Facultad del Ejército

Sede Educativa
Escuela Superior de Guerra
"Tte Grl L. M. Campos"

UNDEF
Universidad de la Defensa Nacional

INFORME FINAL
PROYECTO DE INVESTIGACIÓN:

"La Defensa Cibernética Alcances estratégicos, proyecciones doctrinarias y educativas".

Trabajo de Investigación elaborado desde la Carrera Licenciatura en Relaciones Internacionales Orientación en Escenarios de Conflictos, Misiones de Paz y Desarme

Director: - **Doctor Javier Ulises ORTIZ**
(Investigador acreditado por UNDEF, MinEduc y MinDef)

Investigadores: - **Doctora Claudia FONSECA**

- **Magister Miguel ANSORENA GRATACOS**
(Investigador acreditado por UNDEF, MinEduc y MinDef)

Investigadora auxiliar: Tcnl. Auditora Luz Ivone PERDOMO (Alumna 4° Año, colaboró en elaboración del Cap 3.)

Marzo 2017

Nota: El presente estudio es de carácter académico. Sus contenidos no constituyen la opinión oficial de la Institución. Su utilización es a los solo fines educativos y actividad de investigación científica. El mismo es una síntesis de diversos trabajos parciales desarrollados a lo largo de la investigación que serán oportunamente publicados.

Director del Proyecto:

ORTIZ, Javier Ulises: Doctor en Ciencia Política, Licenciado y Profesor en RRII por la Universidad del Salvador (USAL), Bs. As. Estancia posdoctoral en la Universidad Nacional de Cuyo (UNCuyo), Mendoza. Postgraduado en "Estrategia I y II" (ESG), en "Planeamiento de Defensa" y en "Estrategia y Política de Defensa" (*US National Defense University*), WDC. Profesor de Educación a Distancia (SEADEA). Investigador Principal de la UNDEF, Categoría II del Programa Incentivos del Ministerio de Educación y Jefe de Proyectos, RPIDFA-Ministerio de Defensa. Director de la Lic. en RRII (orientación en Conflictos Internacionales, Misiones de Paz y Desarme) (ESG). Docente del Curso de Estado Mayor (ESG) y de la Maestría en Estrategia Militar (ESGC). Miembro del Registro Expertos CONEAU y de la Cátedra Libre Historia e Historiografía en Paz y Conflictos (UNCuyo).

Investigadores:

ANSORENA GRATACOS, Miguel: Magister en Defensa Nacional por el Instituto Universitario del Ejército y Magister en Dirección de Instituciones Educativas (UnAustral). Licenciado y Profesor en Relaciones Internacionales (RRII) por la Universidad Católica de Salta (UCSalta). Egresado del Curso Superior en Defensa Nacional de la Escuela de Defensa Nacional (EDENA-IUE). Profesor de Educación a Distancia (SEADEA). Investigador Principal de la UNDEF, Categoría IV del Programa Incentivos del Ministerio de Educación y en RPIDFA-Ministerio de Defensa. Docente de la Lic. en RRII (orientación en Conflictos Internacionales, Misiones de Paz y Desarme) (ESG) y de las Escuelas Superiores de Guerra Aérea (ESGA) y de Guerra Conjunta (ESGC) de la UNDEF. Realizó el Curso Formación de Investigadores (ESG).

FONSECA, Claudia Elisabeth: Doctora en Psicología Social y Licenciada en Ciencia Política por la Universidad Argentina John F. Kennedy (UAJFK). Profesora de Educación a Distancia (SEADEA). Docente de la Lic. en RRII (orientación en Conflictos Internacionales, Misiones de Paz y Desarme) (ESG) y en nivel posgrado en la UAJFK. Ex profesora del Colegio Militar de la Nación y del Instituto Universitario de la Policía Federal Argentina (IUPFA). Realizó el Curso Formación de Investigadores (ESG).

PERDOMO, Luz Ivone: Teniente Coronel Auditora del Ejército Argentino. Abogada por la Universidad Católica de La Plata. Alumna de IV año de la Lic. en RRII (orientación en Conflictos Internacionales, Misiones de Paz y Desarme). Jefa de la asesoría legal de la Secretaria General del Estado Mayor General del Ejército Argentino. Colaboró en la elaboración del Cap. 3.

ABSTRACT

La Defensa Cibernética constituye un nuevo ítem de la agenda de Defensa Nacional y, por ende un tema de responsabilidad de las Fuerzas Armadas. El imperativo tecnológico informacional que influye y determina en la agenda internacional, crea nuevos escenarios de cooperación y conflicto, lo que constituye un desafío, a la vez que una oportunidad, para que los estados desarrollen capacidades tendientes a asegurar su accionar y sus intereses en un nuevo campo de acción, aparentemente virtual, pero con impacto directo en todos los ámbitos toda vez que la dinámica de las naciones y sus habitantes, se encuentran directamente asociadas a las infraestructuras críticas y críticas informacionales que interconectan todos los órdenes de la vida. Así entender e investigar la defensa cibernética, en sus distintos ámbitos y aspectos, adaptándose y transformándose a sus necesidades, constituye una necesaria responsabilidad estratégica para la Defensa Nacional.

Los resultados a obtener permitirán al perfeccionamiento de profesionales militares y civiles del área de las ciencias sociales y humanas, vinculados a la Defensa Nacional, en el análisis, conocimiento y aplicación de la nueva concepción militar de la defensa cibernética de las infraestructuras críticas determinado sus alcances estratégicos, proyecciones doctrinarias y apreciar las nuevas proyecciones de capacitación en esta nueva materia propendiendo a la investigación continua, la enseñanza militar específica y la educación en el nivel grado y postgrado. El entendimiento y conocimiento de la adaptación y transformación del sistema de defensa a la Era de la Información como elemento distintivo en las relaciones internacionales actuales en lo atinente al desarrollo de infraestructuras informacionales y sistemas de ciberdefensa en el campo estratégico-militar posibilitará elaborar un cuadro de situación actualizado para proyectos a futuro, cooperación académica y/o extensión educativa.

CAPITULO 3

Conceptos y Marco Legal de la Ciberdefensa en el Sistema Internacional

CAPITULO 4

Apreciación Estratégica de la OTAN en materia de Ciberdefensa frente a dos casos Estonia (ciberataque) y Georgia (ciberguerra).

CAPITULO 5

Estrategias en materia de Ciberdefensa

CAPITULO 6

Proyecciones educativas en el ámbito de la defensa.

Introducción

Al presente, es un hecho insoslayable que nos encontramos no solo en un nuevo siglo sino que la era industrial (que va desde la invención de la máquina a vapor y su segunda fase con el desarrollo del motor a combustión) ha dejado lugar a la denominada era de la información, sustentada sobre los avances tecnológicos. Esta, entendida como el impacto de las telecomunicaciones y la informática conforma la infraestructura tecnológica de la globalización que hace posible la toma de decisiones estratégicas en tiempo real a una escala global.

Daniel Khuel, de la National Defense University de EUA, ha definido en 2009 al ciberespacio como un marco operacional regido por el uso de la electrónica y del espectro electromagnético para crear, guardar, modificar, intercambiar, y desarrollar la información mediante interconexiones e interconexiones a los sistemas de información con sus infraestructuras asociadas (Llongeras Vicente, 2013).

Por su parte, Clarke R Knake, expone que “el ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de internet, podemos comunicarnos con cualquier ordenador conectado con cualquiera otra de las redes de internet. El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde internet. Algunas de esas redes privadas son muy semejantes a internet, pero, al menos teóricamente, se encuentran separadas de ella” (Clark, 2011, p. 17).

En este sistema de producción integrado-transnacional que se desenvuelve en el ciberespacio, participan juntos a los Estados, decenas de miles de empresas altamente tecnológicas de carácter mundial con centenares de miles asociadas. En respuesta a ello, surgen innovadores conceptos como “Estado Digital” (Keyworth y otros, 1998) o en el denominado “Estado-Red” (Castells, 1998), adaptado a los requerimientos de esta nueva era donde la soberanía pasa a ser no solo territorial sino “espacial”. Estos cambios económicos, tecnológicos, políticos y organizacionales impactaron también en lo social, creando inclusión o exclusión respecto de sus beneficios así como en las estructuras de defensa de los Estados. En tal sentido surgen políticas y estrategias de ciberdefensa en respuesta a ello (Ortiz, 1999).

Asimismo, el ciberespacio otorga capacidad a todo tipo de actores (estatales o no estatales) y para influir políticamente de modo indirecto o directo quitando en cierta medida esta atribución propia del Estado y posibilitando el desarrollo y aplicación de poder y amenaza sobre otros a cualquier actor con capacidad en el ciberespacio (Llongueras Vicente, 2011) lo que constituye al ciberespacio como un elemento de influencia estratégica de consideración en materia de seguridad (Llongueras Vicente, 2011).

La Directiva de Política de Defensa Nacional del Ministerio de Defensa de la República Argentina, define al ciberespacio como:

> "*… los usos militares de las novedosas tecnologías asociadas a la robótica, cibernética, sensores remotos, entre otros desarrollos en materia de ciencia y tecnología, han impulsado nuevas formas de librar la guerra que exhiben un salto cualitativo hacia un nuevo paradigma tecnológico. … Otro aspecto asociado al nuevo paradigma tecnológico y a las tecnologías de la información es la importancia que está adquiriendo el ciberespacio para el desarrollo de las operaciones militares. La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la 'guerra real' y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también el ciberespacial. Éste no constituye un 'espacio en sí mismo', sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias*" (Ministerio de Defensa de la República Argentina, 2014).

CAPITULO 1

La globalización y sus nuevos riesgos: la sociedad del riesgo global. Debates.

La estructura internacional y el mundo en general se han transformado. El paradigma y la epistemología de la modernidad madura nos imponen ciertos arquetipos que nos impiden ver las nuevas realidades por lo que necesitamos nuevos mapas cognitivos y nuevas categorías de análisis para comprender esta continua transformación (Tomassini, 1995).

Los cambios políticos, económicos, socioculturales y medioambientales desarrollados en las últimas décadas han conformado una nueva sociedad denominada posmoderna, donde la política y el mismo poder encuentran dependencias con nuevos actores como los que emergen de las tecnologías de la información e Internet misma. Asimismo esta nueva sociedad desarrolla nuevas interacciones (redes sociales) en el ciberespacio donde actores no estatales de distinta naturaleza generan contantemente potenciales riesgos y amenazas de carácter global tanto en el campo de la seguridad, la riqueza y en las relaciones internacionales contemporáneas procurando crear desorden donde los Estados se encuentran potencialmente debilitados por la dependencia tecnológica lo que demanda incorporar en sus agendas el tratamiento de esta problemática. Así, luego del planteo del Fin de la Historia[1] o del Choque de las Civilizaciones[2] o los debates entre teorías realistas e idealistas o enfoques cientificistas y tradicionalistas de relaciones internacionales, se presenta el "Tercer Debate" (modernidad-postmodernidad) que tiene como eje lo que el sociólogo alemán Ulris Beck llamó la Sociedad del Riesgo Global en tanto que ya no está sustentada en un reparto de la riqueza sino de los riesgos (Ibáñez Muñoz, 2010).

El accidente de la central atómica de Chernobyl, en Ucrania, por su impacto de radioactividad en gran parte de Europa Central y Oriental, constituirá el primer indicio de la conformación de percepción social del riesgo común a todos porque afecta todo, inclusive el consumo (Beck, 1983).

[1] El Fin de la Historia, obra del autor estadounidense Francis Fukuyama
[2] Título de la obra de Samuel Huntington en la cual se planteaba con la caída del Muro de Berlín, terminaba un ciclo y comenzaba otro donde el enemigo de Estados Unidos serían Culturas con valores, religión y cultura antagónica a Occidente.

Hoy en día, la tecnología es un bien de consumo masivo. Así, la afectación a su acceso constituye un riesgo y, dado que la sociedad está reconfigurada a partir de su uso (redes sociales) se hace la constante posibilidad de verse su acceso impedido y, por ende en parte su seguridad (Ibáñez Muñoz, 2010).

Así, la inseguridad de la sociedad posmoderna no resulta de la carencia de medios para protegerse sino de buscar poseer constante y permanente seguridad en un mundo tecnológicamente interrelacionado (Castel, 2002).

1.1 Características del poder en la sociedad del Riesgo.

Por su amplitud (siempre creciente) y virtualidad, la seguridad en el ciberespacio no puede ser perfecta. Asimismo la vulnerabilidad de la Red tiene un Talón de Aquiles toda vez que los ataque informáticos afecten las infra estructuras críticas que hacen al funcionamiento mismo del propio sistema. (Howard; Longstaff, 1998)

Este contexto de la nueva “era informacional” se caracteriza por “una crisis de legitimidad está vaciando de significado y función a las instituciones de la era industrial. Superado por las redes globales de riqueza, poder e información, el estado-nación moderno ha perdido buena parte de su soberanía” y donde se manifiestan tres tipos de identidades: las individuales, las de resistencia y las identidades proyecto (Castells, 1999, p 394).

El poder en la Era de la Información:

“*ya no se concentra en las instituciones (el estado), las organizaciones (empresas capitalistas) o los controladores, se difunde en redes globales de riqueza, poder, información e imágenes, que circulan y se transmutan en un sistema de geometría variable y geografía desmaterializada. Pero no desaparece. El poder sigue rigiendo la sociedad; todavía nos da forma y nos domina. No sólo porque los aparatos de distintos tipos aún pueden disciplinar los cuerpos y silenciar las mentes. Esta forma de poder es eterna y, al mismo tiempo, se está desvaneciendo. Es eterna porque los humanos somos, y seremos, predadores. Pero, en su forma actual de existencia, se está desvaneciendo: el ejercicio de este tipo de poder es cada vez menos efectivo para los intereses que pretende servir. Los estados pueden disparar, pero puesto que el perfil de sus enemigos y el*

paradero de sus contendientes son cada vez menos claros, tienden a hacerlo al azar, con la probabilidad de dispararse ellos mismos. El nuevo poder reside en los códigos de información y en las imágenes de representación en torno a los cuales las sociedades organizan sus instituciones y la gente construye sus vidas y decide su conducta. La sede de este poder es la mente de la gente. Por ello, en la era de la información, el poder es al mismo tiempo identificable y difuso" (...) "Quien gane la batalla de la mente de la gente gobernará, porque los aparatos rígidos y potentes no serán un rival, en un espacio de tiempo razonable, para las mentes movilizadas en torno al poder de redes alternativas y flexibles. Pero puede que las victorias sean efímeras, ya que la turbulencia de los flujos de información mantendrá a los códigos en un torbellino constante. Por este motivo son tan importantes las identidades y, en definitiva, tan poderosas en esta estructura de poder en cambio constante, porque construyen intereses, valores y proyectos en torno a la experiencia y se niegan a disolverse". (Castells, 1999, p. 400)[3]

Esta nueva característica la política y el poder en la era de la información determinan condicionamientos a los actores. Ellos poseerán existencia en la medida que mantengan identidad, sostengan su movilidad y por sobre todo generen influencia sobre otros actores.

