave de inversión 15071100018 ante la Secretaría de Hacienda y Crédito Público (SHCP), revela que la construcción del nuevo órgano de *ciberdefensa* militar […] estará listo en 2018; su inversión será de mil 625 millones 821 mil pesos.[100]

Se puede observar que mientras el presupuesto que el gobierno de los Estados Unidos destina para la confirmación y perfeccionamiento de su ciberejército es de 7 mil millones de dólares según se pudo investigar, en nuestro país solo se designa el 11.98 por ciento de esa cifra para iniciar con los elementos necesarios para la creación de esta área de las fuerzas armadas. Una desventaja aparente a todas luces pues la inversión que se debe realizar va desde la infraestructura necesaria como el personal capacitado que integrará esta área de especialidad.

Durante esta investigación se realizó una solicitud de acceso a la información en fecha veintitrés de agosto del año 2018, para verificar el estatus en el que se encuentra el Centro de Operaciones del *Ciberespacio* sin tener respuesta de ningún tipo, cabe resaltar que dichas solicitudes lamentablemente no se contestan bajo el argumento de ser información de seguridad nacional, a continuación se agrega la solicitud:

[100] 24 HORAS, “México se arma contra ciberataques”, *Vanguardia.mx*, Nacional, 20 de enero de 2016, disponible en *https://vanguardia.com.mx/articulo/mexico-se-arma-contra-ciberataques*, última fecha de consulta el 8 de julio de 2019.

Figura 2. Correo electrónico solicitando información específica a la Unidad de enlace de la SEDENA



Gmail

Maximiliano Segura Cantú <lic.maximilianosegura@gmail.com>

**Solicitud de información**

1 mensaje

**Maximiliano Segura Cantú** <lic.maximilianosegura@gmail.com> 23 de agosto de 2018, 9:39
Para: unidadenlace@mail.sedena.gob.mx

Buenas días,

En atención al acceso a la información y transparencia, quisiera saber lo siguiente:

- ¿En que proceso va el desarrollo del Centro de Operaciones del Ciberespacio?
- ¿Cuál es el presupuesto asignado?
- ¿Cuando concluye la construcción de dicho centro?
- ¿Cuál es el organigrama del mismo?
- ¿De quién depende?
- ¿Existe operación de civiles dentro del mismo?

Lo anterior en virtud de una tesis de posgrado en relación a la ciberseguridad y ciberdefensa del INFOTEC pertenenciente a Conacyt.

Atento a sus comentarios.

Saludos cordiales.

--

Fuente: Imagen obtenida en captura de pantalla del correo electrónico del autor de la presente investigación

## 3.1 Estrategia Digital Nacional de Ciberseguridad

El experto en ciberseguridad, José Luis Calderón, opina que es necesaria la construcción de una cultura de la protección de las infraestructuras críticas en el país y que exista una instancia que desarrolle y lleve a la práctica políticas y regulación en la materia.

> En México, las infraestructuras críticas son propiedad, en gran medida, del Estado. Se habla de más de 3.000 instalaciones catalogadas como críticas o estratégicas para el país. Al ser la mayoría propiedad del Estado, su vigilancia y protección deberían ser estrictamente responsabilidad del Consejo de Seguridad Nacional y de sus instituciones –Secretaría de Marina, Secretaría de la Defensa Nacional, Centro de Investigación y Seguridad Nacional (CISEN) y Policía Federal–. Y también por las organizaciones propietarias, quienes, a través de normas como la Ley de Seguridad Nacional o la Ley General del Sistema Nacional de Seguridad Pública, están facultadas para ello [como el] Grupo de Coordinación de Instalaciones Estratégicas (GCIE), ubicado en la División de Inteligencia y, por lo tanto, dependiente de la Policía Federal y la Secretaría de Gobernación.

> Teóricamente, el grupo está dirigido por el titular de la División e integrado por funcionarios de distintos organismos relacionados con la seguridad pública, la seguridad nacional, la procuración de justicia, la inteligencia civil y las organizaciones del Estado que gestionan instalaciones críticas: la Secretaría de Comunicaciones y Transportes, la Comisión Nacional del Agua, Petróleos Mexicanos y la citada CFE.
>
> […] Por lo general, el GCIE realiza labores enfocadas a la prevención de ilícitos, en gran medida a través del uso de la inteligencia. Sin embargo, ha sido un grupo con nulo liderazgo que no ha sabido permear una visión de Estado. Y, además, carece de medios coercitivos para regular y/o establecer políticas y estrategias adecuadas en materia de prevención, profesionalización, resiliencia y las mejores prácticas para la vigilancia y la protección.[101]

Se consultó el documento denominado Estrategia Nacional de Ciberseguridad del año 2017, en el cual se resalta la relevancia de las tecnologías tanto en la vida pública como privada de las personas que cada vez más se conectan y hacen uso de la Internet.

Sin embargo, debido a un incremento en el número de usuarios de Internet, también se han incrementado el número de delitos perpetrados haciendo uso de los medios tecnológicos. El incremento ha sido tal, no solo en México, sino al rededor del mundo que por ello se evidenció la relevancia de la estrategia antes mencionada.

Como objetivo general de la estatefia mencionada es “identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano”,[102] para la consecución de este objetivo se incluyen 5 objetivos estratégicos, de los cuales para efectos del trabajo que se presenta solo interesa el marcado con el número 5 que es la seguridad nacional: “1.

---

[101] Calderón, José Luis, *Infraestructura crítica en México: el enfoque hacia el futuro, en Segurilatam,* disponible en *http://www.segurilatam.com/seguridad-aplicada/infraestructuras-estrategicas/infraestructura-critica-en-mexico-el-enfoque-hacia-el-futuro*, última fecha de consulta el 8 de julio de 2019.
[102] Gobierno de México, *op. cit*., nota 39, p. 4.

Sociedad y derechos. 2. Economía e innovación. 3. Instituciones públicas. 4. Seguridad pública. 5. Seguridad nacional".[103]

Siendo el contenido del objetivo de seguridad nacional "Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional afectando el desarrollo y los intereses nacionales".[104]

Asimismo, para alcanzar estos objetivos estratégicos se consideraron 8 ejes transversales a saber:

1. Cultura de ciberseguridad.
2. Desarrollo de capacidades.
3. Coordinación y colaboración.
4. Investigación, desarrollo e innovación TIC.
5. Estándares y criterios técnicos.
6. Infraestructuras críticas.
7. Marco jurídico y autorregulación.
8. Medición y seguimiento.[105]

En el mismo documento se advierte que la encargada de coordinar, implementar y dar seguimiento a la estrategia es la Subcomisión de Ciberseguridad dependiente de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.

Esta estrategia, cuyo fundamento se encontraba en el Plan Nacional de Desarrollo de la anterior administración, dejaba de manifiesto datos relevantes sobre la situación de la ciberseguridad tanto en México como a nivel mundial en donde se informaba que los ciberataques se incrementaron en un 30 por ciento y representaron pérdidas económicas por 110,000 millones de dólares según datos

---

[103] *Idem*.
[104] Gobierno de México, *op. cit*., nota 39, p. 4.
[105] Calderón, José Luis, *Infraestructura crítica en México: el enfoque hacia el futuro, op. cit*., nota 101.

de la Unión Internacional de las Telecomunicaciones,[106] cifra que significó para México un aproximado de 3,000 millones de dólares según datos de la Organización de Estados Americanos.[107]

> La Policía Federal [hoy extinta], a través de la División Científica, impulsó una Estrategia de Ciberseguridad para fortalecer, entre otros, la concientización social sobre el uso responsable de las TIC. Además el número de incidentes cibernéticos identificados, se ha triplicado de 2013 a 2016, pasando de cerca de 20 mil incidentes a más de 60 mil; mientras que la presencia de sitios web apócrifos con fines de fraude, se incrementó un 11 por ciento entre 2015 y 2016, llegando a cerca de 5 mil; la propagación de virus informáticos con afectaciones en México creció un 57 por ciento de 2015 a 2016, llegando a cerca de 40 mil eventos, destaca el grado de sofisticación utilizado por los ciberdelincuentes en algunos de los casos.[108]

De acuerdo al Índice Mundial de Ciberseguridad y perfiles de ciberbienestar de la Unión Internacional de Telecomunicaciones, México a pesar de contar con una regulación específica respecto a los cibercrímenes en su Código Penal Federal, contar con un Centro Nacional de Respuesta a Incidentes Cibernéticos de la hoy extinta Policía Federal (CERT-MX por sus siglas) y reconocer la certificación de la norma ISO 270001 para la gestión de la seguridad de la información en todas las instituciones gubernamentales, aún no cuenta con un marco de ciberseguridad para la certificación y acreditación de las dependencias ni públicas ni privadas, ni tiene una hoja de ruta de gobernanza nacional para la ciberseguirdad y por ende mucho menos ha establecido, lo que se conoce como benchmarking, o mecanismos para evaluar y comparar los trabajo en la materia.[109]

En ese mismo índice de la UIT también se explica que no se cuenta con desarrollo de proyectos o programas de investigación y desarrollo en materia de estándares de ciberseguridad, mejores prácticas o directrices. Y se mencionan algunos intentos de cursos y conferencias que se han impartido tanto por instituciones gubernamentales como de instituciones educativas, pero a pesar de

---

[106] *Idem*.
[107] *Idem*.
[108] *Ibidem*, p. 6.
[109] El informe se puede consultar en *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf*, última fecha de consulta el 8 de julio de 2019.

estos esfuerzos México sigue sin contar con personal certificado en temas de ciberseguridad.[110]

También se deja al descubierto con los datos presentados por la UIT que nuestro país no se está apoyando de la cooperación con otros Estados para hacer frente a este fenómeno y que parece pretender hacer frente a los problemas de ciberseguridad de manera unilateral en un mundo interconectado.[111]

México debe de tener en cuenta que el tema se inserta en un contexto global y por ello debe potencializar sus esfuerzos con otros Estados para prevenir los ataques a sistemas centrales como los servidores DNS o la infraestructura crítica, y aprovechar más su membresía en los Foros a los que pertenece como el caso del Foro de Respuesta a Incidentes y Equipos de Seguridad que data de 1989.