Esta nueva dinámica del poder encuentra un nuevo espacio, el "ciberespacio" donde se desenvuelve y reconfigura.

El ciberespacio conforma así un ámbito propicio para el desarrollo de distintas nuevas formas de poder e influencia como la cultural denominadas "*soft power"* (Nye , 1990).

Este poder blando permite persuadir, ejercer atracción y conformar las preferencias ajenas para que coincidan con las nuestras. Internet contribuye a generar de manera desorganizada fobias y filias hacia ideologías, hacia estilos de vida, hacia culturas y tradiciones de otros países y sociedades. Tanto si hay una intencionalidad en el marco de la política exterior de un Estado como si no la hay, el poder cultural es tan político como el soft power promovido desde Estados Unidos (Nye, 2002).

[3] El sociólogo español Manuel Castells es considerado el Max Weber de la nueva era de las tecnologías de la información. Su obra, La Era de la Información, traducida a 23 idiomas, es considerada académicamente como base para comprender los impactos de las tecnologías de la información en el presente.

1.2 Tipos de actividad cibernética con incidencia de riesgos y/o amenazas en el ciberespacio.

La Publicación Conjunta 1-02 del Departamento de Defensa de Estados Unidos, en su primera versión que data de 2010 y actualizada a 2016, define al "ciberespacio" 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" (DoD, 2016, p 58).

Varios especialistas asignan el concepto "Global Commons" al momento de entender estratégicamente el ciberespacio. Se entiende actualmente como "Global Commons", provenientes del derecho medieval británico cuando se referían a los terrenos comunales a "aquellos espacios del orbe que no estando bajo jurisdicción o control de Estado alguno, están abiertos al acceso y uso de actores estatales y no estatales" (Grünschläger, 2015).

Así, el ciberespacio ha quedado entendido desde el punto de vista geoestratégico, como uno de los cuatro "Global Commons" (espacios aéreos, aguas, exterior y ciberespacio) en tanto espacios que, *"sin estar sujetos a la soberanía de país alguno, son utilizados por las naciones para transportar personas o bienes y servicios o para transmitir datos"* a lo que se suma que en el ciberespacio *"tanto el continente como el contenido son creados por el hombre y, por lo tanto, su diseño –incluidas sus imperfecciones– son fruto del esfuerzo humano y responden a unas circunstancias concretas que se dieron en el momento de su diseño y desarrollo"* (Gómez de Agreda, 2012. pp. 171 a 173).

Sergio Villaescusa González, miembro del Centro de Formación Interactiva para la Cultura de la Defensa (CFICD) con sede en Sevilla (España), ha realizado un listado de conceptos clave en materia de actividades cibernética consideradas como riesgosas y/o amenazas a la sociedad y los Estados en el ciberespacio:

- "Ciberespionaje industrial": que se caracteriza por robar información sensible (patentes industriales, datos de proveedores, clientes, etc.) a empresas.
- "Ciberespionaje gubernamental": penetración en redes y bancos de datos oficiales.
- "Ciberataques a infraestructuras críticas": centrales nucleares, petrolíferas, etc.
- "Cibermercenarios": hackers contratados para operar contra objetivos precisos.

- “Ciberdelincuencia contra servicios financieros”: mediante el robo de bancos datos de tarjetas de crédito.
- “Ciberdelincuentes aislados”: obtienen información de todo tipo, especialmente de tarjetas de crédito para ser vendidas en el mercado negro.
- “Ciberdelincuentes organizados”: proyección de mafias más dedicados a o mafias que han trasladado al mundo “virtual” sus acciones en el mundo “real”. Fraude online, clonación de tarjetas de crédito, extorsión, blanqueo de capitales, etc”.
- “Ciberhacktivistas”: quienes realizan ataques generalmente contra páginas web y/o publican contenidos por motivaciones político-ideológicas como el grupo Anonymous.
- “Cibersabotaje”: organizaciones autodenominadas ejércitos electrónicos que realizan ataques a websites o difunden noticias falsas, como el Ejército Electrónico Sirio que tras difundir noticias falsas provocó la caída del índice industrial de la Bolsa Industrial de Valores.
- “Ciberterrorismo”: al respecto cabe destacar que ningún grupo terrorista ha tenido mucho éxito en causar daños de significación a infraestructuras civiles o militares (Villaescusa González, 2016).

1.3 La Ciberseguridad

La Unión Internacional de Telecomunicaciones, en su resolución 181, recomendación UIT-TX 1205 de noviembre de 2010, definió “ciberseguridad” como:

“*el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.*

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. 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 incluyen una o más de las siguientes:

- *disponibilidad;*
- *integridad, que puede incluir la autenticidad y el no repudio; y*
- *confidencialidad*". (UIT, 2010, pp. 20 a 22)

En tal sentido, situaciones conflictivas que emergen en ese marco, denominadas por juristas como "el conflicto cibersecuritario", será "la situación de crisis producida por la discordancia entre dos o más entes implicados en el ciberespacio o algunos de sus elementos integrantes, en el ámbito de su individualidad o en la de su campo de relaciones, con deterioro del medio, por causas exógenas al normal funcionamiento del sistema" (Molina Mateos[4], 2013).

[4] Doctor en Derecho por la Universidad Complutense de Madrid.

CAPITULO 2

La defensa cibernética, alcances doctrinarios y proyecciones doctrinales

2.1 La Protección de las Infraestructuras Críticas y las ciberguerras

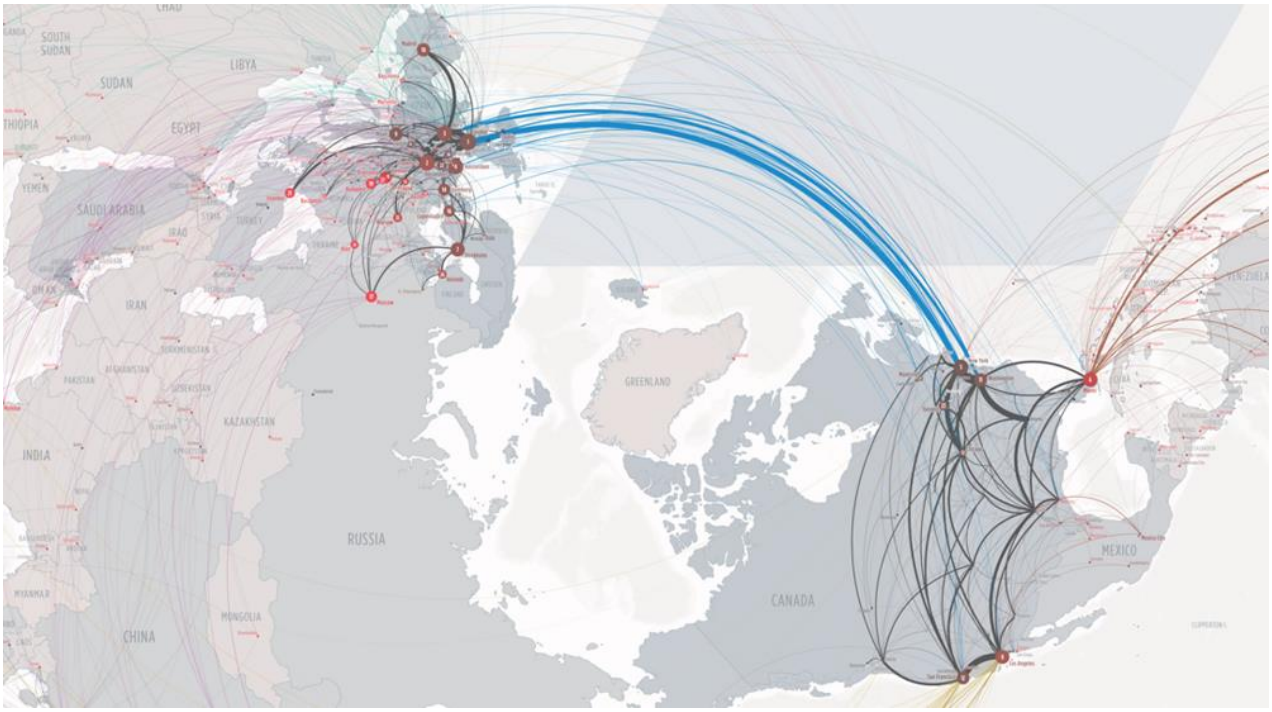
Las nuevas tecnologías se asientan en el espacio urbano. Allí se estructuran los nodos de las infraestructuras críticas dadas por el complejo tecnológico-electrónico-informacional así como la compleja logística que supone sostener los requerimientos de subsistencia de las grandes concentraciones urbanas y la administración de sus recursos. Por lo tanto, la concentración urbana crea un nuevo espacio "las megalópolis" constituyéndose en ellas sistemas "metaestables" que las sostienen y por ello verdaderamente críticos.

El uso de dispositivos digitales en esta era de la información ya es una realidad global donde una parte importante de la población mundial se conecta, trabaja, estudia, se organiza, en síntesis convive con las TICs. Estudios publicados a principios de 2016 indican que cerca de la mitad de la población mundial, (47%), que alcanzó más de 7.300 millones, son usuarios de Internet. Asimismo, un 51 % utiliza móviles y se estima en que un 31 % de la población mundial está presente en redes sociales: de ellos el 27 % se conecta a ellas a través de sus dispositivos móviles.

En cuanto a la penetración del uso de Internet por áreas geográficas, se ordena en orden decreciente:

- 88 % en América del Norte
- 83 % en Europa
- 68 % en Oceanía
- 64 % en Europa del Este
- 60 % en América del Sur
- 54% en Asia del Este
- 53% en Medio Oriente
- 41% en el Sudeste Asiático
- 40% en Asia Central
- 29% en África
- 27% en el Sur de Asia. (We Are Social, 2016)

Asimismo, los nuevos sistemas de la era de la información construyen redes globales donde sus interconexiones o nodos se asientan en las megalópolis. Este nuevo espacio es virtual, pero a la vez real ya que es el soporte de la infraestructura de esta era posindustrial, signada por intercambios tecno-informativos en gran parte del quehacer humano. Así, se puede apreciar el principal núcleo de nodos donde se realizan esos intercambios, principalmente en y entre EUA y Europa:



https://www.telegeography.com/telecom-maps/global-internet-map.html

La Oficina de Protección de la Infraestructura Crítica de los Estados Unidos (EUA) entiende por "infraestructura crítica" (IC) a los sistemas que tienen incapacidades o podrían ser debilitados o destruidos con impacto en la defensa y seguridad económica de la nación, incluyendo bancos, transporte, sistemas de agua, servicios del gobierno y gobiernos públicos[5].

En virtud de estos nuevos espacios, resurgen correlativamente en la agenda de defensa los objetivos de preservar recursos estratégicos como el agua (el control y aseguramiento de sus fuentes), los alimentos, las fuentes de energía, etc. claramente identificados por el asesor en

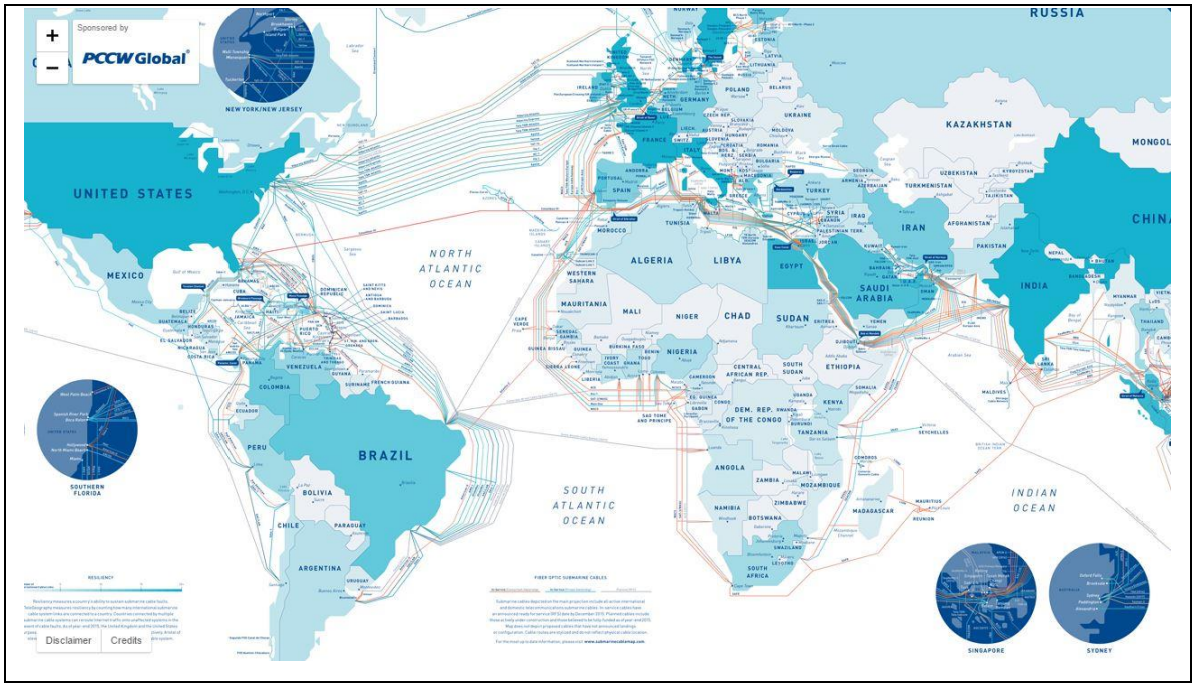
[5] Plan of "Critical Infrastructure Assurance Office" (CIAO); Strategy to Secure Cyberspace -NSSC) y National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

temas de defensa en Francia Philippe Delmas en su clásico libro “El brillante porvenir de la Guerra” ese “porvenir”, estará dado por nuevos conflictos por la necesidad de agua, alimentos, su transporte, etc. (Delmas, 1995).

En términos del presente enfoque, esos objetivos se encuentran directamente asociados a los nodos ya que los sistemas de aprovisionamiento de agua, las redes de producción y distribución de energía, etc., están integradas al sistema informacional para su control y distribución. Así, ese nuevo “campo”, demanda sistemas de protección, previsión, aseguramiento y defensa contra los riegos y catástrofes provocados por incidentes no intencionales, intencionales o desastres.

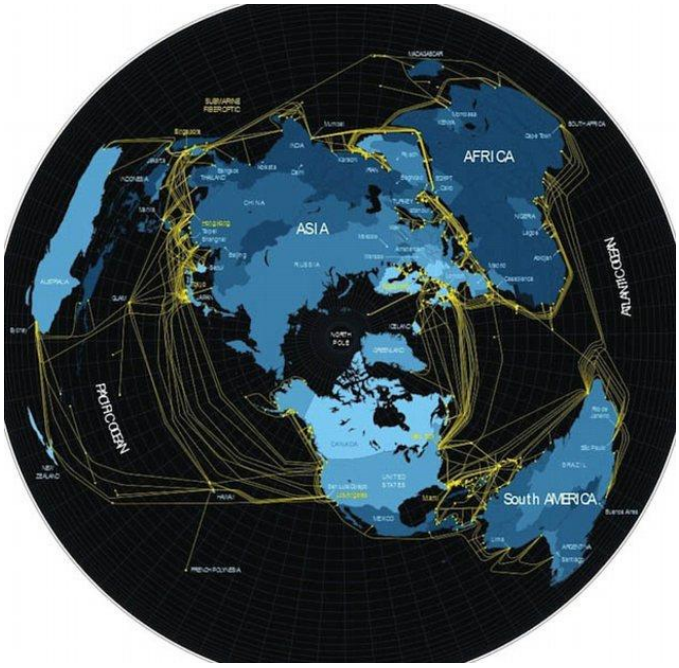
Para Manuel Castells el atentado 0911 en Nueva York fue el inicio de la primera guerra mundial del siglo XXI, la "guerra red", que busca imponer sus objetivos utilizando las únicas armas eficaces en su situación de inferioridad tecnológica y militar (Castells, 2002).

Asimismo, esa amplia interconexión de datos se da por medio satelital, terrestre e inclusive a través de cables submarinos. Esta interconectividad es el reflejo del surgimiento de un nuevo espacio (5to espacio) que se suma al terrestre, marítimo, aéreo y espacial, el ciberespacio que inclusive se manifiesta en aquellos por medios terrestres, marítimos, el campo electromagnético e, inclusive satelital.



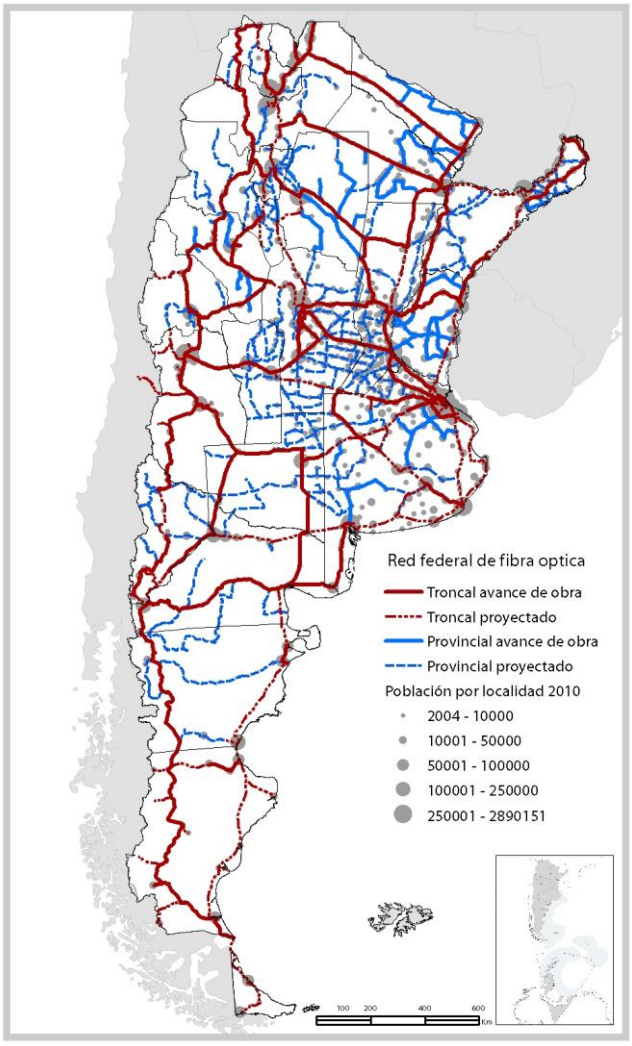
http://visualoop.com/media/2016/03/Submarine-Cable-Map-2016.jpg

Una visión geocéntrica de la misma se puede apreciar en mapas como:[6]



A modo de ejemplo y, para el caso terrestre, se puede apreciar la significación de la infraestructura de fibra óptica nacional en el siguiente mapa:[7]

[6] Tomado de: http://www.dailymail.co.uk/sciencetech/article-2175327/What-internet-really-looks-like--massive-sprawling-global-collection-wires-keeps-world-connected.htm
[7] Tomado de: http://atlasid.planificacion.gob.ar/atlas.aspx


Red federal de fibra optica
Troncal avance de obra
Troncal proyectado
Provincial avance de obra
Provincial proyectado
Población por localidad 2010
2004 - 10000
10001 - 50000
50001 - 100000
100001 - 250000
250001 - 2890151
100
200
400
600
km

2.2 Las Ciberguerras. Un debate doctrinario.

La era de la información posee un nuevo "espacio" informacional y una infraestructura "crítica" que lo soporta, demandando esfuerzos en igual sentido. Los nuevos conflictos de esta era han dado lugar a la denominada guerra de la información, donde se ataca el nudo o "nodo" que hace al control, la comunicación, administración, comercialización, etc., esto es, las redes informáticas y las infraestructuras que las soportan. No se trata solamente de poder atacar un pozo petrolero para evitar el flujo de combustible como era un ataque en la transición de la era industrial a la nueva era. Se trata de atacar un centro financiero, un sistema de comunicaciones gubernamental o infectar una red de computadoras vinculadas a la defensa, afectando así al sistema de una nación, desarticulando sus capacidades. Por tal motivo, las estrategias nacionales, bilaterales y multilaterales en esta materia se orientan hacia la identificación y protección de las infraestructuras críticas de cada nación y región en la faz pública y por medio de acciones conjuntas con empresas en lo privado.

Nicolás Arpagian, especialista en ciberseguridad, redactor de la revista francesa Prospectiva Estratégica y autor del libro "La Cyberguerre, la guerre numérique a commencé"[8] indica que fue Norbert Winer (1894-1964), profesor del Massachussets Institute of Technology (MIT) quien en 1964 creó el término "cibernética" al designar la disciplina que estudia el problema del control y la comunicación en general y William Gibson, autor de obras de ciencia ficción, quien desarrollará en 1984 el término "ciberespacio" como un lugar indefinido en el mundo que existe y donde millones de personas viven a diario.

Según el coronel de la Fuerza Aérea de EEUU, Richard Szafranski el concepto de estrategia militar desarrollado por el antiguo estratega chino Sun Tzu, al potencializarse por la tecnología informativa, se ha convertido "en las sofisticadas operaciones sicológicas de la guerra moderna" (Szafranski, 1999). El autor define a la guerra (warfare) como "el conjunto de todas las actividades letales y no letales emprendidas para someter la voluntad hostil de un adversario o un enemigo. En este sentido, guerra (warfare) no es sinónimo de guerra (war)" (Szafranski, 1999).

[8] Arpagian, Nicolás (2009). "La Cyberguerre, la guerre numérique a commencé", Ed. Vuilbert, París.

Para Szafranski, la guerra (entendida como warfare): no requiere la declaración de guerra; ni la existencia de una condición extensamente reconocida como un estado de guerra, puede ser comenzada por o contra un estado controlado, patrocinados por un estado, o grupos no estatales; es la actividad hostil dirigida contra un adversario o enemigo; su propósito no es necesariamente matar al enemigo, sino tratará de someterlo; su capacidad máxima es someter a un adversario sin eliminarlo; el adversario es así sojuzgado cuando se comporta de un modo coincidente con el que los agresores o defensores intentan imponerle. Así, en relación al impacto de las tecnologías de la información, John Arquilla y David Ronfeldt han establecido un nuevo concepto de "guerras controladas de información", donde en este nuevo tipo de guerras se intenta atacar el conocimiento o las creencias del adversario, dado que ambos afectan la adopción de decisiones humanas (Arquilla; Ronfeldt, 2001).

El gran objetivo de este nuevo tipo de guerra es la destrucción de las capacidades tecno-informacionales de los actores en la era postindustrial.

El especialista Martin Libicki, es quien ha expuesto la dificultad que supone formular una definición categórica en la materia debido a la existencia de siete tipos principales de Guerra de la Información (IW), cada uno de ellos con sus propias características:

- *Command and Control Warfare, C2W*: son las acciones contra y en defensa de las actividades de organización y mando de las fuerzas combatientes. Se trata de operaciones integradas para la destrucción de la capacidad de acción de las fuerzas, basadas en la destrucción o inhabilitación de su mando y de la cadena correspondiente.
- *Intelligence-based Warfare, IBW*: es la forma de combate basada en la rápida y efectiva adquisición de información inteligente, y en su uso efectivo inmediato.
- *Electronic Warfare, EW*: son aquellas acciones encaminadas al control del espectro electromagnético del enemigo o a su destrucción, mediante la utilización de energía propia.
- *Psychological Warfare, PSYW*: es uso de propaganda y otras acciones psicológicas para influenciar la moral y la percepción del enemigo, y fortalecer las propias.
- *Hacker Warfare*: son ataques a sistemas informáticos civiles con la finalidad de copiar, destruir, impedir el acceso o alterar la información contenida en ellos.

- *Economic Information Warfare, EIW*: es la aplicación de las tácticas y técnicas de la IW al campo de los intereses económicos.
- *Cyberwarfare*: es combate entre contendientes en un campo de batalla virtual, también se utiliza para designar futuras guerras robóticas (Arquilla y Ronfeldt, 2001).

Por su parte, Francois-Bernard Huyghe, especialista francés en ciencias de la información estratégica desarrollará la distinción entre:

- Ciberguerra (cyberwar – information warfare): que se orienta estrictamente a la conducción de operaciones militares según los principios relativos de los canales de información, tendientes a destruir o controlar los sistemas de comunicación del adversario y,
- Netguerra (netwar): corresponde a los conflictos a gran escala entre naciones o sociedades comerciales. En este caso el agresor va a buscar modificar o pervertir lo que una población civil (consumidores, opinión pública, electores, clientes, etc.) saben o creen de ella misma o del mundo que lo rodea [9] (Arpagian, 2009, pp 22 y 23).

Esta distinción es coincidente con la perspectiva estadounidense de John Arquila y David Ronfeldt, investigadores estadounidenses de la RAND Corporation, quienes en su clásico en la materia "Networks y Netwars" (Arquila, J y Ronfeldt, 2001) preparado para la Secretaría de Defensa de los EUA en 2001, analizan la agenda de los conflictos por desarrollarse en el ciberespacio producto de la globalización y los necesarios cambios organizacionales que se requerirán para enfrentarlos. En tal sentido asignaban una especial importancia a la defensa de las "infraestructuras tecnológicas" que las soportan (Ortiz, 2012).

Para el académico Joseph Nye, ex asistente al Secretario de Defensa de EUA, "la ciberguerra es una acción hostil en el ciberespacio cuyos efectos amplían o son equivalentes a una violencia física importante.

[9] Huyghe, François-Bernard (2001) *L'Ennemi à l'ère numérique: Chaos, information, domination,* Broché, Defense, París, tomado de Arpagian, Nicolas (2009). *La Cyberguerre*, Vuilbert, París.

En el mundo físico, los gobiernos ejercen prácticamente un monopolio en el uso de fuerza a gran escala, el defensor tiene un conocimiento íntimo del terreno y los ataques terminan como consecuencia del desgaste o del agotamiento. Tanto los recursos como la movilidad son costosos” (Nye, 2012). Nye entiende que países grandes como EUA, Rusia, Gran Bretaña, Francia y China tienen una capacidad mayor que otros estados y actores no estatales para controlar el mar, el aire o el espacio, pero casi no tiene sentido hablar de predominio en el ciberespacio, porque la dependencia de sistemas cibernéticos complejos para el respaldo de actividades militares y económicas crea nuevas vulnerabilidades en los estados grandes.

Nye expone que “en el mundo cibernético, los actores son diversos (y a veces anónimos), la distancia física es inmaterial y algunas formas de ataque son baratas. Como Internet estuvo destinada para facilitar el uso más que por cuestiones de seguridad, los atacantes actualmente tienen ventaja sobre los defensores. La evolución tecnológica, inclusive los esfuerzos por “reconfigurar” algunos sistemas para una mayor seguridad, llegado el caso puede cambiar esto, pero, por ahora, la situación sigue siendo así”.

Para Nye, el actor más importante posee la capacidad limitada para desarmar o destruir al enemigo, ocupar territorio o usar estrategias de contrafuerza de manera efectiva, pero en la ciberguerra, es la más dramática de las potenciales amenazas, donde los estados con recursos técnicos y humanos elaborados en principio podrían crear un trastorno masivo y una destrucción física a través de ciberataques contra blancos militares y civiles.

Por tal motivo, Nye expone que las respuestas a una ciberguerra deben incluir una forma de disuasión interestatal, capacidades ofensivas y planes para una recuperación rápida de las redes y la infraestructura si la disuasión fracasa.