También es de rescatar que el Estado Mexicano debiera muestra más actividad en el Comité Interamericano contra el Terrorismo, específicamente en el Programa de Cibereseguridad promoviendo iniciativas de investigación y fortalecimiento de sus capacidades técnicas y políticas de ciberseguridad.

Precisamente en la página del Programa en comento se destacan los siguiente tres pilares: Desarrollo de políticas, Desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos) e Investigación y divulgación de los que México debería tomar parte activa.

> - Desarrollo de políticas: el programa ayuda a los Estados miembros de la OEA a desarrollar estrategias nacionales o regionales de ciberseguridad que involucren a todas las partes interesadas relevantes y que se ajusten a la situación legislativa, cultural, económica y estructural de cada país y apoyen las evaluaciones a nivel nacional sobre la capacidad y la madurez de la ciberseguridad. Bajo esta vía, el programa apoya el desarrollo de medidas de fomento de la confianza en el *ciberespacio*.
>
> - Creación de capacidad: El programa ayuda a establecer y desarrollar la capacidad de los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT) existentes y brinda asistencia técnica personalizada y oportunidades de ejercicio para

[110] *Idem*.
[111] *Idem*.

fortalecer las instituciones y organizaciones nacionales y regionales. El desarrollo de una fuerza laboral de ciberseguridad también se lleva a cabo a través de diversas formas de oportunidades de desarrollo profesional.

- Investigación y divulgación: El programa desarrolla documentos técnicos, conjuntos de herramientas e informes basados en investigaciones para guiar a los responsables de políticas, CSIRT, operadores de infraestructura, organizaciones privadas y la sociedad civil, destacando los desarrollos actuales e identificando los problemas y desafíos clave de seguridad cibernética en la región.[112]

El Plan Nacional de Desarrollo 2019-2024, anuncia que se deberá repensar la seguridad nacional y reorientar a las fuerzas armadas, y que estos institutos armados seguirán aportando a las diversas esferas del quehacer nacional: la aeronáutica, informática, industria, ingeniería, entre otras.[113]

Infortunadamente y tras al menos cuatro años de intentar fortalecer la ciberseguridad en México, incluso con una oficina de "Estrategia Digital Nacional" pocos parecen ser los avances en la materia. Ya el año pasado, 2018, quien fuera director jurídico de dicha oficina Ernesto Ibarra Sánchez, señaló que el proceso de implementación de la Estrategia Nacional de Ciberseguridad, "será una serie de recomendaciones de mediano y largo plazo para el gobierno del próximo presidente Andrés Manuel López Obrador, entre las que se encuentran el que la cibersguridad es un tema del más alto nivel".[114]

Entender la ciberseguridad como una estrategia de recomendaciones para un mandatario en turno es no entender el riesgo que enfrentan las infraestructuras críticas de México en un mundo globalizado. ¿Qué resultados se obtuvieron de los más de mil 625 millones de pesos invertidos en la implementación de una

---

[112] OEA, Programa de Ciberseguridad, disponible en *http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp*, última fecha de consulta el 8 de julio de 2019.

[113] El Plan Nacional de Desarrollo 2019-2024 se puede consultar en línea.

[114] Riquelme, Rodrigo, Estrategia Nacional de Ciberseguridad queda en recomendaciones para gobierno de AMLO", El Economista 29 de agosto 2018, disponible en *https://www.eleconomista.com.mx/empresas/Estrategia-Nacional-de-Ciberseguridad-queda-en-recomendaciones-para-gobierno-de-AMLO-20180829-0035.html*, última fecha de consulta el 8 de julio de 2018.

"Estrategia Nacional de Ciberseguridad"?, "la ausencia de un coordinador o de una Agencia Nacional de Ciberseguridad dentro de la estrategia se debe principalmente a dos motivos: la decisión de todas las entidades y sectores consultados para la elaboración del documento y el tiempo en el que fue presentado, al finalizar el Quinto año de la administración [de Enrique Peña], cuando ya no es momento de generar políticas públicas", opinó Víctor Lagunes, jefe de la Unidad de Innovación y Estrategia Tecnológica de Presidencia de la República de la anterior administración.[115]

Al momento no existen documentos públicos que puedan accederse para poder evaluar la ciberseguridad y las acciones del ciberejercto mexicano a dos años de su creación.

Ernesto Ibarra comentó que:

> […] se han realizado algunas acciones contenidas en la Estrategia, como la campaña de comunicación digital sobre ciberseguridad que se encuentra en el sitio Gob.mx/ciberseguridad y un mapeo de las escuelas y universidades que imparten programas de ciberseguridad en sus planes de estudio. También se ha comenzado con la transferencia de conocimiento entre la Unidad de Inteligencia Cibernética federal y las unidades de los estados y se ha estado trabajando en un índice de ciberseguridad que atienda a la realidad de las circunstancias del país.[116]

Finalmente en la referida página citada por el ex director de la Estrategia Digital Nacional se observan Blogs respecto a la colaboración de la Policía Federal y Gran Bretaña para combatir el cibercrimen de fecha 11 de julio de 2016, el curso de la IBERPOL a la Policía Federal del 7 de septiembre de 2016, la Segunda Semana Nacional de Ciberseguridad, del 30 de noviembre de 2016, la nota de que la Policía Federal impulsa la campaña de Ciberseguridad México 2017, de fecha 17 de marzo de 2017, y dos notas más.

---

[115] Riquelme, Rodrigo, "Estrategia Nacional de Ciberseguridad, marcada por fin de sexenio", *El Economista*, 5 de diciembre de 2017. Disponible en *https://www.eleconomista.com.mx/politica/Estrategia-Nacional-de-Ciberseguridad-marcada-por-fin-de-sexenio-20171205-0041.html*, última fecha de consulta el 8 de julio de 2019.

[116] Riquelme, Rodrigo, Estrategia Nacional de Ciberseguridad, *op. cit*., nota 106.

Si se navega por esta página se observará que no cuenta con mayor contenido.

Ante esta situación ha sido complicado conseguir más información respecto a la conformación de un ciberejército en México, tras analizar distintos elementos de los ciberejercitos de diversos Estados en la práctica en el capítulo anterior podemos identificar algunos elementos básicos, por ejemplo:

1. Los ciberejercitos se implementan más como un medio de *ciberdefensa* que como una estrategia para enfrentar a alguna potencia extranjera.
2. Es necesario que los Estados tengan un adecuado control de las amenazas y crímenes que se comenten en el *ciberespacio*, especialmente todos aquellos que tienden al ciberespionaje.
3. La protección de las infraestructuras consideradas como estratégicas o críticas son prioridad en el diseño de las estrategias de protección encargadas a la ciberseguridad.
4. En cuanto a los sistemas de Tecnologías de la Información y Comunicación tanto los ciudadanos como las empresas deben de estar conscientes de los riesgos en el uso de estos sistemas y deben implementar medidas de seguridad donde hagan uso del ciberespcacio.
5. El papel de la administración pública es fundamental ya que también es necesario que se refuercen las medidas de seguridad en sus sistemas de Tecnologías de la Información y Comunicación. En este aspecto las oficinas de gobierno de las administraciones tanto locales como centrales deben de ser apropiadas y en conjunto facilitar la implementación de inversiones estratégicas en materia de seguridad.
6. La creación de oficinas especializadas en temas de ciberseguridad serán también aspecto clave en el desarrollo de una adecuada política de ciberseguridad y *ciberdefensa*, tanto una Oficina Nacional que se encargue de dar respuesta a los posibles ataques y vulnerabilidades como organismos especializados en el diseño de políticas nacionales de ciberseguridad.
7. La cooperación internacional en estos temas es sin lugar a dudas un factor clave tanto para la adquisición de tecnologías, la capacitación de personal,

así como para la contención de peligros que puedan hacerse frente de manera conjunta y la ayuda mutua.[117]

Otros de los elementos necesarios que se vieron tras el análisis de las estrategias de *ciberdefensa* y ciberestrategias de los diversos Estados del capítulo anterior, que es preciso rescatar son aquellos respecto de la capacitación de personal especializado en la materia y la inversión de los Estados en el desarrollo de tecnología desde el interior, esto quiere decir que los Estados desarrollen su propio software y hardware para evitar dependencias de tecnologías desarrolladas por otros en el mejor de los casos, ya que en el peor de los casos de puede caer en la obtención de tecnología hardware y software de manufactura extranjera que puede traer consigo elementos de espionaje o puertas traseras que generan inteligencia para Estados productores.