Por ello, el referido Arpagian expone que “la ciberguerra irrumpió en nuestras sociedades para incrustarse en todos los campos, desde el militar hasta el civil. Las redes informáticas provocaron una suerte de extensión de los campos de batalla hacia un mundo virtual en plena interacción con la realidad”… “la ciberguerra pone en tela de juicio los fundamentos mismos de la forma de hacer la guerra. La ciberguerra obtiene resultados importantes a bajo costo. Es más barato movilizar 10.000 computadores que 10.000 soldados. La tecnología de las redes reequilibra la geopolítica” (Arpagian, 2011).

Así, Arpagian indica que insurgentes iraquíes el 18 de diciembre de 2009 lograron hachear sistemas de operaciones militares de los aviones Predator de los EUA por medio de un software informático que no cuesta más de 26 U$S.

El gran objetivo de este nuevo tipo de guerra (guerra - no guerra al decir de Alvin Toffler) es la destrucción de las capacidades informacionales y las infraestructuras críticas. Esta concepción de la guerra como no solo militar ha sido desarrollada en otras partes del planeta. Diversos documentos en EUA, Europa y otros países como India, Rusia y China, comienzan a conceptualizar estratégicamente sobre el tema y generar acciones. De este modo el espacio informacional y la infraestructura física crítica se encuentran en una concepción amplia que las interrelaciona estratégicamente (Toffler, 1994).

Asimismo, Maxime Pinard, Director de Ciberestrategia en el Instituto de Relaciones Internacionales y Estratégicas (IRIS) de Francia, expone que el término de ciberguerra no tendría sustento en ninguna realidad concreta, ya que "ciertamente hay ciberataques, pero no ciberguerra en el sentido de un conflicto entre, al menos, dos protagonistas identificados que causan daños humanos y económicos el uno contra el otro". Pinard, entiende que: "los ciberataques parecen nuevos cuando en realidad sólo corresponden a técnicas clásicas de sabotaje y perturbación de las comunicaciones del enemigo" donde "nos dirigimos hacia una militarización reforzada del ciberespacio con un riesgo certero de engranaje donde los cibernautas (simple usuarios) serán las principales víctimas"[10].

Por su parte, el contraalmirante Arnaud Coustillière, responsable de la ciberdefensa en el Ministerio francés de Defensa en 2014, expuso que "si podemos neutralizar los radares con el arma informática antes que con un misil, es mucho mejor", a la vez que rechaza suponer la existencia de una ataque desbastador en materia informática dado que "estamos tan globalizados que no lo creo. Sin embargo, un ataque catastrófico contra las infraestructuras vitales sí puede producirse"[11].

[10] URL: http://www.pagina12.com.ar/diario/elmundo/4-256329-2014-09-28.html
[11] Ídem 17.

T. Chand, Comodoro de la aviación de la Fuerza Aérea de India, en oportunidad de un encuentro indú-ruso para la cooperación en ciberdefensa, desarrollado a mediados de 2014 en el marco de la visita oficial del Presidente ruso Vladímir Putin a su par hindú Narendra Modi indicó que "la ciberguerra afecta a todo tipo de tropas" al señalar que India se encuentra creando un mando contra la ciberguerra y se requiere la cooperación bilateral[12].

Actualmente se generan cambios continuos en las estrategias militares, capacidades militares, cambios en las organizaciones, en las operaciones terrestres, y en los procedimientos militares. Estas guerras de "cero bajas" tienen distintos enfoques, pero todas incluyen un punto: el impacto de las tecnologías de la información en el campo militar.

Recientemente, el Consejo de Seguridad de las Naciones Unidas, mediante la resolución 1113 del 2011, definió a la "guerra cibernética", como:

- el uso de computadoras o medios digitales por un gobierno o con el conocimiento explícito o la aprobación de ese gobierno contra otro Estado, o propiedad privada dentro de otro Estado incluyendo:
- el acceso intencional, interceptación de datos o daños a la infraestructura digital y a la infraestructura controlada digitalmente la producción y distribución de dispositivos que pueden usarse para subvertir la actividad interna (CEDN, 2015).

2.3 Características de una guerra cibernética

La Guerra Cibernética se caracteriza por ser eminentemente asimétrica y, asimismo, no debe confundírsela con Guerra Electrónica. El modelo de interconexión ISO - OSI define la existencia de siete capas conceptuales cuando dos o más computadores interactúan entre sí, a saber: capa Física, de Datos, de Red, de Transporte, de Sesión, de Presentación y de la Aplicación. Así, mientras que Guerra Electrónica "incumbe el uso de niveles de la referencia cercanos a la capa Física y se corresponde con los ámbitos "tradicionales" de los conflictos: tierra, mar y aire; la "Guerra Cibernética" se

[12] Ídem 17.

desarrolla en un nuevo ámbito de las hostilidades entre estados-naciones: El Ciberespacio (Uzal, 2012, pp 40).

Dado que la ciberguerra utiliza todas las herramientas electrónicas e informáticas para afectar y/o destruir los sistemas electrónicos y de comunicación del enemigo, manteniendo seguros los propios, sus principales características serían:

- complejidad,
- asimetría,
- objetivos limitados,
- corta duración,
- menos daños físicos para los soldados,
- mayor espacio de combate y menor densidad de tropas,
- transparencia,
- lucha intensa por la superioridad de la información, aumenta la integración,
- mayores exigencias impuestas a los comandantes,
- nuevos aspectos de la concentración de fuerzas, reacción rápida, e igual de devastadora que una guerra convencional (Gema Sánchez Medero, 2010).

Algunos autores han descripto a la ciberguerra dentro del ciberespacio como el quinto dominio de la guerra junto a la tierra, el mar, aire y el espacio, entendiendo que los avances tecnológicos ponen en riesgo a los ejércitos y a la sociedad debido a los ciberataques

Asimismo, un interesante estudio realizado en Chile, aprecia como las operaciones en el ciberespacio mantienen igualmente los principios de la guerra:

- Objetivo: dirigir los ataques informáticos hacia un objetivo claramente definido.
- Ofensiva: capturar, retener y explotar la iniciativa.
- Masa: sincronizar todos los elementos (programas o virus) de poder y concentrarlos donde tengan un efecto decisivo sobre el objetivo, en un corto período de tiempo.
- Economía de fuerzas: distribuir los medios informáticos de manera efectiva.
- Maniobra: movimiento de los medios informáticos que permitan lograr una ventaja frente al objetivo, haciendo que el enemigo pierda el equilibrio y lograr que sus acciones sean inefectivas frente a los ataques.

- Unidad de mando: los ataques informáticos generalmente son liderados por una persona responsable de ellos, el que posee la autoridad para coordinar y dirigir todos los medios hacia un propósito único.
- Seguridad: los ataques informáticos poseen medidas que protegen a los autores y los medios utilizados, permitiendo eliminar los rastros dejados en la web, tanto de los equipos como de los códigos.
- Sorpresa: los ataques informáticos se realizan en un momento, lugar o de una manera en que la víctima no está preparada, lo que puede cambiar decisivamente el equilibrio. Esto se logra buscando las vulnerabilidades de los sistemas mediante el ciberespionaje.
- Simplicidad**:** en informática los medios por los cuales se realizan los ataques son simples programas con códigos sencillos pero letales, siendo esta simplicidad lo que permite el éxito de las operaciones de ataques informáticos (Gómez Abutridy, 2014).

2.3 Estudios militares en Argentina sobre ciberdefensa[13].

La Guerra de las Malvinas – Conflicto del Atlántico Sur (CAS) (1982) fue el bautismo de fuego del Arma de Comunicaciones del Ejército en operaciones convencionales donde se manifiesta la "Revolución de la Informática" aplicada al avance de las telecomunicaciones como inicio de los sistemas de información hasta llegar a los desarrollos de C4ISR (comando y control, comunicaciones, computadoras, información, observación y reconocimiento). En ese escenario de conflicto se presentó claramente la presencia de acciones de guerra electrónica (Arcangeles, 1983). En 1982 las lecciones aprendidas de la guerra de 1973 en Medio Oriente clarifican las diferencias entre Guerra Electrónica y Contramedidas electrónicas.

A fines del siglo XX se realizan las primeras evaluaciones 1990-1999 como resultado del impacto de las Tecnologías de la Información en el campo militar terrestre donde se apreciaba la videncia de un Sistema Único de comunicaciones, conformado por distintos subsistemas integrados de modo físico y electrónico orientados a la tecnología

[13] Parte de este relevamiento fue presentado en el Seminario Internacional Informations Operations del US Foreign Military Studies Office (FMSO), Escuela de Comando y Estado Mayor del Ejército de EEUU, desarrollado en Sep 2007 en Ft Leavenworth Kansas durante la exposición del J.U. Ortiz.

satelital. Se procuraba desarrollar un sistema informático de forma modular y acciones de seguridad informática desde la Dirección General de Comunicaciones e Informática del Ejército. La Red digital de Integración de Sistemas del Ejército comenzó a ser la respuesta a las necesidades planteadas en el pasado.

Actualmente en la Escuela Superior Técnica, dependiente del Instituto Universitario del Ejército Argentino, se dicta la carrera de Ingeniería en Informática, de la que son cursantes civiles y militares se especializan en aspectos que hacen a la seguridad informática mediante cursos de post-grado como "Especialista en Criptografía y Seguridad Teleinformática".

Esta Especialización está destinada a profesionales Ingenieros, Licenciados en Electrónica, Informática o Sistemas de Información. Es objetivo general de la Especialización es el de posibilitar a los graduados en informática, telecomunicaciones y electrónica el conocimiento y la profundización de los conceptos fundamentales que hacen a los sistemas de seguridad utilizados para resguardar la información. Incluye, además, las herramientas teóricas y prácticas que es necesario utilizar, tanto durante su procesamiento, como durante la fase de transmisión.

Asimismo, la Escuela de Comunicaciones y la Escuela Superior Técnica del Ejército (EST) desarrollan cursos de capacitación en materia de seguridad informática y de las comunicaciones, guerra electrónica, etc. Estas capacidades también se encuentran en los institutos de formación de la Armada Argentina y en la Fuerza Aérea Argentina.

En materia de seguridad informática, la EST ha participado activamente en la organización de Congresos Nacional e Internacional de Seguridad en Sistemas Teleinformáticos y Criptografía (CONSECRI). Cabe destacar que Argentina desde el año 2000 es sede para América del Sur de la Asociación Internacional de Comunicaciones Electrónicas de las Fuerzas Armadas (AFCEA Internacional), como organización civil sin fines de lucro, que reúne a especialistas en temas de C4ISR (Comando, Control, Comunicaciones, Computación, Información, Vigilancia y Reconocimiento).

Ha desarrollado seminarios con apoyo de organismos nacionales con responsabilidad en seguridad en la red en Guerra y Operaciones de Información, Ciberataques, Protección de Datos y Libertad de Información, Seguridad física de los sistemas, etc.

En la Escuela Superior de Guerra "Tte Gral. Luis María Campos" (ESG) del Ejército Argentino funciona el Adiestrador Táctico (ADITAC) que es un sistema constituido por personal y equipos que permite, actuando en forma integrada, adiestrar o entrenar al personal mediante un software de simulación. El objetivo del ADITAC es adiestrar a los comandantes, Jefes de Planas Mayores, en los procesos de toma de decisiones enmarcados en situaciones simuladas que ocurren en tiempo real.

En los últimos años, en la ESG se han desarrollado diversos estudios militares sobre el tema. De ellos se destacan las siguientes apreciaciones:

2.4 La Estrategia Cibernética.

Según Enrique Stel, Oficial de Comunicaciones y Veterano de la Guerra de Malvinas, para alcanzar "el poder en el ciberespacio, se requiere de un Estrategia Cibernética; organizar la Fuerza Cibernética; desarrollar las Caber-armas que esa estrategia particular requiera" y adecuar la normativa jurídica nacional e internacional a esta nueva realidad. El espacio cibernético donde se desarrollan las "operaciones cibernéticas" no está delimitado por el tradicional teatro de operaciones o guerra, por lo cual se amplía su radio de acción y tiempo (Stel, 2005).

2.5 Las Guerras del futuro.

Jorge Manuel Cerezo, Oficial del Ejército Argentino, afirma que las guerras del futuro serán GI, los ejércitos modernos deben proteger la información y las redes propias y penetrar y apoderarse de la información o destruir las redes del adversario en el nuevo campo de batalla, el ciberespacio (Stel, 2005).

2.6 El dislocamiento estratégico operacional.

Roberto Pritz, ex Director de la Escuela Superior de Guerra "Tte Gral Luis M. Campos", estima que el "dislocamiento estratégico operacional" es una situación que se logra por medio de la aproximación directa o indirecta sobre la fuerza enemiga producto del desequilibrio de su dispositivo, desarticulación de su comando, afectación de su moral y de la capacidad de maniobra y obtención de sus líneas de menor resistencia y expectativa. Entre otras condiciones para lograrlo se requiere desarticular el comando del enemigo, desquilibrar sus fuerzas, afectar su moral y capacidad de maniobra, desorganizar sus abastecimientos y afectar sus líneas de comunicaciones. En las nuevas guerras de la información y ciberguerras este “dislocamiento” se alcanza por medio de capacidad tecnológica, informática y digital. El objetivo es desarticular el comando enemigo antes y con mayor énfasis mediante las operaciones de guerra de la información (Prtiz, 2005).

2.7 Las amenazas a la infraestructura de información nacional.

Hugo L. Cargnelutti, vocal de la Comisión del Arma de Comunicaciones y miembro de AFCEA Argentina, entiende que es necesario aplicar la teoría sistémica de Warden de los "cinco anillos estratégicos" para realizar GI estratégica, atacando el "sistema de sistemas" C4ISR mantener con TI la capacidad de comando y control (C2). (Cargnelutti, 2002) Las amenazas a la infraestructura de información nacional son muy reales, no tradicionales y altamente diversificadas por lo cual es necesario desarrollar conceptos operacionales y estructuras organizativas que les permitan, ser capaces de luchar a fin de obtener la superioridad en este nuevo ámbito y también poseer la habilidad suficiente para combatir en ese ámbito, tomando ventaja de los errores que el adversario cometa en el espacio de información, concluye.

2.8 Los objetivos básicos de la Seguridad Informática militar

Fabian Calvete, Oficial Ingeniero Militar en Informática de la Escuela Superior Técnica aprecia que la seguridad informática militar debe cumplir con cuatro objetivos básicos: confidencialidad de la información, integridad del mensaje, confiabilidad o autenticidad y disponibilidad. Para aplicar la guerra informática en forma puramente ofensiva, el oficial entiende que se necesita formar elementos con profesionales que puedan penetrar en las redes del enemigo u oponente y como medida de control y supervisión, para testear nuestras medidas defensivas Estas organizaciones deben estar como mínimo formando parte de la GUC (Gran Unidad de Combate). Serían los "crackers" del ejército en situaciones de conflicto.

Luego el "escuadrón de asalto", compuesto por soldados altamente entrenados, romperá las defensas del enemigo para identificar usuarios válidos en sus sistemas, obtener acceso, escalar privilegios en el sistema, creando "nuevos huecos para poder desplazarse, ocultar cualquier evidencia de su presencia" y, obtener, alterar o destruir la información u operación del sistema. Esta será una guerra con bajas principalmente materiales (Machiandiarena, Tabeada y Gaidano, 2003).

2.9 La Guerra Cibernética en la Defensa Nacional.

Para Roberto Uzal, Oficial retirado del Ejército Argentino, ingeniero militar y doctor en Administración (FCE-UB), experto en sistemas siendo Director de la Maestría en Ingeniería de Software y Director del Doctorado en Ingeniería de la Universidad Nacional de San, "una de las situaciones más desfavorables por las que puede pasar un país es la de recibir Ataques Cibernéticos y, por incapacidad Tecnológica, terminar adjudicando los desastres ocasionados por dichos ataques a accidentes impredecibles". Para Uzal, el Crimen Cibernético y Terrorismo Cibernético no son "extrapolables" a Guerra Cibernética, en ningún aspecto: ni en su naturaleza, ni en lo tecnológico o en los aspectos legales / institucionales ni tampoco en el "gerenciamiento" / liderazgo así como tampoco en las potenciales consecuencias. Para Uzal, "los aspectos de la Guerra Cibernética deben ser encarados con criterio de Defensa Nacional" ya que la Guerra

Cibernética “consiste en adquirir capacidad de defensa ante agresiones que pueden ser más graves que un ataque nuclear al territorio nacional y la posibilidad de poder “neutralizar” la fuente emisora de dichas agresiones”.

Asimismo, expone que “se deberían definir claramente las “reglas de involucramiento” de los recursos asignados a la Guerra Cibernética” donde la “distancia” entre las máximas autoridades gubernamentales de las unidades de Guerra Cibernética deben ser la mínima posible.

Expone que hay que generar recursos humanos aptos para este nuevo tipo de guerra, especialmente a nivel gerenciamiento y todo ello, a partir de una alianza estratégica con Brasil “para mantener el control de Ciberespacio a nivel regional”, entendiendo que la “Guerra Cibernética debería ser un tema de permanente estudio, reflexión y propuestas representando el mayor desafío a ser encarado por el área de Defensa” (Uzal, 2012, pp 41 a 47).

2.10 Los desafíos Operacionales en el espacio cibernético como nuevo campo de lucha.

El Oficial de la Fuerza Aérea Argentina Exequiel Rodríguez Cisneros, expone que la nueva realidad de la informática, el Ciberespacio, crea condiciones de vulnerabilidad y plantean desafíos en materia de seguridad y defensa, lo que demanda nuevos instrumentos militares y fuerzas adiestradas al respecto. Esos desafíos demandarán:

– Desarrollar una fuerza de cibercombatientes para el trabajo interdisciplinario,

– Establecer una estructura de conducción de las operaciones ciberespaciales,

– Redefinir algunos aspectos del arte operacional,

– Propiciar la investigación y el desarrollo tecnológico para obtener capacidades ciberespaciales.

– Establecer nuevas estrategias de protección de las infraestructuras críticas.

– Definir los actos de guerra cibernética.

–Actualizar la legislación vigente para especificar las agresiones en el Ciberespacio, y el derecho del Estado a su legítima defensa.

– Capacitar y concientizar a todos los integrantes del Sistema de Defensa (Rodríguez Cisneros, 2012).

2.11 Los lineamientos para la seguridad cibernética en Teatro de Operaciones

Daniel Giudici, Oficial de la Armada Argentina, entiende que la Ciberguerra constituye una amenaza asimétrica, porque un ataque cibernético no reconoce límites y sus perpetradores generalmente operan de manera anónima pudiendo afectar núcleos de importancia para el funcionamiento de un Estado. En tal sentido, el dominio de las Fuerzas Armadas en un Teatro de Operaciones requiere estructuras orgánicas con adecuado personal para defenderse de un ataque cibernético.

Por tal motivo, para Giudici, surge la necesidad de identificar herramientas informáticas para el empleo defensivo contra potenciales agresiones cibernética, apreciando que la dependencia tecnológica aumenta la probabilidad de sufrir ataques cibernéticos. Así, se requiere de estructuras orgánicas que aseguren el intercambio de datos, con personal capacitado que procure alcanzar los requisitos mínimos de seguridad para la interoperabilidad, asegurando de manera confiable la defensa homogénea del sistema de información a partir de un manual de procedimientos y accionar conjunto para el manejo de la información y de la seguridad cibernética que facilite las coordinaciones, e interoperabilidad de las fuerzas desplegadas en un Teatro de Operaciones (Giudici, 2013).

2.12 La Ciberguerra como amenaza a los sistemas de defensa integrados y basados en redes del Teatro de Operaciones.

Sergio D. Miranda, Oficial de la Fuerza Aérea Argentina, entiende que un teatro de operaciones moderno se destaca por la presencia en el Puesto Comando de sistemas integrados en redes para tener rapidez y precisión en la toma de decisiones en tiempo real a los efectos coordinar las fuerzas y el accionar conjunto de los medios para mantener el ritmo de batalla y tener iniciativa en el enfrentamiento. Por tal motivo surgen del

oponente los ataques en el ciberespacio para penetrar las redes más seguras, sustraer información y/o bien modificarla. Por tal motivo, se requieren medidas para incrementar las capacidades de ciberdefensa en estas redes a partir de una organización necesaria con personal capacitado y con equipos móviles coordinados desde un Centro de Emergencia y Respuesta Rápida que detecte las vulnerabilidades (Miranda, 2014).

2.13 La Guerra Cibernética en el nivel operacional.

Para Eduardo Paez, Oficial de la Armada Argentina, la Guerra Cibernética en el Nivel Operacional requiere una organización y funcionamiento de los distintos servicios de informática de las tres Fuerzas Armadas de modo interrelacionados en un Comando Conjunto de Ciberdefensa con capacidades para operar con efectividad en un escenario virtual frente a amenazas cibernéticas para mantener la capacidad de las operaciones militares en un Teatro de Operaciones (Paez, 2014).

2.14 La ciberguerra y el Derecho Internacional de los Conflictos Armados (DICA).

Héctor Flores, Oficial retirado del Ejército Argentino, Doctor en Ciencia Política y profesor de la Escuela de Defensa Nacional, entiende que "dentro del amplio espectro de los desafíos que implica el diseño de FFAA, las relacionadas al ciberespacio son quizás las más trascendentes por configurar un ámbito nuevo, con escasas normas internacionales específicas respecto a su de empleo y donde lo científico tecnológico impacta y modifica día a día las bases de proyección de fuerzas". Para Flores, las armas o los medios de guerra "no pueden evaluarse en forma separada al método de guerra con el que se prevé utilizar". Debido a ello, la licitud de un arma "no depende solo de su diseño o de su fin previsto, sino también de la manera que se prevé utilizarla en el campo de batalla".

Flores entiende que esta nueva forma de guerra no solo plantea desafíos de orden práctico para las FFAA sino sino también de orden jurídico, dado que "la guerra es un hecho de naturaleza política, ajustada al derecho a la legítima defensa ante una agresión

externa estadual de otra/s FFAA y al Derecho Internacional Humanitario (DIH) – Derecho Internacional en los Conflictos Armados (DICA)". Aunque no exista disposición en el DIH en la materia, Flores refiere a Michael, Schmitt quien expone que "los ataques a través de redes informáticas están sujetos al derecho humanitario si forman parte de un conflicto clásico o de una ciberguerra con la intención de causar muertos, heridos, daños o destrucción, o en la que sea previsible que los haya" (Schmitt, 2002).

En tal sentido, Flores expone que "la XXVIII Conferencia Internacional de la Cruz Roja y de la Media Luna (Ginebra del 28 de noviembre al 1º de diciembre 2003), reafirmó, por consenso, el objetivo de garantizar "la licitud de las nuevas armas de conformidad con el derecho internacional", en vista "del rápido avance tecnológico de las armas y con el objeto de protegen a la población civil de los efectos indiscriminados de las armas y a los combatientes de los sufrimientos innecesarios y las armas prohibidas". Así, "la licitud de un arma no depende solo de su diseño o de su fin previsto, sino también de la manera que se prevé utilizarla en el campo de batalla" (Flores, 2015, pp 1 a 19).

2.15 El ciberespacio como espacio geopolítico y el rol de las FFAA.

Julio G. Lucero, Oficial de la Fuerza Aérea Argentina, Ingeniero de Sistemas y Magíster en Administración de Sistemas de Información entiende que "como espacio geopolítico, el ciberespacio puede dar lugar a teorías y conceptos de la ciencia geopolítica". Así, se puede asociar la proyección estratégico-espacial argentina en la virtualidad de interés nacional, al desarrollo tecnológico, donde "el ciberespacio es un nuevo escenario que tiene características propias y distintivas que obligan a una adecuación de los protocolos existentes para operar con éxito en él". En este escenario "un ciberconflicto está caracterizado por su originalidad desafiante y dinámica, lo que lleva a un proceso continuo y perseverante de aprendizaje para lograr y mantener efectividad", siendo un Comando Conjunto Cibernético el principal responsable en tal sentido.

Asimismo, se requiere la "Ocupación Científica del Espacio", que otorgue "una posición relativa favorable de la región, tanto para la discusión de la gobernanza del

ciberespacio, como también para el ingreso a un universo de oportunidades posibles para las futuras generaciones que tiene como límite solo la imaginación”. En tal sentido, Lucero estima que el Plan Nacional de Ciencia, Argentina Innovadora 2020, “genera un marco estratégico, político y social propicio para avanzar en la vinculación de Ciencia, Tecnología, Defensa y Desarrollo Económico”.

Por su parte, desarrollar “una estructura de defensa en el Ciberespacio no implica un obligado atentado a las libertades individuales, ya que tecnológicamente es posible ejercer una protección efectiva y de acuerdo a normas legales si se limitan los trabajos a los estratos de la “Nube” que no involucran la información privada, es decir, si se trabaja sobre las capas: Física, Datos y Red del modelo OSI-ISO28. Conceptual y operativamente se podría considerar al ciberespacio como un macro sistema en el cual, a través de diferentes tecnologías, los estados deberían controlar y supervisar las acciones que se efectúan de forma tal de saber si se ajustan a derecho, acuerdos sociales y/o comerciales y, a su vez, para corroborar que no amenazan los intereses nacionales”.

En este marco, para Lucero, “las fuerzas armadas, por el poder que administran, son comandadas por el Jefe de Estado. Representan la última herramienta para asumir la defensa de la nación contra un enemigo militar externo. Son instrumentos que el estado tiene a su disposición para ejercer la plena defensa de sus intereses vitales. Como parte del Estado Argentino y subordinado a sus autoridades legítimas, ocupan el rol definido por éstas en la temática tratada. No obstante, la tarea ya asignada de brindar seguridad a sus sistemas de información propios puede ser complementada con un estado de Alerta Estratégico, en el marco de una Actitud Estratégica netamente defensiva, a los efectos de colaborar en lograr un oportuno tiempo mínimo de reacción ante los ataques a los sistemas críticos. Sólo una estrategia creativa e integral permitirá neutralizar los efectos perjudiciales de las acciones irregulares en el Ciberespacio” (Lucero, 2015, pp 26 a 42).

2.16 Principales ciberataques en los últimos años

Diversos hechos confirman el surgimiento de los ciberataques en la agenda de defensa y seguridad internacional. De los que se destacan, en lo que va del nuevo siglo XXI, entre otros, los siguientes:

2000. En mayo se detecta el virus I Love You, que causó daños por más de 10.000 millones de dólares en el mundo entero

2003. En enero, expertos desactivan el virus Slammer que ralentizó internet en Europa y América del Norte y cortó de la red otras regiones, en particular, Corea del Sur.

2004. A ppios de mayo, un nuevo virus, denominado Sasser, ataca a infraestructuras de Italia infectando decenas de miles de computadoras y afectando en normal funcionamiento de Correos y Ferrocarriles.

2005. El 16 de agosto un virus atacó varios medios y bancos estadounidenses.

2007. En mayo el sistema informático de Estonia es atacado por Internet en un equivalente a la utilización de un millón de computadoras. Estonia queda paralizada durante varias semanas y requerirá la ayuda de la OTAN para recomponer sus sistemas. James Appathurai, vocero de la NATO expresó sobre el ataque que esta situación "no es de tanques y artillería" y tras la reunión de los Jefes de la OTAN a mediados de junio de ese año sintetizó en que "todos estuvieron de acuerdo en que es imprescindible mejorar la capacidad de protección de los sistemas informáticos de importancia crítica".

2008. Coincidiendo con la operación militar rusa en Georgia, varias webs gubernamentales de este país son atacadas con el troyano BlackEnergy, paralizando sistemas informáticos y tomando el control de la web del presidente georgiano. Asimismo, en diciembre trasciende que el virus denominado Conficker infectó desde ese entonces y hasta abril del 2009, más de 12 millones de computadoras británicas afectando los sistemas de buques de la Armada y el Parlamento. Asimismo, se da a publicidad que un hacker habría coordinado un ataque que logró robar información de 130 millones de tarjetas de débito y crédito de Heartland Payment Systems, empresa multinacional de pagos. Se efectúan este año en torno a la denominada Guerra de Georgia, ciberataques entre fuerzas rusas y georgianas.

2009. Soldados estadounidenses desplegados en Irak capturaron a combatientes de un grupo chiíta rebelde con computadoras portátiles con imágenes tomadas por los aviones robot ‘Predator’. Según expertos, habían tomado el control del sistema informático de transmisión de las imágenes del avión.