Hay que destacar que México cuenta con el Centro de Estudios Superiores Navales, en donde se imparten Maestrías desde un punto de vista técnico, capacitando al personal militar e invitados de la administración pública federal, así como invitados de otros países en concordancia con México, respecto de posgrados de los que destacan la Maestría y Doctorado en Seguridad Nacional, en donde se imparte la materia de "poder nacional" matería que destaca de acuerdo a lo que plantea en este estudio, lamentablemente, tal como se expuso en páginas anteriores, no se tiene mucha información al respecto ni por petición vía transparencia ni por medio de su portal web,[118] puesto que habla de ejercicios de alumnados en línea de generaciones 2016-2017 y estudios llevados en línea de generaciones del 2016-2018.

También, es importante mencionar que dentro de las habilidades con las que cuenta este posgrado, no se hace mención al área del "ciberespacio" como

---

[117] Véase UNISA, Europa, "Ciber Security Strategy for Germany", *op. cit*., nota 68, pp. 3-7.

[118] Centro de Estudios Superiores Navales, Maestría en Seguridad Nacional, plan de estudios, disponible en *https://cesnav.uninav.edu.mx/cesnav/links_acc_progr/segnac_site/plan_estudios.html*, consultado el 14 de diciembre del 2019.

escenario de conflicto, ya que solo menciona de manera textual en la información del portal las unidades de superficie, terrestres, áereas y aeronavales, dejando de lado el tema que nos ocupa en la presente investigación.

De igual forma, imparten la Maestría en "Seguridad de la Información" de donde se desprende de su portal web,[119] dentro del apartado "áreas de investigación" la doctrina de la Guerra de Información, destacando, las capacidades de los perfiles de egreso en temas tales como "elementos de seguridad ofensiva", "analiza el funcionamiento y explotación de las redes informáticas y equipos periféricos", sin embargo, dentro de su apartado de "habilidades y destrezas" no se encuentra información que tenga relación con ejercicios ofensivos utilizando las Tecnologías de la Información y Comunicación como área estratégica, insistiendo el desconocimiento real de los alcances de dichos posgrados, ya que como se mencionó en párrafos anteriores, no se cuenta con mucha información al respecto en virtud de la secrecía que guardan las instituciones de defensa de este país.

También la Secreataría de Marina, desde 2017, cuenta con una Unidad de Ciberseguridad (UNICIBER), que se creó con la finalidad de "planear, coducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa, para la protección de la infraestructura crítica de las Secretaraía de Marina. Armada de México y coaduvar en el esfuerzo Nacional en el mantenimiento de la integridad, estabilidad y permanencia del Estado Mexicano".[120]

Ahora bien, hay que destacar que México cuenta con instrumentos jurídicos que hacen alusión a la salvaguarda de la nación tanto para temas internos (Ley de Seguridad Interior), así como para temas de la protección de la soberanía nacional (Ley de Seguridad Nacional), en donde en ésta última dentro del artículo 3, fracción I, III, V y VI, mencionan las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que tienen

---

[119] *Idem*.

[120] García, Mariano y Quevedo, José Antonio, "México implementa una estratgia de seguridad cibernética junto a España y Francia", Infodefensa.com, 12 de octubre de 2017, disponible en *https://www.infodefensa.com/latam/2017/10/12/noticia-unidad-ciberseguridad-semar.html*, última fecha de consulta el 23 de diciembre de 2019.

que ver con el tema que nos ocupa, mencionando también, dentro de su artículo 5, el catálogo de las acciones que serán catalogadas como amenazas a la Seguridad Nacional, de las que destacan las siguientes fracciones: I.- Actos tendientes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; II.- Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano; XI.- Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia; y XII.- actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, mismos que tienen relevancia con el presente estudio.

Dentro de la propia Legislación, se establece la conformación de un Consejo de Seguridad Nacional el cual estará conformado por el titular del Ejecutivo Federal, quien presidirá dicho consejo; el secretario de gobernación, quien fungirá como Secretario Ejecutivo; el Secretario de la Defensa Nacional; el Secretario de Marina; el Secretario de Seguridad Pública; el Secretario de Hacienda y Crédito Público; el Secretario de la Función Pública; el Secretario de Relaciones Exteriores; el Secretario de Comunicaciones y Transportes; el Procurador General de la República; y el Director del Centro de Investigación y Seguridad Nacional.

En esta legislación se facultan las atribuciones del Centro de Investigación Nacional y Seguridad Nacional, el cual fue extinto por el ahora presidente de la república Andrés Manuel López Obrador, por lo que ahora se le conoce como el Centro Nacional de Inteligencia (CNI), a quien se le designó el presupuesto de 2.6 mil millones de pesos, de donde se destaca, que dentro de sus atribuciones de conocimiento, lo cual se lee en el artículo 19 de la Ley de Seguridad Nacional, en su fracción V: “proponer medidas de prevención, disuasión, contención y desactivación de riesgos y amenazas que pretendan vulnerar el territorio, la soberanía, las instituciones nacionales, la gobernabilidad democrática o el Estado de Derecho”, sin embargo, se ve necesario el integrar dentro de dichas facultades la de operaciones ofensivas y combate, las cuales son las que se proponen dentro del presente estudio de tesis.

### 3.2 Estándares del *ciberejército* norteamericano y otros *ciberejércitos* ¿ejemplos para México?

Es por lo dicho en el capítulo anterior, y en virtud de que nuestro Estado vecino del Norte cuenta con la mayor inversión en tecnología de alta gama que puede generar no solo el soporte respecto a la ciberseguridad y *ciberdefensa*, sino que resulta necesario que el ciberejercito mexicano se apegue a las buenas prácticas internacionales de la ofensiva, puesto que no puede haber un ejército exitoso que solo resista el ataque a su soberanía, en este caso de la cibersoberanía, por lo que resulta necesario resaltar los siguientes aspectos importantes como consideraciones esenciales para la creación de una fuerza elite Mexicana, por lo que procederemos al análisis del ciberejercito estadounidense, el cual se detalla en palabras de Oscar Pastor Acosta a continuación y que debido a la relevancia de las aportaciones se transcribe a continuación:

> … el USCYBERCOM se compondrá de las ciberunidades de los diferentes servicios que componente las Fuerzas Armadas Estadounidenses, en concreto:
>
> 1. Cibermando del Ejercito (ARCYBER): aportando la componente cibernética del ejército en tierra, denominada Segundo ejército, incluirá las siguientes unidades subordinadas:
>
> - IX Mando de señales del Ejercito, o el Mando de Tecnología Global de Red del Ejercito (NETCOM)
> - I Mando de Operaciones de información (del componente terrestre).
> - Mando de Inteligencia y Seguridad del Ejercito, que estará bajo el control operacional del cibermando del Ejercito para las acciones en el *ciberespacio*.
>
> 2. Cibermando de la fuerza Aérea (AFCYBER): aportando la componente cibernética del Ejercito del Aire, denominada XXIV Fuerza Aérea, Incluirá las siguiente unidades subordinadas:
>
> - Ala 67 de Guerra de Red.
> - Ala 688 de Operaciones de Información.
>
> 3. Ala 689 de Comunicaciones de Combate. Cibermando de la Flota (FLTCYBERCOM): aprontando la componente cibernética de la Armada denominada X Flota. Incluida entre otras las siguientes unidades subordinadas
>
> Mando Naval de Guerra en Red.
>
> Mando Naval de Operaciones de *Ciberdefensa*.
>
> Mando Naval de Operaciones de la Información.

4. Cibermando de la Infantería de Marina (MARFORCYBER): apurando un componente cibernética de la Infantería de Marina:

> Por otro lado, desde hace tiempo se viene revisando la Doctrina Militar estadounidense, en sus deferentes componentes, para adecuarla a los nuevos retos que suponen las operaciones militares en el ciberespacio, intentando definir las capacidades que deberán prepararse para afrontarlas.
>
> Así, el Ejército de Estados Unidos establece, en su Plan de Capacidad de los años 2016-2028 para concepto de Operaciones en el Ciberespacio (CyberOps), que estas se componen de: comprensión de la Cibersituación (CyberSA), Operaciones de la Red Cibernética (CyNetOps), Ciberguerra (CyberWar) y, finalmente, Soporte Cibernético (CyberSpt).

5. Comprensión de la cibersituación: se compondría del conocimiento inmediato, tanto del adversario como del aliado, así como de toda la información pertinente sobre las actividades en el ciberespacio o en el espectro electromagnético. Se obtiene a partir de la combinación de actividades de inteligencia y operativas en el ciberespacio así como en el resto de dominios, llevadas a cabo tanto de manera unilateral como a través de la colaboración con socios de los sectores público o privado. La discriminación entre las amenazas naturales y artificiales es una pieza clave de este análisis.

> Una apropiada comprensión de la cibersituación permitirá la toma de decisiones adecuadas, en todos los niveles de decisión, a través de productos a medida de cada audiencia, que pueden ir desde los boletines de sensibilización con una amplia difusión dirigida a los usuarios en general, hasta informes de cuestiones específicas, extremadamente sensibles y de naturaleza clasificada. Una Buena comprensión de la cibersituación debe incluir también las capacidades para:
>
> - La comprensión del adversario y del aliado, así como de las actividades relevantes en el *ciberespacio*.
> - La evaluación de las capacidades cibernéticas amigas.
> - La evaluación de las capacidades cibernéticas e intenciones del adversario.
> - El análisis de las vulnerabilidades cibernéticas del adversario y del aliado.
> - La comprensión de la información que fluye a través de las redes para deducir su propósito y su criticidad.
> - La comprensión de los efectos y el impacto en la misión, resultante de las degradaciones en el *ciberespacio* amigo y también adversario.

6. CyberWar: es el componente de las CyberOps que extiende el poder cibernético más allá de los límites de la Defensa del ámbito cibernético propio, para detector, detener, denegar, y derrotar a los adversarios, Las capacidades de la cyberWar tienen como objetivo las redes de telecomunicaciones y los ordenadores, así como los procesadores y controladores integrados en equipos, sistemas e infraestructuras

La CyberWar incluirá acciones de ataque en las que se combinarán ataques a redes informáticas, con otras capacidades de apoyo, (por ejemplo, ataque electrónico, o ataque físico) para negar o manipular la información o la infraestructura

En la CyberWar, se combinarán medios políticos, de inteligencia, sensores y procesos, altamente automatizados para identificar y analizar la actividad maliciosa, al tiempo que se ejecutarán acciones de respuesta con autorización previa para eliminar ataques hostiles antes de que pueda causar impacto. Además, se usarán principios tradicionales de seguridad de los ejércitos como la defensa en profundidad. Se incluirá la vigilancia y el reconocimiento para emitir alertas tempranas de las acciones enemigas.

En un desglose detallado de las capacidades para la CyberWar se incluirán también:

- Acceder, tanto por medio directos como a distancia, a redes, Sistema con nodos marcados como objetivos, con el fin de garantizar el acceso que requieren las acciones de la CyberWar contra objetivos fugaces.
- Permitir el acceso recurrente, tanto por medios directos como a distancia a redes, sistemas o nodos marcados como objetivos, para garantizar el acceso requerido para las CyberOps.
- Acceder al hardware y software del adversario, por medios directos o a distancia, con el fin de garantizar la información del adversario, con el fin de garantizar las acciones de la CyberWar.
- Acceder a recopilar y explotar la información del adversario marcada como objetivo, por medios directos o a distancia, con el fin de detector, disuadir, denegar y derrotar a las acciones y la libertad de acción del adversario.
- Habilitar la capacidad de agregar, administrar, descifrar, traducir lingüísticamente, analizar e informar sobre todos los datos recogidos en los sistemas de gestión, del conocimiento, con el fin de apoyar las CyberOps y a los mandos críticos de batalla.
- Proporcionar capacidades de CyberWar, tanto a distancia como de forma expedicionaria, con el fin de detectar, disuadir, denegar y derrotar a las acciones y la libertad de acción con el adversario.
- Proporcionar capacidades, basadas en sensores para la detección automatizada de ataques de red y de intrusiones con el fin de detectar, disuadir, denegar y derrotar a las acciones del adversario, integrar la defensa a profundidad, garantizar la libertad de acción propia y de los aliados, así como negar la libertad de acción del adversario en el momento y lugar de nuestra elección.
- Atacar (negar, degradar, interrumpir, engañar, o destruir) las redes del adversario y su infraestructura crítica con el fin de detectar, disuadir, denegar y derrotar las acciones y la libertad de acción del adversario.
- Proporcionar capacidades, basadas en sensores, de respuesta a la intrusión o el ataque a la red, con el fin de detector, disuadir, denegar y derrotar las acciones del adversario, integrando la defensa en profundidad y garantizando la libertad de acción amistosa, así como

negando la libertad de acción del adversario, en el memento y el lugar de nuestra elección.
- Atacar las redes del adversario con el fin de con el fin de detectar, disuadir, denegar y derrotar sus acciones y su libertad de acción.
- Atacar (negar, degradar, interrumpir, engañar o destruir) los procesadores y controladores integrados en los equipos y sistemas del adversario, con el fin de detectar, disuadir, denegar y derrotar sus acciones, integrando la defensa en profundidad y garantizando la libertad de acción propia y aliada, así como negando la libertad de acción del adversario en el momento y el lugar de nuestra elección.
- Proporcionar conocimiento de la situación del adversario y de otras redes específicas, con el fin de aumentar el conocimiento general de las situación del comandando, permitiendo las cyberOps, así como las acciones integradas del comandante.
- Mapear y entender al adversario y otras estructuras específicas de la red, fin de garantizar todos los aspectos de las CyberOps.
- Rastrear, localizar, predecir las actividades del adversario en el ciberespacio, a fin de garantizar nuestras acciones de CyberWar y del conocimiento de la cibersituación.
- Atacar la información del adversario con el fin de disuadir, socavar o engañar a los adversarios, apoyando los objetivos generales del comandante de la misión.
- Mitigar o evitar las medidas de ciberdefensa del adversario, con el fin de ejecutar las capacidades propias de la CyberWar.
- Impactar en la infraestructura cibernética del adversario, con el fin de apoyar la efectividad de las acciones en el ciberespacio, así como los objetivos generales del comandante de la misión.[121]

De lo anterior, vemos tal como lo describe el autor mencionado, la necesidad de generar este tipo de capacidades tácticas apegadas a la realidad mexicana de un grupo de elite a efectos de que la soberanía nacional no se vea mermada por siempre tener el carácter de pasivos ante los ejercicios bélicos diarios de los cuales como nación somos víctimas, situación que recae incluso como motivante del presente estudio, ya que se han visto claros ejemplos en donde la ofensiva juega un papel esencial como un elemento de poder ante situaciones críticas, tal como el ciberataque ordenado el jueves veinte de junio de este año por el presidente de los Estados Unidos Donald Trump ante la situación tensa con Irán.[122]

---

[121] Pastor Acosta, Oscar, "Capacidades para la defensa en el *ciberespacio*", en *El ciberespacio. Nuevo escenario de confrontación*, *op. cit*., nota 13, p. 242.

[122] Guimón, Pablo "EEUU lanzó este jueves un ciberataque a Irán autorizado por Trump, 24 de junio 2019, disponible en *https://elpais.com/internacional/2019/06/23/estados_unidos/1561302401_346950.html*, última fecha de consulta 10 de septiembre del 2019.

No podemos dejar pasar por alto, que las naciones con mayor avance en este tema, generan capital humano con base al concepto de *CyberPower*,[123] en donde no solo tiene una definición subjetiva de un poder dentro del cyber, sino, que genera una línea a seguir dentro del aprovechamiento y modus vivendi de esta era digital.

Para poder lograr lo anterior, es de suma importancia que se generen los recursos estratégicos los cuales constan de cuatro componentes esenciales, el recurso financiero, material, tecnológico y humano,[124] en donde el último de los mencionados debe de ser capacitado especialmente en las áreas de matemáticas, ciencias físicas, ciencias biológicas, ingeniería, ciencias sociales, ciencias del comportamiento, artes y humanidades, en donde las últimas de las mencionadas solo son necesarias para la preservación de la cultura y la humanidad, pero menos relevantes en comparación con las primeras de las mencionadas, las cuales son esenciales para la producción del poder nacional.[125]

Una aportación que también puede ser incluida en estas consideraciones para la creación y funcionamiento de un ciberejercito mexicano es la lección aportada por el gobierno chino en el que se incluye el entrenamiento de soldados en el tema de ciebrarmas y la simulación de ataques por medio de sistemas de información y virus informáticos.

En la actualidad existen ya concursos para jóvenes talentos en los que se convoca precisamente para que desarrollen soluciones y alternativas sobre casos hipotéticos de ataques a infraestructuras críticas.

Otra de las consideraciones que se deberían de considerar para el caso mexicano es tomado de la experiencia de la estrategia de defensa nacional del Reino Unido y que se trata específicamente de la creación de un Centro para la

---

[123] "The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power". Kramer, Franklin D, Starr, Stuart H., y Wentz, Larry K., Cyberpower and National Security, hacienda referencia a The Law of Land Warfare, p. 22

[124] Tellis, Ashley J., Bially, Janice, Layne, Christopher, McPherson, Melissa, Sollinger, Jerry M., *Measuring National Power in the Postindustrial Age*., California, Arroyo Center, Rand, 2000, p. 28.

[125] Ibidem, p. 14.

Protección de las Infraestructuras Nacionales, en particular llama nuestra atención la parte de las Sesiones Info Sec que son la elaboración de documentos de interés general en los que se investiga y pone a disposición la información que se genera sobre los riesgos que puede haber en torno a la infraestructura crítica nacional.