El 30 de marzo el portal letón Chas informó que el programa espía GhostNet atacó las páginas de los ministerios de Exteriores de Bangladés, Barbados, Brunéi, Bután, Filipinas, Indonesia, Irán y Letonia. El diario afirmó también que los espías electrónicos dejaron “huellas” en embajadas de Alemania, Chipre, Corea del Sur, India, Indonesia, Malta, Pakistán, Portugal, Rumania, Tailandia y Taiwán. El 8 de abril The Wall Street Journal informó de que hackers rusos y chinos atacaron sistemas que controlan las redes eléctricas en territorio estadounidense probablemente para introducir programas que podrían producir cortes en caso de una crisis o una guerra. El 21 de abril el periódico The Wall Street Journal comunicó que ciberdelincuentes consiguieron violar el sistema informático del Pentágono y robaron la información sobre el nuevo caza de quinta generación Joint Strike Fighter, también conocido como F-35 Lightning II. Según los expertos, los datos se podrían utilizar para elaborar sistemas de defensa contra el avión. El 8 de julio las autoridades de Corea del Sur informaron de un ataque contra páginas de las instituciones y bancos del país.

El 21 de diciembre la televisión Fox News informó de que el FBI comenzó a investigar el robo de decenas de millones de dólares a Citigroup y que las sospechas del crimen recaían sobre hackers rusos. Este año se detectan ciberataques contra los gobiernos de EUA y Corea del Sur al mismo tiempo.

2010. En junio un programa Stuxnet, creado específicamente para tomar control de sistemas que manejan las operaciones internas de plantas industriales ataca a varios países, afectando miles de sistemas informáticos de automatización industrial utilizados en plataformas petroleras, oleoductos, centrales eléctricas y nucleares. Se ven afectados Pakistán, India, China (afectando a 6 millones de PC), Indonesia (18% de los ataques), EUA (2%) y en Irán (66%). Se estimó que el control de daños llevó hasta dos meses.

En tal sentido, a fines de septiembre de ese año Mahmud Liayi, responsable de tecnología informática del Ministerio de Industria iraní expresó que “una guerra electrónica fue lanzada contra Irán“, afectando a 30.000 computadoras en el país, entre

ellas el equipo de la central nuclear de Bushehr, inaugurada un mes antes. En noviembre y diciembre Anonymous organizó una serie de ataques DDoS contra compañías y organizaciones que se oponían a la actividad de Wikileaks, en particular PayPal, Visa, Mastercard. Durante 2010, desde Japón y Corea del Sur, se efectúan simultáneamente ciberataques a distintos ámbitos gubernamentales de ambos países.

2011. En enero los sistemas de contraseñas del ministerio de Finanzas de Canadá fueron víctimas de un ciberataque procedente de máquinas instaladas en China. De acuerdo al Norton Cybercrime Report 2011, el gasto anual mundial en ciberseguridad alcanzó los US$ 114 mil millones. A fines de octubre, se conoce la aparición de un nuevo malware detectado en Irán, Sudán, Francia, Vietnam, India, Suiza, Holanda y Ucrania, llamado *Duqu*, creado para realizar espionaje industrial y no para arruinar físicamente sistemas industriales y entendido como precursor de un futuro Stuxnet, dado que la información que recolecta sería usada para un nuevo ataque más poderoso. En junio, el grupo bancario Citigroup informó de un ataque a una base de datos de tarjetas en EUA que afectó a 360.000 personas. En marzo, piratas violaron la red informática de la República Sudafricana, sucursal de la empresa EMC, obteniendo información sobre la tecnología SecurID que se utiliza para proteger redes en el mundo.

2012. A fines de mayo se supo que Anonymous logró acceder al servidor del Ministerio de Justicia de Estados Unidos donde estaban almacenados datos sobre todos los crímenes cometidos en territorio estadounidense.

El mismo mes, expertos de la empresa rusa Kaspersky y la Unión Internacional de Telecomunicaciones anunciaron que detectaron el programa maligno Flame destinado a atacar ordenadores de instituciones públicas de Irán y otros países de Oriente Próximo y, probablemente, desarrollado por servicios secretos de EUA e Israel. El 12 de junio varios medios rusos declararon que fueron víctimas de un ataque DDoS realizado por una red de 133.000 ordenadores infectados.

La noche del 28 de noviembre una organización iraní de hackers, Parastoo, atacó uno de los servidores del OIEA y publicó las direcciones de correo de cien empleados exigiendo que firmaran una petición para investigar la actividad nuclear de Israel.

El 21 de diciembre, en India, piratas consiguieron acceder al sistema de la operadora de tarjetas prepago Visa y MasterCard en ese país y extrajeron 5 millones de

dólares en 4.500 cajeros automáticos. A mediados de febrero de 2013, y luego de atacar también a una operadora estadounidense, se apropiaron de 40 millones de dólares realizando 36.000 transacciones. Se conoce como Gauss troyano, a una operación de espionaje informático que extrajo ese año datos confidenciales de miles de sistemas informáticos situadas en Medio Oriente: Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí y Egipto.

2013. En marzo se efectuó uno de los mayores ataques DDoS que ralentizó el funcionamiento de internet en varios países europeos. La página de la organización Spamhaus que lucha contra correos basura fue el principal objetivo de los piratas. El 14 de abril, el día de las elecciones presidenciales en Venezuela, hackers desconocidos agredieron la cuenta de Twitter de Nicolás Maduro informando sobre supuestos fraudes. El 23 de abril se violó la cuenta de Twitter de la agencia AP donde se publicó una información falsa sobre dos explosiones en la Casa Blanca en que el presidente Obama resultó herido. El 26 de julio un ciberataque afectó los sitios de doce instituciones públicas y la Bolsa de Venezuela. De la agresión se responsabilizaron Anonymous Venezuela y Venezuelan Hackers. En junio el FBI y Microsoft realizaron una operación conjunta para desmantelar una de las mayores redes de cibercrimen que infectó unos 1.000 ordenadores para cometer fraudes por más de 500 millones de dólares.

El 29 de julio Anonymous violaron las páginas del presidente y varias instituciones de Perú. El 7 de agosto piratas violaron la página en alemán y del centro ruso de prensa de RIA Novosti publicando información falsa sobre la muerte de Mijaíl Gorbachov. La agencia sufrió también ataques DDoS en mayo y julio de 2013. En septiembre se dio a conocer de un ataque contra sistemas de la oficina del primer ministro belga Elio Di Rupo así como a la infraestructura informática del Ministerio de Relaciones Exteriores de Bélgica.

El 28 de octubre los hackers violaron las cuentas Facebook y Twitter del presidente de EUA, Barack Obama, pero no consiguieron controlarlas. El 26 de octubre se registraron 25 intentos de ataque a la red de electricidad hidroeléctrica de la ciudad de Chicago. El 8 de noviembre quedaron vulneradas las páginas del Presidente de

Singapur después de que las autoridades del país anunciaran medidas contra el grupo de hackers Anonymous.

En marzo, se detecta que una empresa rosarina que desarrolló un videojuego sobre una “guerra” en las Islas Malvinas, que es furor en la red, denunció que recibió ataques cibernéticos a sus servidores desde el Reino Unido, los cuales se repitieron varias veces y, conforme indicó su directivo: “la magnitud de la embestida superaba los 2 gigabits por segundo, incluso llegando a picos de 5 gigabits por segundo”. “Haciendo una analogía, sería el tráfico aproximado de unas 5 mil computadoras hogareñas conectadas a internet en forma simultánea”.

2014. El 29 de julio hackers del grupo Ciberberkut, creado después de la disolución de las fuerzas especiales ucranianas Berkut, bloquearon con un ataque DDoS por casi 24 horas la página del presidente de Ucrania, Petró Poroshenko, a quien acusaron de “genocidio de su propio pueblo”. Asimismo, el 10 de julio, The New York Times informó que piratas chinos atacaron en marzo el archivo de la Oficina de Administración de Personal de Estados Unidos obteniendo datos sobre funcionarios que solicitaron información clasificada. En septiembre de ese año, se filtran a la opinión pública, luego de obtener las claves, fotos personales íntimas de celebridades, especialmente de EUA, alojadas en la nube. A finales de 2014, un ataque lanzado contra una planta de acero alemana provocó daños físicos, de acuerdo con un reporte de la Oficina Federal para la Seguridad de la Información de Alemania.

2015. El 3 de abril la página web del Servicio de Radio de las Islas Malvinas (FIRS bajo el nombre británico de las Malvinas), fue hackeada para mostrar un video con el himno argentino e imágenes de la guerra entre Argentina y Reino Unido por la soberanía del archipiélago. Junto al video, la web se mostraron leyendas: "#LasMalvinasSonArgentinas", "transmisión interrumpida" y "hackeada por Líbero".

Asimismo, la página del Comité de Cuentas Públicas (PAC) de las islas sufrió un ataque similar. Posteriormente el hacker denominado Libero anunció que “voy a interrumpir la radio de las islas y poner el Himno Nacional". En torno a las operaciones por el control ruso de Sebastopol en Ucrania, trascendió la serie de ciberataques a las fuerzas ucranianas estacionados en esa región.

Ataque a la empresa Sony. Este ataque en concreto produjo daños por valor de 100 millones de dólares, y se comprometieron 100 Tb de datos. Asimismo, en 2015, la Oficina de Administración de Personal de Estados Unidos recibió un ciberataque que dejó sin protección los datos confidenciales de más de 20 millones de personas, entre ellos personal militar y dando a conocer sus números de la seguridad social, contraseñas, usuarios, así como sus huellas dactilares. Aparentemente el ataque provenía de servidores chinos. Asimismo, ese mismo año, Hacking Team, una controvertida firma de software italiana, popular por suministrar de forma legal herramientas de espionaje e intrusión remota como spyware y malware sufre un ataque. Cabe destacar que entre sus clientes figuran agencias de inteligencia y gobiernos. La compañía sufrió un ataque donde se han filtrado a la red 500 Gb de datos confidenciales. En abril se efectúa un ataque a la empresa francesa TV5, afectando 10 canales, el cual es adjudicado a miembros del ISIS. En diciembre unos 100 millones de usuarios visitan mensualmente las páginas web de la BBC apreciaron un ciberataque a sus páginas, lo que afectó el servicio temporalmente. Para mediados de 2015 se estima que el ISIS, con presencia en Siria e Irak, posee 60.000 "ciber"- seguidores que retwitean los mensajes del grupo terrorista. Asimismo el propio ISIS posee un sistema de ciberdefensa en sus instalaciones en Raqqa, Siria, desde donde también ataca sistemas militares occidentales. Asimismo, si bien no se puede considerar totalmente como ciberataque, cabe destacar que entre fines de 2014 y mediados de 2015, se descubrió una vulnerabilidad de seguridad que afecta a mil millones de dispositivos Android, esto representaba el 95% de los usuarios.

A fines de 2015, Ucrania experimentó un ciberataque contra la red eléctrica estatal que dejó sin suministro, durante varias horas, a más de 80.000 hogares en el Oeste del país. Posteriores análisis forenses del incidente, revelaron que los autores del ciberataque no hicieron uso de tecnologías especialmente novedosas ni sofisticadas. Los atacantes emplearon un malware conocido como *BlackEnergy3* –supuestamente creado por hackers rusos en 2007– y utilizado en cientos de ciberataques menores contra países de Europa del Este, en especial Polonia[14].

A mediados de septiembre de 2015, John McAfee, fundador de una de las mayores empresas de seguridad informática y entonces precandidato presidencial de los

[14] http://www.blog.rielcano.org/a-vueltas-con-la-atribucion-cibernetica /

EEUU, afirmó que “China ha avanzado tanto que en cualquier momento podría tomar el control de EE.UU”, "desactivando la electricidad, tomando el control de aviones y vehículos". MCAfee expresó que: "la guerra fue declarada, lo siento, yo no quiero traer malas noticias al mundo. Estamos en guerra y ni siquiera intentamos armarnos", "Estamos en guerra cibernética con China hace dos años, pero parece que nadie se dio cuenta. Ellos atacaron al Departamento de Seguridad Nacional, al FBI, a la CIA, pero nuestras autoridades o están durmiendo y no se dan cuenta de nada, o simplemente no nos dicen nada"[15].

2016. A fines de julio de este año, Bruce Schneier, experto en seguridad informática, aseguró en el diario Washington Post que las máquinas de votación que se usarán en las elecciones de noviembre en EEUU podrían ser hackeadas por un ciberataque desde el extranjero. Las declaraciones se hicieron al mismo tiempo que mails de la candidata Hillary Clinton como los de miembros del Partido Demócrata, justo antes de comenzar la convención de ese partido, fueran hackeados y publicados, señalando agencias de inteligencia norteamericanas a hackers de Rusia como principales culpables[16].

[15] https://actualidad.rt.com/actualidad/186757-john-mcafee-china-capaz-tomar
[16] http://www.politicargentina.com/notas/201607/15595-experto-en-seguridad-informatica-dice-que-rusia-podria-hackear-las-maquinas-de-votacion-en-eeuu.html

2.17 Escenarios de ciberguerra y la "ciberguerra preventiva

En un interesante artículo español de Francisco Andrades publicado a mediados de 2013, se planteaban 5 escenarios de ciberguerras de probable ocurrencia, las cuales al presente se podría decir que si bien no hay declaración formal (y probablemente nunca lo habrá), ya han comenzado sus operaciones[17]:

- Ciberguerra entre EEUU y China.
- Ciberguerra de países occidentales contra "Estados enemigos" como Irán o Corea del Norte
- Ciberguerra OTAN-Rusia
- Acciones globales de Anonymous y el Hacktivismo
- Una difusa ciberguerra contra el terrorismo

Estas apreciaciones ponen de manifiesto que a las doctrinas de guerra preventiva de EUA, Rusia y China, se hacen correlativas acciones de "ciberguerra preventiva", donde se adelantan ataques cibernéticos ante la probabilidad (segura para el afectado) de que va a ser atacado.

En tal sentido, Manuel Ricardo Torres Soriano, experto español en la materia plantea que "todos los actores estatales tratan de disuadir a sus potenciales enemigos desarrollando capacidades de respuesta que les permitan sobrevivir y responder militarmente a una agresión previa", pero el equilibro disuasorio para que sea posible "no solo es necesario poseer los medios para el ataque, sino también ser vulnerable a la represalia del enemigo", de donde surgen problemas cuando se hace referencia a ciberguerras (Torres, 2011; pp. 14-19).