Finalmente no se descartan las aportaciones del especialista José Luis Calderón respecto a una institución que se encargue de entre otras funciones de:

- El desarrollo de estrategias de cooperación a nivel sectorial, nacional e internacional.
- La creación de un catálogo actualizado de infraestructuras públicas y privadas con una adecuada clasificación y un seguimiento periódico de las mismas.
- La elaboración de guías y estándares para la protección de las infraestructuras.
- La promoción del conocimiento de buenas prácticas y metodologías de protección.
- El fomento de la profesionalización de cuadros.
- El impulso de una regulación clara, moderna y acorde a la realidad del país.
- La creación de una comunidad de protección de infraestructuras que contemple un sistema de información.[126]

### 3.3 Expectativas para las fuerzas armadas en el PND 2019-2024

En el Plan Nacional de Desarrollo del actual gobierno se prevé dentro de sus estrategias articular la seguridad nacional para garantizar la integridad y la soberanía nacionales, dentro de los objetivos estratégicos se encuentra establecer un Sistema Nacional de Inteligencia, actualizar el catálogo y clasificación de instalaciones estratégicas, fortalecer y mantener la seguridad interior del país y garantizas la defensa exterior de México, mejorar las capacidades tecnológicas de

[126] Calderón, José Luis, *op. cit*., nota 94.

investigación científica en los ámbitos de seguridad pública, seguridad interior, generación de inteligencia estratégica y procuración de justicia entre otras.[127]

Es de destacar que en el repensar la seguridad nacional y reorientar a las Fuerzas Armadas se tomará en cuenta las diversas esferas del quehacer nacional dentro de lo que se encuentra la informática.[128]

Con un personal activo de 279,010 personas y un presupuesto de 127 753 millones de pesos para el año 2029 se debe de evaluar, cuántas de estas personas estarían realmente capacitados para integrar un ciberejército.

Una buena noticia para esta nueva administración es que el Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales (IMEESDN) que se inauguró el 4 de octubre de 2018, seguirá funcionando.

Este Instituto es un espacio educativo que promueve la investigación en materia de seguridad. “Sus objetivos particulares van más allá del ámbito militar, implican integrar civiles y militares en los temas de desarrollo y defensa nacional, a través de estudios de nivel doctorado, formando investigadores científicos”.[129]

Los planes de estudio se encentran “definidos por las nuevas agendas en las que se establecerá cuáles son las amenazas a la seguridad nacional, los riesgos y escenarios en el corto y largo plazos”.[130]

### 3.4 Dificultades a considerar en la implementación de las consideraciones para un ciberejército en México

---

[127] Plan Nacional de Desarrollo 2019-2024, p. 22. Disponible en *https://lopezobrador.org.mx/temas/plan-nacional-de-desarrollo-2019-2024/*, última fecha de consulta el 17 de septiembre de 2019.
[128] *Ibidem*, p. 23.
[129] Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales (IMEESDN), disponible en *https://www.gob.mx/sedena/articulos/instituto-mexicano-de-estudios-estrategicos-en-seguridad-y-defensa-nacionales-imeesdn?idiom=es*, última fecha de consulta el 17 de septiembre de 2019.
[130] Medellín, Jorge Alejandro, “El ejército mexicano pone en marcha su Instituto de Estudios Estratégicos”, Defensa.com. Actualidad, 10 de octubre de 2018. Disponible en *https://www.defensa.com/mexico/ejercito-mexicano-pone-marcha-instituto-estudios-estrategicos*, última fecha de consulta el 17 de septiembre de 2019.

Como se expuso en capítulos anteriores, la realidad muestra que los Estados deben de invertir en seguridad nacional y que los temas tecnológicos y los ataques cibernéticos a infraestructuras críticas es una actividad que se da todos los días a lo largo del mundo.

Sin embargo es relevante considerar que para poder establecer las consideraciones mínimas para el establecimiento de un ciberejército en México y poder considerar los estándares que se tienen en los Estados Unidos expuestos con anterioridad, es necesario reconocer en primer lugar que nuestro país no tiene serias limitaciones tecnologías que probablemente se requieren superar pues, desde que se adoptó un modelo de sustitución de importaciones en la primera mitad del siglo se ocasionó que se importaran las innovaciones tecnológicas más que apostar a invertir para que se desarrollara la capacidad tecnológica al interior del país, "la investigación siempre ha sido un proceso largo, costoso e incierto. Bajo estas circunstancias, a los empresarios mexicanos les pareció más razonable adquirir tecnología en el extranjero que propiciar su desarrollo en el propio país".[131]

Esta situación ha ocasionado hasta el día de hoy que las tecnologías de las que disponemos no sean las más adecuadas, que sea oneroso adquirir estas tecnologías, que las instituciones se encuentran marginadas respecto a la actividad productiva, evidentemente esto impacta el aprendizaje que se vuelve lento.[132]

La historia ha demostrado que las demandas y presiones generadas por la ampliación del mercado interno y el proceso incipiente de industrialización ha provocado el surgimiento de escuelas como el Instituto Politécnico Nacional que fue una respuesta efectiva en su época para la demanda de técnicos de alto nivel.[133]

---

[131] Álvarez, Norma L., *et. al*., Tecnología e Industria en el futuro México, posibles vinculaciones estratégicas, Capítulo V, El Problema Tecnológico de México. Rezago Tecnológico e Industrialización Sustitutiva, Centro de Investigación para el Desarrollo A. C., s/f, p. 157. Disponible en *http://cidac.org/esp/uploads/1/Tecnolog__a_e_industia_en_el_futuro_de_M__xico_PDF.pdf*, última fecha de consulta el 17 de septiembre de 2019.

[132] *Idem*.

[133] Peña A., Luis de la, "Ciencia y Tecnología en México, país dependiente", *Revista de Cultura Científica*, UNAM, núm. 10. Disponible en

Sin una adecuada infraestructura tecnológica, la capacitación adecuada del capital humano, y un plan definido es prácticamente imposible implementar las directrices para un ciberejército.

Otra de las áreas de oportunidad que deberán ser atacadas antes de llevar a cabo la implementación de las consideraciones que se proponen es el tema de la cooperación internacional en la materia de seguridad pues como se puso de manifiesto en capítulos anteriores, es necesario considerar que los ataques en el ciberespacio ya no solo afectan a los países de manera individual sino que estos ataques que se suscitan todos los días a lo largo del mundo tienen consecuencias a escala global como se puso de manifiesto con los casos que se comentaron líneas atrás.

En el caso de nuestro país es de gran relevancia su posición geográfica con respecto a los Estados Unidos pues desde el año 2001 con el ataque a las Torres Gemelas, el país vecino del norte se interesó por las condiciones de seguridad en nuestro país. Por este motivo se:

> desarrollaron esquemas de cooperación para garantizar el libre flujo de bienes y personas por medio de la llamada Asociación para la Seguridad y la Prosperidad (ASPAN). Sin embargo, el combate a la delincuencia organizada que opera en ambos países fue a partir de 2008 el principal motivo de vinculación colaboración. La Iniciativa Mérida se convirtió gradualmente en el programa de vinculación estratégica más importante. Pensada como un programa de cooperación, la Iniciativa Mérida se enfocó en el fortalecimiento de las instituciones de defensa y seguridad privada, al igual que aquellas relacionadas con la procuración de justicia e inteligencia.[134]

El gobierno de los Estados Unidos a pesar de haber invertido millones de dólares en la asistencia militar y policiaca en México deja ver su inconformidad cuando se trata de evaluar los avances que se han tenido en la materia pues el:

> … gobierno en Estados Unidos en enero de 2017 ha cuestionado la cooperación con México en el ámbito de seguridad. De hecho, el presidente

*https://www.revistaciencias.unam.mx/pt/153-revistas/revista-ciencias-10/1309-ciencia-y-tecnolog%C3%ADa-en-m%C3%A9xico,-pa%C3%ADs-dependiente.htm*l, última fecha de consulta el 17 de septiembre de 2019.

[134] Atlas de seguridad y defensa de México 2016, p. 426. Disponible en *https://www.casede.org/PublicacionesCasede/Atlas2016/Cooperacion.pdf*, última fecha de consulta el 18 de septiembre de 2018.

> Donald Trump ha puesto en duda las capacidades de las instituciones mexicanas de defensa e incluso, ha planteado la posibilidad de enviar tropas estadounidenses a territorio mexicano. Esto pone en entredicho el principio de "responsabilidad compartida", piedra angular de la cooperación en el marco de la Iniciativa Mérida. Además abre una hipótesis de confrontación muy peligrosa entre los dos países, lo cual se pensaba superado.[135]

Esta situación deja a la vista la necesidad también de diversificar la cooperación en la materia con otros países de los que se pueda compartir verdaderas experiencias y no estar en una situación desigual.

Por ello a continuación se mencionan las consideraciones para la implementación de un ciberejército en México, pero que no hay que dejar de observar las condiciones adversas que se han prestado en este apartado, y por el contrario considéralas en el contexto para el diseño e implementación de este cuerpo militar especializado en tecnologías.

### 3.5 Consideraciones para la implementación de un ciberejército

El ciberespacio es un ambiente en el que convergen distintos actores, empresas, individuos, agentes del Estado. Parte del trabajo que los gobiernos realizan en el ciberespacio son tendientes a defender sus activos e intereses estratégicos, en particular salvaguardar la seguridad nacional.

Como primera medida en la implementación de un ciberejército se encuentra realizar un análisis pormenorizado de los riesgos que existen en el entorno digital para el caso mexicano en particular. Se debe contar con instrumentos que revelen la planeación y alcance de las políticas de seguridad digital en todo el territorio de la República Mexicana, saber cuáles son los sectores que se contemplan y los servicios que se ofrecen a la sociedad a fin de considerar las vulnerabilidades de los sistemas, consecuencias en la inactividad de las mismas y por supuesto contemplar su mantenimiento.

Por otro lado, se requiere establecer medias que se deben realizar en caso de que haya un ataque a alguna de las infraestructuras críticas y por supuesto establecer políticas generales para garantizar la seguridad de las instalaciones y

[135] *Idem*.

sistemas. Dentro de los ataques que deben ser considerados por el ciberejército se encuentra el cibercrimen del que ya hablamos al inicio de este trabajo, también el ciberespionaje, el ciberterrorismo, el ciberactivismo, y la por supuesto la ciberguerra.

Dentro de los ataques que se pueden realizar también hay que considerar las vulnerabilidades. Todo experto en el tema de vulnerabilidades reconoce que se entiende por estas a "cualquier debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas".[136] Es por esta razón que es necesario diseñar estrategias para la detección de errores de diseño, o bien de implementación, administración o bien operación en un sistema informático.

Una vez reconocidos los riesgos, vulnerabilidades y amenazas a las infraestructuras críticas de un Estado y así como su planeación estratégica para poder combatir, disminuir o acabar con las mismas se está en la posibilidad de diseñar estrategias de seguridad, dentro de las cuales se encuentra precisamente la creación de un ciberejército.

En cuanto a la inversión en el ciberejército hemos visto que no hay uniformidad en cuanto al recurso económico que invierten los Estados en la creación de un ciberejército, sin embargo tenemos como ejemplo los siete mil millones de dólares que invierte Estados Unidos en su ciberejército frente a los aproximadamente mil seiscientos veinticinco millones que invierte México por lo que es claro que los recursos que se deben destinar a la conformación de este cuerpo especializado debe de incrementarse.

En lo que respecta al personal que se adhiere a estas actividades son dos cosas las que hay que considerar en las directrices. La primera es el número de personas que se integran a la institución que en el caso de Alemania por ejemplo inició con 260 miembros y que sin embargo creación hasta alcanzar las 13,500

---

[136] Documentos de Seguridad y Defensa 60, Estrategia de la información y seguridad en el Ciberespacio, Escuela de Altos Estudios de la Defensa, España, Ministerio de Defensa, p. 31. Disponible en *https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf*, última fecha de consulta el 18 de septiembre de 2019.

personas. Resulta necesario también señalar que México deberá de continuar con las labores de educación e impartición de cursos que permitan capacitar a su personal en temáticas de ciberguerras y como prevenirlas, en analizar y reconocer el tipo de ciberarmas que se pueden utilizar en los ataques.

Las directrices que deben guiar la creación del ciberejército en México por su puesto se encuentra el dotar de capacidades especializadas a su recurso humano en temas de criptografía, defensa de redes de computadoras desde la detección de intrusos, sensores así como para tener la capacidad e respuestas y prevención ante los posibles ataques.

También el conocimiento y respeto para las mejores prácticas hace posible tener un mayor acceso y gestión de identidades, así como el intercambio seguro de la información a fin de no caer presa fácil de los ataques dirigidos.

Finalmente, como se resaltó de este trabajo es de fundamental importancia tener en claro que la cooperación internacional en estos temas dado que como quedó expuesto en líneas anteriores, es necesaria la cooperación internacional para hacer frentes a los retos de ciberseguridad en el ciberespacio y que el contexto de cada país determina los alcances y limitaciones en la implementación de ciberejércitos a nivel mundial.

# Conclusiones

# Conclusiones

A lo largo de esta investigación se aportaron cada uno de los elementos que conforman las categorías de estudio para poder analizar las posibles consideraciones para implementar un ciberejérctio en nuestro país. Se definieron conceptos clave como seguridad nacional, ejército, conflicto armado, entre otros que dieron sustento al resto del trabajo.

Se presentaron algunos ejemplos de los ataques por parte de gobiernos en el ciberespacio para reconocer algunas estrategias militares cuya intención es un enfrentamiento entre Estados y no entre grupos como los terroristas o los hacktivistas. Sin embargo, como se dejó de manifiesto, pese a que puedan existir diversos incidíos de que un Estado es el perpetrador de una actividad en contra de la infraestructura crítica de un Estado, normalmente no se ha logrado identificar al cien por ciento cuál es el Estado perpetrador de los ataques en el ciberespacio y normalmente los gobiernos de los Estados niegan tener algún tipo de injerencia en esos asuntos.

Finalmente se presentaron algunos ejemplos de Estados que ya cuentan con sus ciberejércitos a fin de que se pudiera tener una idea de qué gobiernos ya han implementado sus ejércitos en el ciberespacio y analizar caso por caso las particularidades de esas fuerzas armadas del ciberespacio.

Una vez analizado el contexto en el que se encuentran las fuerzas armadas en nuestro país en relación al tema de la ciberseguridad y la *ciberdefensa* se concluye que existen distintas acciones y objetivos que se pueden rescatar de las experiencias de las estrategias de ciberseguridad planteadas por otros Estados, sobre todo los que se analizaron en el capítulo segundo de esta investigación en donde podemos afirmar que se están haciendo implementaciones bien intencionadas para poder resistir ataques desde el exterior e interior de nuestro país.

Queda mucho trabajo por hacer en relación al ciberjercito, ya que si bien es cierto, se están haciendo esfuerzos para incrementar el poder de nuestras fuerzas armadas, pero también lo es, que no es suficiente, ya que no podemos como nación

quedarnos como espectadores pasivos en recepción de ataques, sino que tenemos que cambiar nuestra mentalidad, hacia una mentalidad propositiva, especialmente en el ámbito de la educación en todos los niveles y generar esfuerzos conjuntos entre las iniciativas públicas y privadas, a efectos que los talentos nacionales dentro de las diversas ramas de conocimiento, incluyendo por supuesto a los especialistas jurídicos, sean llamados a un esfuerzo conjunto para poder hacer frente a esta era digital y alcancemos un poder nacional en donde se pueda medir por la profesionalización, aprovechamiento de nuestros recursos y poder de nuestras fuerzas armadas, que dicho sea de paso, es la institución gubernamental que mayor confianza genera en los ciudadanos de México.

Se tiene que poner especial atención en la inversión dentro de los paquetes económicos con un programa establecido en donde se genere un punto de acuerdo para dotar a las fuerzas armadas de capital económico que genere los elementos necesarios en un corto, mediano y largo plazo para la integración y profesionalización del ciberjercito Mexicano.

Resulta necesario la participación internacional de nuestro ciberejercito en los ejercicios de aprendizaje y en el intercambio de información, ya que como se mencionó en el cuerpo del estudio, este tipo de conductas no tiene jurisdicción para los sujetos activos, pero si consecuencias para los pasivos, por lo que estas sinergias resultan positivas para la generación de aliados de nuestra nación.

La importancia de la transparencia dentro de las Instituciones castrenses, permitirá que personal calificado civil, pueda tener acceso a información que de luz sobre los avances tecnológicos en esta materia, pero no solo eso, también dará pauta a que a corto plazo, exista una participación multisectorial en aras de un bienestar plural.

No podemos dejar pasar por alto, que México requiere una estrategia sólida de ciberseguridad que no sea modificada al cambio de cada gobierno, la estrategia debe de ser solamente una, la de dotar al país de los mejores elementos para contrarrestar el cibercrimen nacional e internacional.

México cuenta con el capital humano suficiente para hacer frente a este reto, basta con impulsar los conocimientos de vanguardia y en no pensar en que la inversión en TIC debe de ser susceptible de autoridad, sino de todo lo contrario, de siempre buscar la innovación dentro las casas de estudio y centros de investigación.

Espero que esta investigación ayude a otros abogados a entender que esta materia no es exclusiva de las ingenierías, que se requieren nuevos especialistas jurídicos que puedan aportar mayor análisis en este tipo de conductas, y que las nuevas generaciones de nativos digitales generen un entorno seguro para la era digital.

# Bibliografía


24 HORAS, “México se arma contra ciberataques”, *Vanguardia.mx*, Nacional, 20 de enero de 2016, disponible en *https: //vanguardia.com.mx/articulo/mexico-se-arma-contra-ciberataques*, última fecha de consulta el 8 de julio de 2019.