Así, entiende que es posible que un actor estatal "posea los medios técnicos y humanos necesarios para utilizar el ciberespacio para atacar a otro Estado, pero al mismo tiempo puede ser inmune a una ciber-represalia", como el caso de Corea del Norte. Por tal motivo entiende que "el uso de represalias militares convencionales solo es viable si sus consecuencias son proporcionales al daño causado por el ciber-ataque (Torres Soriano, 2013).

[17] http://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html

Sin embargo, un ataque contra el agresivo régimen norcoreano provocaría inevitablemente una escalada bélica que arrastraría a Corea del Sur y derivaría en una guerra abierta contra un país dotado de un pequeño arsenal nuclear. La legitimidad de una respuesta de este tipo quedaría, igualmente, en entredicho si la opinión pública no percibe una equidad entre el ataque y la respuesta”. Así, se desconocen por razones de inteligencia y contrainteligencia que ataques se realizan o se han sufrido, salvo los que afectan a ámbitos públicos. Por su parte, permanentemente los diferentes ejércitos se preparan en «tiempos de paz» para el desarrollo de operaciones en el campo de batalla cibernético., buscando la vulnerabilidad del adversario, y muchos se esfuerzan por infiltrarse en sus sistemas y plagarlos de «bombas lógicas» y «puertas traseras», para poder utilizarlas cuando se inicien las hostilidades.

Esta situación crea una confusión en entre el tiempo de guerra y el de paz, “lo que dificulta el poder catalogar la conducta de los contendientes y denunciar a un actor cuando esté quebrantando la paz y la seguridad internacionales”.

Asimismo, el experto entiende que las ciber-armas solo son efectivas cuando se prueban y pueden afectar las infraestructuras del adversario, con lo cual la disuasión clásica se hace dificultosa. Para el autor, “la lógica de la ciberguerra no solo hace compleja la disuasión, sino que también beneficia al contendiente que decide tomar la iniciativa y lanzar el primer ataque. El tiempo transcurrido entre la decisión de llevar a cabo el ataque y sus efectos es prácticamente imperceptible, lo que dificulta la existencia de sistema de alerta temprana y anticipación. Esto crea un entorno estratégico tremendamente inestable, con una elevada posibilidad de iniciar un ciber-conflicto, como consecuencia de un error, una mala interpretación de las acciones del adversario, o una incorrecta atribución de responsabilidades”.

En tal sentido, Torres Soriano expone que uno de los elementos característicos de la ciberguerra “son los problemas de atribución de responsabilidades entre los contendientes”, porque todo ciberataque no siempre deja rastros del responsable. Otro dilema estratégico es la mutua responsabilidad público-privado de la defensa cibernética.

Por lo que concluye que “en definitiva, la intrincada y compleja naturaleza público-privada de los principales activos de la ciber-defensa hace imprescindible una incesante cooperación entre Fuerzas Armadas, empresas e instituciones, lo que obliga a replantearse algunas de las principales ideas acerca de cómo debería gestionarse este tipo de conflictos”.

CAPITULO 3

Conceptos y Marco Legal de la Ciberdefensa en el Sistema Internacional.

El artículo 2.4 de la Carta de las Naciones Unidas afirma que: “Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas” y en el Art. 51 señala que "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas". Asimismo, los art. 42 y 51 determinan las excepciones por parte del Consejo de Seguridad. Esta norma implica necesariamente que un país tiene derecho a la guerra cuando es en defensa propia, pero la ciberguerra no es una evidencia factible en tal sentido. Por su parte, el protocolo adicional I de los convenios de Ginebra, el Artículo 36 – Armas nuevas expone que: “cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante”.

En ese marco la ciberguerra constituye un ámbito indefinido para la aplicabilidad de las normas. Paralelamente cada vez más país países se encuentran diseñando estrategias de ciberseguridad para enfrentar los nuevos riesgos, que se corresponden con nuevos tipos de delitos y ataques que vulneran no solo al ciudadano sino al país. Muchos actores internacionales como la OTAN y la Comunidad internacional han planteado la necesidad de militarizar la ciberseguridad, y se imnpone cada vez más el concepto de ciberdefensa.

La militarización de la red no debe ser entendida como una ocupación de la red por fuerzas militares con el solo objeto de controlar los movimientos en ella, sino que se

plantea como el derecho de cada nación a disponer de caber armamento en defensa de sus legítimos intereses.

En ese sentido, el ex director de la Inteligencia Nacional de los EUA, Mike McConnell, declaró en una entrevista de 2009 que las ciber armas deben ser consideradas como armas de destrucción masiva.[18]

El ciberespacio comienza a ser considerado dentro de la doctrina militar como un espacio de batalla más, conjuntamente con tierra, aire y mar. Ello ineludiblemente, provoca un cambio en las situaciones internacionales, creando nuevas alianzas, nuevos actores hegemónicos en la materia.

Internet, revolucionó la vida de las personas y sus comunicaciones a escala mundial, plantea en el ámbito del derecho nuevos dilemas. Ha demandado un proceso de adaptación de instrumentos jurídicos y disciplinas jurídicas preexistentes. También ha afectado derechos fundamentales de raigambre constitucional, como el derecho a la intimidad, y ha alterado la operatividad de las fronteras nacionales. Se argumenta que existen lagunas del derecho en esta temática, sin embargo se argumenta que la actual estructura legal puede adaptarse a los cambios tecnológicos a través de la jurisprudencia, siendo esto una ventaja, razonamiento por el cual no habría carencias normativas.

La opinión mayoritaria de los autores considera que las actividades que se desarrollan en Internet constituye una amenaza para el concepto mismo de soberanía, considerando a esta como "el poder de una nación para impedir que otros interfieran en asuntos internos".

Las amenazas se clasifican en:

- Amenazas por el efecto: que causan a quienes reciben los ataques: robo de información, destrucción, etc.
- Amenazas por el medio utilizado: virus informático, denegación de servicio, etc
- Amenazas por el origen: El hecho de conectar una red a un a entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto se puede hacer robo de información o alterar el funcionamiento de una red. Sin embargo, el

[18] Mike MaConnell en una entrevista ofrecida en el programa televisivo "Charles Rose Show" (8 de enero de 2009)

hecho de que la red no esté conectada a un entorno externo, no nos garantiza la seguridad de la misma. Las amenazas puede ser externas o internas.

- Amenazas externas: Se originan fuera de la red local. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer que es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos. Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red.
- Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas. Los usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc Además tiene algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.
- Los sistemas de intrusos o IPS y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno.

3.1 Ciberguerra: conflicto en el ciberespacio.

Richard Clarke en su libro "Ciber War" define la ciberguerra como "una acción perpetrada por un actor estadual en contra de una computadora o red informática con el propósito de neutralizar la red enemiga. Hay diferentes formas de amenazas son las más conocidas el sabotaje, el espionaje y el corte de suministro eléctrico a una población. (Clarke, 2010) Es la atribución a un actor estatal lo que marca la diferencia con el ciber terrorismo y los ciberdelincuentes: el atacante pertenece a una institución, fuerza armada, está dentro de una cadena de mando.

Quienes llevan a cabo las acciones ciberterroristas no se identifican con entidades gubernamentales y sus ataques son contra blancos políticos intentando causar terror en la población.

Cabe destacar que para Clarke -quien se desempeñó como Coordinador Nacional de Seguridad, Protección de Infraestructura y Antiterrorismo del Consejo Nacional de

Seguridad durante la Administración Clinton- no es adecuado utilizar la palabra terrorismo informático para describir las potenciales amenazas informáticas, considerando el problema de percepción por el que atraviesan los programas de defensa cibernética del gobierno, por el uso equivocado de la palabra terrorismo, aclarando que resulta dificultoso distinguir entre el accionar de hackers de otros realizados por terroristas.

De acuerdo a lo manifestado por fuentes del Pentágono a la prensa, EUA propende a alinear esta política de defensa del ciber espacio con sus aliados de la OTAN. Al respecto, el informe de noviembre de 2011 que elevara el Departamento de Defensa al Congreso norteamericano, indicaba que "las leyes de los Conflictos armados se pueden aplicar tanto en la guerra tradicional como en la ciberguerra". EUA ve a los ataques cibernéticos como una acción bélica. Podría adaptar en su nueva estrategia el derecho vigente de defensa, propio contenido en la Carta de Naciones Unidas al incorporar los ciberataques a la definición de conflicto armado. Cabe destacar que todavía no hay un tratado internacional que establezca definiciones para considerar que un acto es ciberagresión.

- Ciberseguridad: conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros.
- Ciberdefensa: conjunto de acciones e defensa activas, pasivas, preactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.

3.2 El Ciberespacio en el Derecho Internacional: el Manual de Tallin

Una guerra no deja de ser tal porque se libre en el ciberespacio en vez del aire, tierra o agua. Si consideramos al ciberespacio como un escenario más en el cual los estados a través de sus ejércitos participarían en guerras cibernéticas, cabe investigar si es posible aplicar el "ius ad bellum" (o el derecho que regula el recurso de la fuerza por parte de los Estados) y el "ius in bello" (derecho de la guerra o derecho internacional humanitario, que regula el comportamiento durante el uso de la fuerza en un conflicto

armado) a dicho contexto, siendo este uno de los mayores desafíos para los hombres del derecho.

Hay diversas posturas jurídicas al respecto. Algunos autores dicen que se necesitaría un marco legal específico, otros autores opinan que todas las normas del DIH que rigen la conducción de las hostilidades serían adaptables y aplicables durante un conflicto armado cibernético, ya que en definitiva las normas a las que nos referimos tienen por objetivo proteger a la población y los bienes civiles contra los efectos de las hostilidades bélicas, por ello es que podemos incluir a los ataques cibernéticos.

Recientemente expertos en la materia han confeccionado una especie de corpus normativo denominado **“**Manual de Tallin”, que lleva el nombre de la capital de Estonia, donde se compiló y perpetro el primer ataque cibernético de un país a otro. Se creó a pedido del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN.

El manual de 282 páginas no es un cuerpo normativo oficial de la OTAN, pero es una guía importante para situaciones que se puedan plantear en el ciberespacio, toma normas vigentes de carácter internacional sobre conflictos armados como la Declaración de San Petersburgo de 1868 o las Convenciones de Ginebra de 1949, y las aplica adaptándolas al ciberespacio (Arozarena Gratacos, M., Fonseca, C., Ortiz, J.U. y Perdomo, I., 2014) .

Marco Roscini, profesor de Derecho Internacional en la Universidad de Westminster, en Londres, dijo que el manual es el primer intento en su clase de mostrar que las leyes de guerra, algunas de las cuales datan del siglo XIX, son lo suficientemente flexibles para aceptar las nuevas realidades de los conflictos en el espacio cibernético.

A continuación se exponen algunos interrogantes legales y primeras respuestas:

- ¿Una computadora puede ser considerada un arma?

Si, efectivamente son consideradas armas, aunque no convencionales, por su capacidad para causar un daño tanto a un enemigo como a población civil. En este punto se debe evaluar si pueden ser considerados sus efectos indiscriminados. Esta conceptualizacion es importante porque su uso podría estar prohibido por una Convención internacional.

- ¿Cómo definir al combatiente del ciberespacio?

Cabe recordar que “combatiente” es todo miembro de las fuerzas armadas, excepto el personal sanitario y religioso. En una acción de combate los combatientes deben distinguirse de la población civil. Estas se distinguen por su uniforme, un signo definitivo y armas a la vista.

Un aspecto del ciberespacio que plantea dificultades es el anonimato tras el que se esconden quienes participan de las operaciones cibernéticas, por lo que hay dificultades para establecer si los participantes forman parte de las fuerzas armadas, son combatientes regulares o no, o son mercenarios de las mismas.

- ¿Han cambiado las amenazas en la guerra cibernética?

Si, las amenazas han dejado de provenir de naciones identificadas y tienen múltiples orígenes en estados fallidos, grupos terroristas o incluso “solitarios”, el recurso a los ciberataques supone un medio rápido, económico y ágil que, vulneran la seguridad de nuestros países de manera sensible. Cabe agregar que las operaciones de guerra convencional pueden estar acompañas de operaciones en el ciberespacio.

- La definición de “objetivos militares” ¿es aplicable a estos conflictos?

Si, considerándose como tal a las fuerzas armadas, los establecimientos y construcciones así como sus materiales, también otros bienes que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a acción militar y cuya destrucción total o parcial, captura o neutralización tenga, en las circunstancias del caso, una concreta ventaja militar.

Los convenios internacionales prohíben ataques contra “objetivos civiles”.

Cabe un interrogante, si cuando se habla de “objetivo” sea civil o militar, se alude también a “información” que se pudiera capturar o destruir. Es evidente que la información puede ser un “objetivo”.

- ¿El empleo legítimo de la fuerza en respuesta a un ataque?

La legítima defensa se encuentra normada en el artículo 51 de la Carta de la ONU, puede ser individual o colectiva, y dice: “Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad

internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales”. Este artículo se aplica a la guerra cibernetica.

- ¿Cómo opera el concepto de neutralidad?

Opera igual que en la guerra convencional, un país neutral debe abstenerse de participar de las hostilidades. Por otro lado, los contendientes deben tener en cuenta que lanzar un ataque desde la red informática de una nación neutral está prohibido, de la misma manera que ejércitos hostiles no pueden pasar por el territorio de un país neutral.

- ¿Cómo juegan los principios de distinción y proporcionalidad?

El principio de distinción exige a las partes en conflicto que distingan entre civiles y combatientes, entre bienes civiles y militares. Solo son legítimos los ataques perpetrados contra combatientes u objetivos militares.

Se prohíben los ataques indiscriminados, es decir no causar daños o víctimas excesivas en relación al resultado militar esperado. Por ejemplo un virus informático que se duplica constantemente que infecta redes militares y que por su interconexión también causa daños inestimables a infraestructura cibernética civil constituiría una infracción del DIH.

Finalmente debemos recordar la Cláusula Martens, principio subsidiario aplicable al ciberespacio, que dice que en los casos no previstos por el derecho positivo, las personas civiles y los combatientes están bajo la protección y la autoridad de los principios del derecho internacional derivados de la costumbre establecida, los principios de humanidad y la conciencia pública.