Álvarez, Norma L., *et. al*., Tecnología e Industria en el futuro México, posibles vinculaciones estratégicas, Capítulo V, El Problema Tecnológico de México. Rezago Tecnológico e Industrialización Sustitutiva, Centro de Investigación para el Desarrollo A. C., s/f, p. 157. Disponible en *http://cidac.org/esp/uploads/1/Tecnolog__a_e_industia_en_el_futuro_de_M_ _xico_PDF.pdf*, última fecha de consulta el 17 de septiembre de 2019

Añaños Meza, María Cecilia, “La idea de los bienes comunes en el sistema internacional: ¿renacimiento o extinción?, *Anuario Mexicano de Derecho Internacional*, vol. 14, diciembre 2014, disponible en *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542014000100005*, última fecha de consulta el 25 de mayo de 2019. Una cita fue omitida.

Atlas de seguridad y defensa de México 2016, disponible en *https://www.casede.org/PublicacionesCasede/Atlas2016/Cooperacion.pdf*, última fecha de consulta el 18 de septiembre de 2018.

Banco Mundial, “Gasto Militar (% del PIB), Instituto Internacional de Investigación para la Paz de Estocolmo (SPIRI), Yearbook: Armaments, Disarmament and International Security, disponible en *https://datos.bancomundial.org/indicador/ms.mil.xpnd.gd.zs*, última fecha de consulta el 24 de mayo de 2019.

BBC, iWonder, “El virus que tomó control de mil máquinas y les ordenó autodestruirse”, BBC News Mundo, 11 de octubre de 2015, disponible en *https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet*, última fecha de consulta el 26 de mayo de 2019.

BBC, Mundo, Cuáles son los 10 países del mundo que gastan una mayor parte de su riqueza en armamento, 3 de mayo de 2018, disponible en *https://www.bbc.com/mundo/noticias-internacional-43984570*, última fecha de consulta el 24 de mayo de 2019.

Bendovschi, Andrea, “Cyber-Attacks – Trends, Patterns and Security Countermeasures”, en *Procedia Economics and Finance*, núm. 28, 2015.

Botero, Juan David, Ciberejercito alemán: 5 cosas que deberías saber”, en Enter.co, disponible en *https://www.enter.co/chips-bits/seguridad/ciberejercito-aleman-5-cosas-que-deberias-saber/*, última fecha de consulta el 5 de junio de 2019.

Brenner, Susan W., “La Convención sobre Cibercrimen del Consejo de Europa”, Revista Chilena de Derecho y Tecnología, Centro de Estudios en Derecho Informático, Universidad de Chile, vol. 1, núm. 1, 2012.

Bugnion, François, “El derecho de Ginebra y el derecho de la Haya”, Revista Internacional de la Cruz Roja, Comité Internacional de la Cruz Roja, 31 de diciembre de 2001, disponible en *https://www.icrc.org/es/doc/resources/documents/misc/5tdqeh.htm*, última fecha de consulta el 24 de mayo de 2019.

Calderín, Juanafer F. y Jiménez, María, “Estados Unidos, Rusia o China presentan ventajas para el cibercrimen”, *Observatorio Internacional de Estudios sobre Terrorismo*, 7 de julio de 2016, disponible en https://observatorioterrorismo.com/entrevistas/eeuu-rusia-y-china-son-paraisos-del-ciberterrorismo/, consultado el 21 de mayo de 2019.

Calderón, José Luis, Infraestructura crítica en México: el enfoque hacia el futuro, en Segurilatam, disponible en *http://www.segurilatam.com/seguridad-aplicada/infraestructuras-estrategicas/infraestructura-critica-en-mexico-el-enfoque-hacia-el-futuro*, fecha de consulta el 8 de julio de 2019.

Casar Corredera, José Ramón, “Introducción”, *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN*,* Consejo Superior de Estudios de la Defensa Nacional, núm. 126, España, Ministerio de Defensa, 2012.

Centeno, Danya, *México y el Convenio de Budapest. Posibles incompatibilidades*, Red en Defensa de los Derechos Digitales (R3D) y Derechos Digitales. América Latina, 2018, p. 3, disponible en *https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf*, última fecha de consulta el 3 de junio de 2019.

Defunción de *ciberespacio*, Definicion.de, disponible en *https://definicion.de/ciberespacio/*, última fecha de consulta el 24 de mayo de 2019.

Documentos de Seguridad y Defensa 60, Estrategia de la información y seguridad en el Ciberespacio, Escuela de Altos Estudios de la Defensa, España, Ministerio de Defensa, p. 31. Disponible en *https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf*, última fecha de consulta el 18 de septiembre de 2019.

DW, “Ciberdefensa: el Bundeswehr y sus desafíos”, Actualidad, Política, Disponible en *https://www.dw.com/es/ciberdefensa-el-bundeswehr-y-sus-desaf%C3%ADos/a-44989489*, última fecha de consulta el 5 de junio de 2019.

Ejército de Tierra Español, D001-001 Doctrina del Ejército de Tierra, Empleo de las Fuerzas Terrestres, 3a. ed., Dirección de Investigación, Doctrina, Orgánica y Materiales- Mando de Adiestramiento y Doctrina, 2003.

EFE, "Cronología del 'caso Snowden', el joven que reveló el espionaje masivo de Estados Unidos", 20 minutos, 7 de julio de 2013, disponible en *https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/,* última fecha de consulta el 23 de mayo de 2019.

EFE, "EU acusa a dos espías rusos y dos 'hackers' de robar datos de Yahoo.", *El Universal*, 15 de marzo de 2017, disponible en *http://www.eluniversal.com.mx/articulo/techbit/2017/03/15/eu-acusa-dos-espias-rusos-y-dos-hackers-de-robar-datos-de-yahoo*, consultado el seis de diciembre de 2018 a las 17:38 horas.

Estrategia Nacional de Ciberseguidad 2017, disponible en: *https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf*, última fecha de consulta el 8 de julio de 2019.

Euronews, "Alemania lanza su ciber-ejército", abril 2017, disponible en *https://es.euronews.com/2017/04/06/alemania-lanza-su-ciber-ejercito*, última fecha de consulta el 5 de junio de 2019.

European Union Agency for Network and Information Security, (UNISA), Europa, "Ciber Security Strategy for Germany", Noticias, 2011, disponible en *https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1*, última fecha de consulta el 5 de junio de 2019.

Feliu Ortega, Luis, "La ciberseguridad y la *ciberdefensa*", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN*,* Consejo Superior de Estudios de la Defensa Nacional, núm. 126, España, Ministerio de Defensa, 2012.

García, Mariano y Quevedo, José Antonio, "México implementa una estratgia de seguridad cibernética junto a España y Francia", Infodefensa.com, 12 de octubre de 2017, disponible en *https://www.infodefensa.com/latam/2017/10/12/noticia-unidad-ciberseguridad-semar.html*, última fecha de consulta el 23 de diciembre de 2019.

García Campos, Juan Manuel, "El ciberejército de Putin", *Magazine digital*, disponible en *http://www.magazinedigital.com/historias/reportajes/ciberejercito-putin* fecha de consulta el 21 de mayo de 2019.

Gobierno de España, Presidencia del Gobierno, *Estrategia de ciberseguridad nacional*, s/f, disponible en European Union Agency for Network and

Information Security, disponible en *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy*, última fecha de consulta el 5 de junio de 2019.

Gobierno de México, "Estrategía Nacional de Ciberseguridad" México 2017, disponible en *https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf*, última fecha de consulta 16 de diciembre del 2019.

Grünschläger, Gustavo Ricardo, "Global Commons", *Revista de la Escuela de Guerra Naval*, Armada de Argentina, núm. 61, diciembre 2015, p. 46. Disponible en *http://www.cefadigital.edu.ar/bitstream/123456789/334/1/4_Revista_61_Global_Commons_w4.pdf,* última fecha de consulta el 25 de mayo de 2019.

Guimón, Pablo "EEUU lanzó este jueves un ciberataque a Irán autorizado por Trump, 24 de junio 2019, disponible en *https://elpais.com/internacional/2019/06/23/estados_unidos/1561302401_346950.html*, última fecha de consulta 10 de septiembre del 2019.

Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacionales (IMEESDN), disponible en *https://www.gob.mx/sedena/articulos/instituto-mexicano-de-estudios-estrategicos-en-seguridad-y-defensa-nacionales-imeesdn?idiom=es*, última fecha de consulta el 17 de septiembre de 2019.

ITU, "Half of all countries aware but lacking national plan on cybersecurity, UN agency reports", *UN News, Global perspectives stories*, 5 July 2017. Disponible en *https://news.un.org/en/tags/cyber*, última fecha de consulta el 4 de junio de 2019.

Jun, Jenny, LaFoy, Scott y Sohn, Ethan, *North Korea's Cyber Operations, Strategy and Responses. A report of the CSIS Korea Chair*, Londres, Nueva York, Boulder, Lanham, Center for Strategic and International Studies, Roman & Littlefield, 2015, disponible en *https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf*, ultima fecha de consulta el 6 de junio de 2019.

Kramer, Franklin D, Starr, Stuart H., y Wentz, Larry K., Cyberpower and National Security, hacienda referencia a The Law of Land Warfare.

Krepinevich, Andrew F., "Calvary to Computer. The Pattern of Military Revolutions", *The National Interest*, Fall 1994.

Leal Buitrago, Francisco, "La doctrina de seguridad nacional: materialización de la Guerra Fría en América del Sur*", Revista de Estudios Sociales*, núm. 15, junio de 2003, p. 74.

Lee, Dave, “Los países mejor preparados para resistir un ciber ataque… y los peores”, *BBC News Mundo*, 31 de enero de 2012, disponible en *https://www.bbc.com/mundo/noticias/2012/01/120131_ciberataques_paises_mejor_peor_preparados_adz*, consultado el 21 de mayo de 2019.

López de Tursio y Sánchez, Javier, “La evolución del conflicto hacia un nuevo escenario bélico”, en *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, Consejo Superior de Estudios de la Defensa Nacional, núm. 126, España, Ministerio de Defensa, 2012.

Martín del Barrio, Javier, “El secretario general de la ONU dice que hay ‘ciberguerra entre los Estados’”, *El País*, publicado el 19 de febrero de 2018, disponible en *https://elpais.com/internacional/2018/02/19/actualidad/1519058033_483850.html*, última fecha de consulta el 3 de junio de 2019.

McKinsey&Company, Perspectiva de ciberseguridad en México, México, Consejo Mexicano de Asuntos Internacionales, junio, 2018.

McMaster, H. R., “Continuity and Change. The Army Operating Concept and Clear Thinking about future War, Military review, March – April 2015, p. 10. La traducción es libre. Disponible en *https://www.queensu.ca/kcis/sites/webpublish.queensu.ca.kciswww/files/files/2015/MilitaryReview_20150430_art005.pdf*, última fecha de consulta el 26 de mayo de 2019.

Medellín, Jorge Alejandro, “El ejército mexicano pone en marcha su Instituto de Estudios Estratégicos”, Defensa.com. Actualidad, 10 de octubre de 2018. Disponible en *https://www.defensa.com/mexico/ejercito-mexicano-pone-marcha-instituto-estudios-estrategicos*, última fecha de consulta el 17 de septiembre de 2019.

Murguía Rosete, José Antonio, “Actualidades del derecho internacional convencional: la negociación y los tratados internacionales”, en Velázquez Elizarrarás, Juan Carlos, *El derecho internacional público en la agenda política de las relaciones internacionales*, México, UNAM, 2005.

Navarro Bonilla, Diego, “Espionaje, seguridad nacional y relaciones internacionales”, *Colección de estudios internacionales*, núm. 14, 2013-2014, pp. 9 y 10, disponible en *https://web-argitalpena.adm.ehu.es/pdf/USPDF170933.pdf*, última fecha de consulta el 24 de mayo de 2019.

OEA, Programa de Ciberseguridad, disponible en *http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp*, última fecha de consulta el 8 de julio de 2019.

Pastor Acosta, Oscar “Capacidades para la defensa en el *ciberespacio*”, *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN,

Consejo Superior de Estudios de la Defensa Nacional, núm. 126, España, Ministerio de Defensa, 2012.

Peña A., Luis de la, “Ciencia y Tecnología en México, país dependiente”, *Revista de Cultura Científica*, UNAM, núm. 10. Disponible en *https://www.revistaciencias.unam.mx/pt/153-revistas/revista-ciencias-10/1309-ciencia-y-tecnolog%C3%ADa-en-m%C3%A9xico,-pa%C3%ADs-dependiente.html*l, última fecha de consulta el 17 de septiembre de 2019.

Perieira Menaut, Antonio – Carlos, “Después de la soberanía”, *Revista de derecho político*, núm. 50, 2001.

Piña Libien, Hiram Raúl, “Los delitos informáticos previstos y sancionados en el ordenamiento jurídico mexicano”, Segundo Congreso Nacional, “Cultura de la Legalidad e Informática Jurídica, México, Secretaría de Gobernación, 2012.

Plan Nacional de Desarrollo 2019-2024. Disponible en *https://lopezobrador.org.mx/temas/plan-nacional-de-desarrollo-2019-2024/*, última fecha de consulta el 17 de septiembre de 2019.

Ramírez García de León, Xavier Jared, *Conflicto armado no internacional en el México actual y cuasibeligerancia de los cárteles narcotraficantes*, Tesis, México, UNAM, Facultad de Derecho, 2012.

Reguera Sánchez, Jesús, “Aspectos legales en el *ciberespacio*. La ciberguerra y el Derecho Internacional Humanitario”, *Análisis del Grupo de Estudios en Seguridad Internacional*, Universidad de Granada, 14 de junio de 2015.

Remus, Titiriga, “Cyber-attacks and international law of armed conflicts; a ‘jus ad bellum’ perspective”, en *Journal of International Commercial Law and Technology*, vol. 8, no. 3, 2013

Riquelme, Rodrigo, “Estrategia Nacional de Ciberseguridad, marcada por fin de sexenio”, El Economista, 5 de diciembre de 2017. Disponible en *https://www.eleconomista.com.mx/politica/Estrategia-Nacional-de-Ciberseguridad-marcada-por-fin-de-sexenio-20171205-0041.html,* última fecha de consulta el 8 de julio de 2019.

Riquelme, Rodrigo, Estrategia Nacional de Ciberseguridad queda en recomendaciones para gobierno de AMLO”, El Economista, 29 de agosto 2018, disponible en *https://www.eleconomista.com.mx/empresas/Estrategia-Nacional-de-Ciberseguridad-queda-en-recomendaciones-para-gobierno-de-AMLO-20180829-0035.html*, última fecha de consulta el 8 de julio de 2018.

Robles Castillo, Margarita, “El concepto de arma cibernética en el marco internacional: una aproximación funcional”, *Documento de Opinión, Instituto Español de Estudios Estratégicos, Boletín Electrónico*, 3 de octubre de 2016, pp. 10 -12. Disponible en

*http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf*, última fecha de consulta el 26 de mayo de 2019.

S/A, *India's National Security Strategy*, 2019, p. 39, disponible en *https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf*, última fecha de consulta el 5 de junio de 2019.

S/A, "La OTAN publica manual de ciberguerra", Diario TI, 21 de marzo de 2013, disponible en *https://diarioti.com/la-otan-publica-manual-de-ciberguerra/62351*, última fecha de consulta el 24 de mayo de 2019.

S/A, *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*, disponible en *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf*, última fecha de consulta el 5 de junio de 2019.

Salazar, Juan Pablo, "La migración de la guerra al espacio digital", disponible en *https://www.sites.oas.org/cyber/Documents/2016%20-%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf*, última fecha de consulta el 24 de mayo de 2019.

Salazar, Juan Pablo, "La migración de la guerra al espacio digital", disponible en *https://www.sites.oas.org/cyber/Documents/2016%20-%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf*, última fecha de consulta el 21 de mayo de 2019.

Sánchez Medero, Gema, "Los Estados y la ciberguerra", Boletín de Información (Ministerio de Defensa), núm. 317, disponible en *https://dialnet.unirioja.es/servlet/autor?codigo=1005925*, última fecha de consulta el 3 de junio de 2019.

Seara Vázquez, Modesto, *Derecho internacional público*, 15a. ed., México, Porrúa, 1994.

Secretaría de la Defensa Nacional, ¿qué hacemos?, Gobierno de México, disponible en *https://www.gob.mx/sedena/que-hacemos*, última fecha de consulta el 8 de julio de 2019.

Seguridad Nacional y *Ciberdefensa*, ISDEFE, cátedra ISDEFE-UPM 6, página 127.

Schmitt, Michael N., Taillin Manual on The International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Edinburgh,

Cambridge University Press, 2013, disponible en *http://csef.ru/media/articles/3990/3990.pdf*, ultima fecha de consulta el 21 de **septiembre** de 2019.

Schmitt, Michael N., *International Law in ciberespace: The Koh Speech and Tallinn Manual Juxtaposed*, Harvard International Law Journal, vol. 54, 2012.

Stackelberg, Filippa von, "Germany prepares for cyber war", New security learning. Technology-Assisted Training for Security, Defence and Emergency Services, disponible en *http://www.newsecuritylearning.com/index.php/feature/88-germany-prepares-for-a-cyber-war*, última fecha de consulta el 5 de junio de 2019.

Tellis, Ashley J., Bially, Janice, Layne, Christopher, McPherson, Melissa, Sollinger, Jerry M., *Measuring National Power in the Postindustrial Age*., California, Arroyo Center, Rand, 2000.

Unión Internacional de Telecomunicaciones, Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar, Informe, 2017, disponible en *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf*, última fecha de consulta el 8 de julio de 2019.

United States of America, Department of Defense, "Militaru and security developments involving the Democratic People's Republic of Korea", Anual Report Congress, 2013, disponible en *https://dod.defense.gov/Portals/1/Documents/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf*, última fecha de consulta el 5 de junio de 2019.

Valdés Ugalde, José Luis, "Globalización vs. Soberanía: gobernanza, guerra o progreso y orden mundial, *Norteamérica*, año 2010, núm. 2, julio – diciembre de 2015.

Waxman, Matthew C., "Cyber Attacks as "Force" Under UN Charter Article, vol. 2, núm. 4, Columbia Law School, 2011, en disponible en *https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1882&context=faculty_scholarship*, última fecha de consulta el 4 de junio de 2019.