Problemas específicos que se plantean para la ciberdefensa:

En primer lugar, al examinar las respuestas legales a los efectos de la ciberdefensa, la situación varía entre los diferentes países y regiones, con diferente grado de desarrollo de las nuevas tecnologías y con diferente grado de desarrollo de sus legislaciones. Más de 45 países han firmado el Convenio de Ciberdelincuencia, tanto en el espacio del Consejo de Europa como Naciones Unidas. Sin embargo, hay distinta

escala de operatividad del mismo, debida a múltiples circunstancias, entre ellas la efectiva incorporación a los ordenamientos nacionales de las disposiciones internacionales.

Cabe agregar que cuando se habla de la ciberdelincuencia se alude a delitos penales nacionales o transnacionales y no de ciberguerra, pese a que en esta se desarrollen acciones iguales a los ciberdelitos.

Muchos países permanecen absortos en sus prioridades y problemas internos. Esta actitud supone un desconocimiento de las ventajas globales de la cooperación y armonización internacional en ciberdefensa.

El convenio sobre ciberdelincuencia es altamente positivo, crea conciencia internacional sobre la evolución y magnitud de este problema, logrando consensos políticos aunque mínimos sobre las conductas a prohibir y de los mecanismos de persecución y colaboración jurisdiccional. Es un gran avance al propiciar definiciones legales estándar, posibilitar la extradición y fortalecer la cooperación policial y judicial entre Estados. Se debe avanzar hacia convenios internacionales sobre estrategias a adoptar en materia de ciberdefensa.

Problemas específicos pendientes de resolver en el plano jurídico:

- Alcanzar consensos sobre ciertas definiciones legales tales como ciberguerra, ciberdefensa. Ello, a los efectos de armonizar normativas de derecho internacional o Convenios internacionales de diferentes estados, ello contribuye a articular una efectiva cooperación internacional. Si los países adhieren a Convenciones internacionales sobre la materia, se podrían desarrollar adecuadamente los procedimientos de extradición, intercambio de pruebas y toda clase de información.
- Un aspecto interesante es que la constante innovación tecnológica hace que los marcos normativos queden obsoletos, de allí la necesidad de una actualización constante.
- Se debe propiciar un desarrollo normativo en materia de cooperación policial. Ej: organismos internacionales ad hoc, intercambio de información en tiempo real e instrumentos de cooperación transfronterizos.

En síntesis el Manual expone sobre una mutación de la categoría jurídica de ciberdefensa, donde en un nuevo escenario, el ciberespacio, en el ocurren crímenes y

guerras. El control del ciberespacio hace peligrar los valores del Estado de Derecho, especialmente en los derechos fundamentales. Concluye que Cibercrimen y ciberamenazas no son categorías equivalentes, existen ciberdelitos que no constituyen amenazas a la seguridad nacional, tampoco todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética.

CAPITULO 4

Apreciación Estratégica de la OTAN en materia de Ciberdefensa frente a dos casos Estonia (ciberataque) y Georgia (ciberguerra).

La época actual, donde las relaciones internacionales se mueven en todos los ámbitos de desarrollo de los países, ha llevado a que el conocimiento y estudio de las Políticas de Defensa de los Estados constituya un factor preponderante para la materialización de alianzas y proyectos en conjunto para el desarrollo de políticas acordes al nuevo escenario mundial.

Así, es posible afirmar que el tema de las Políticas de Defensa es parte de la agenda permanente de las relaciones internacionales de hoy, donde la globalización ha llevado el concepto de fronteras virtuales como una expresión normal para la interacción que se produce en el sistema internacional.

Lo anterior se ha derivado, desde el fin de la Guerra Fría simbólicamente identificada con la caída del Muro de Berlín, a un nuevo cuadro mundial de desafíos y oportunidades, cuyo enfrentamiento sería posible con soluciones propias, creativas, atrayentes y especialmente nacionales. En este nuevo contexto, tan afirmado en los 90, aparecen con gran énfasis los procesos de integración entre los distintos actores internacionales. La cooperación ha pasado a ser parte del vocablo común afectando en parte la Soberanía de los Estados al emerger con mucha fuerza organizaciones no gubernamentales, multinacionales, etc.

Dar respuesta a este nuevo panorama pos Guerra Fría fue el principal desafío de las Fuerzas Armadas del Siglo XXI. La institución militar ve afectados sus valores y normas, el grupo social militar cambia sus costumbres, las organizaciones deben actualizarse y las formas de profesionalidad varían. Ahora bien, es preciso señalar que la función de la Defensa es similar para las distintas naciones, tendiendo como objetivo mantener la Soberanía y la integridad territorial.

La Política de Defensa es una expresión de cómo la sociedad se organiza para el cumplimiento de la función anteriormente señalada, lo que depende de las características propias de cada Estado. Bajo esta premisa, la cultura, la historia, la situación geográfica de cada país y el sistema internacional en sus relaciones interestatales son fuentes para que cada país defina cuáles son sus necesidades específicas de Defensa.

A partir de 1995, los ministerios de Defensa de los países americanos, en sus agendas, discutían temas como: la transparencia en la materia, la cooperación en áreas como búsqueda y rescate, desastres naturales, delitos cibernéticos y operativos antinarcóticos; así como nuevas dimensiones de la Seguridad Internacional que evaluaba riesgos, amenazas y oportunidades; nuevos roles en materia de educación, medio ambiente, ciencia y tecnología e institucionalización de los sistemas de Defensa en áreas como la democracia y las relaciones cívico-militares.

En los últimos años, y en materia de Política Internacional, el análisis se centra en las nuevas tendencias de Seguridad, las que intentan despegarse del marco de referencia de la Guerra Fría, preocupándose ahora del fenómeno de la globalización y de las Nuevas Tecnologías.

Jeimy Cano expone sobre los "eventos recientes sobre fuga de información, las noticias de atacantes informáticos doblegando protocolos y tecnologías de seguridad, las fallas de seguridad que se han presentado tanto en el sector público como en el sector privado, son argumentos suficientes para evidenciar que estamos en un nuevo escenario de riesgos y amenazas, donde la información se convierte en un arma estratégica y táctica que cuestiona la gobernabilidad de una organización o la de una nación" (Cano, p.4)

Así, las Nuevas Amenazas y riesgos han hecho surgir una visión más amplia del problema de la Seguridad, abarcando más allá el ámbito de la Defensa, extendiéndose a aspectos políticos, económicos, tecnológicos y ambientales. El análisis de las Nuevas Amenazas se centró en la construcción de un marco conceptual común en donde el multilateralismo, la institucionalidad de la Seguridad Regional y profundización de la cooperación entre los distintos actores enfrentar las Nuevas Amenazas.

Las amenazas emergentes con proyección al siglo XXI surgen de la actual situación en la medida que no se adoptan soluciones eficaces para enfrentarlas o superarlas.

En este marco, la Defensa Nacional se centra en problemas como la diversificación de los actores que inciden en la Seguridad Nacional, como por ejemplo, empresas y organizaciones no gubernamentales con amplio Desarrollo en la materia. Asimismo, se centra en la modificación de los conceptos de Seguridad Internacional; el análisis del Estado como regulador y articulador del proceso de globalización, en donde el Estado sigue siendo el único actor internacional dotado con capacidad de hacer uso legítimo de la fuerza en los conflictos Inter – Infra – Supra estatales, así como también en la evaluación del Desarrollo de regímenes de gobernabilidad global (ONU, OTAN) ante amenazas asimétricas, como el terrorismo, el narcotráfico, la ingobernabilidad democrática y la respuesta ante la mayor demanda sobre operaciones de paz por parte de la Organizaciones de Naciones Unidas.

Ahora, dentro de la OTAN, ha aparecido una nueva amenaza: los ciberataques a infraestructuras críticas que ponen en riesgo la libertad de acción de los Estados Miembros. Para la OTAN, la primera estrategia que deberían adoptar los Estados es la de reconocer al Nuevo Enemigo Cibernético difícil de reconocer o capturar en una sociedad cada vez más informatizada y donde no hay barreras al conocimiento de las nuevas tecnologías.

Como señala Cano, en este sentido, “el concepto de guerra tradicional, se transforma para darle una nueva función del Estado frente a la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos, ante las amenazas emergentes en el escenario de una vida más digital y gobernada por la información.(…) Es por ello que las reflexiones y decisiones sobre la seguridad tienen una renovada connotación.” (Cano, p. 5) Bejarano explica que “en el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Si antes en el ámbito de la defensa estaba claro que nos movíamos en las tres dimensiones de tierra, mar y aire, e incluso el espacio, ahora contamos con una dimensión adicional, y más intangible que las anteriores. (…) El ciberespacio no tiene fronteras, es un nuevo campo de batalla. (Bejarano, p. 51)

Es a raíz de esta nueva concepción de amenaza que resulta importante analizar los principales antecedentes que, necesariamente, incidieron a la OTAN a reestructurar sus

capacidades y crear equipos de respuesta inmediata frente a ciberataques considerada como una Nueva Amenaza al orden internacional.[19]

Caso 1 Estonia:

Fue la primera vez que un país miembro solicitó apoyo a la OTAN por un ataque a sus sistemas de información y comunicaciones. En aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro[20] [21]

Cronología: (Artiles, pp. 178-179)

"Los ciberataques a Estonia tuvieron lugar entre el 27 de abril y el 18 de mayo de 2007. Durante este periodo los ataques variaron su objetivo, volumen y método, pero en líneas generales se pueden distinguir dos fases principales:

Fase 1, del 27 al 29 de abril, en donde los ataques debida a la inmediatez del conflicto tenían un componente emocional y esto en sí mismo constituía la motivación para unirse a los ciberataques y como todo acto emocional eran básicamente de naturaleza simple, es decir, sin grandes complejidades de carácter técnico y organizativo y sin capacidad de convocar a un número de atacantes lo suficientemente grande como para causar daños serios y poner en una situación de crisis o indefensión a Estonia.

Según Lauri Alman, la primera fase se caracterizó por el uso de herramientas de ciberataque rudimentarias y simples, llevados a cabo por hacktivistas sin grandes

[19] El análisis de las Nuevas Amenazas se centró en la construcción de un marco conceptual común en donde el multilateralismo, la institucionalidad de la Seguridad Regional y profundización de la cooperación entre los distintos actores enfrentar las Nuevas Amenazas. Las amenazas emergentes con proyección al siglo XXI surgen de la actual situación en la medida que no se adoptan soluciones eficaces para enfrentarlas o superarlas. Como afirma Andrés Fontana en su trabajo "Nuevas Amenazas: Implicancias para la Seguridad Internacional Y El Empleo de las Fuerzas Armadas" éstas Nuevas Amenazas son diferentes a las amenazas tradicionales que afectaban la Soberanía y la integridad de un Estado. Estas Nuevas Amenazas afectan la estabilidad del Estado. Son desestabilizadoras tanto en el plano internacional como interno. Afectan la Seguridad del ciudadano y las instituciones.

[20] Ministerio de Defensa. Dirección General de Relaciones Internacionales. Instituto Español de Estudios Estratégicos. Documento informativo del IEEE 09/2011. Nuevo concepto de Ciberdefensa de la OTAN (marzo 2011)

[21] "los ciberataques cometidos contra Estonia, en la primavera de 2007, conocidos por ser el primer caso en que unas operaciones cibernéticas afectan de manera clara, drástica y global a la seguridad nacional de un país; y los ciberataques cometidos contra Georgia, en el verano de 2008, conocidos por ser el primer caso en el que las operaciones cibernéticas son iniciadas y conducidas conjuntamente con operaciones militares armadas." Artiles, Nestor. "La Situación de la ciberseguridad en el ámbito internacional y en la OTAN". Instituto Español de Estudios estratégicos. Cuaderno de estrategia N° 149. Pág. 167

conocimientos técnicos, los cuales hacían uso de herramientas que a su disposición se emplazaban en sitios web, rusos mayoritariamente, conjuntamente con las correspondientes instrucciones. Las herramientas estaban especialmente diseñadas para atacar sitios web de Estonia y especialmente del gobierno, del ministerio de Defensa y de los principales partidos políticos. El primer ataque, registrado e informado, relacionado con el caso Estonia fue contra sitios web gubernamentales durante la noche del 27 de abril de 2007.

En concreto, cuenta Laury Alman que miembros del gobierno estonio se encontraban en una reunión en la sala de situación del gobierno cuando el responsable jefe de relaciones públicas entra en la sala y comenta que no eran capaces de cargar los comunicados de prensa en los sitios web oficiales del gobierno, los miembros del gobierno allí presentes no le dieron más importancia hasta que fueron advertidos expresamente que estaban bajo ciberataque, esto ocurrió la noche del 27 al 28 de abril de 2010 a la 01 de la mañana.

Una vez confirmado que el país estaba bajo ciberataque el gobierno procedió de manera inmediata a organizar un equipo de respuesta liderado y coordinado por el Equipo Nacional de Respuesta ante Incidentes Informáticos (Estonian CERT) y compuesto por personal experto de los ministerios de Comercio y Comunicaciones, y de Defensa, así como de los servicios de Inteligencia. Este fue un gran triunfo de Estonia: identificar la gravedad del asunto con celeridad y organizar inmediatamente un equipo de respuesta multidisciplinar e investirle de la autoridad necesaria.

Fase 2, del 30 de abril al 18 de mayo, en donde el conflicto en las calles se difumina trasladándose al ciberespacio, donde los ánimos de los ciudadanos de Estonia (rusos y estonios) se calman y no hay lugar para ataques emocionales, en esta situación más fría los ataques se volvieron más complejos tanto en el aspecto técnico como en el organizativo y en la coordinación; sucediéndose ataques mucho más sofisticados que necesitaban de un mayor conocimiento de las herramientas de ciberguerra, al menos por parte de los organizadores y de un uso de grandes «botnets» y de una coordinación minuciosa y precisa."

Estonia dio al mundo tres lecciones de respuesta política a un ciberataque masivo contra la seguridad nacional

1. El gobierno identificó con celeridad que estaban bajo un ataque de gran dimensión que podía derivar en una crisis de seguridad nacional.
2. Formaron inmediatamente un equipo multifuncional para coordinar la respuesta; en el que se incluían expertos de la esfera técnica, política, militar, diplomática y jurídica.
3. Reconocieron desde el primer momento ante el mundo que estaban siendo víctimas de un ciberataque.

Caso 2 Georgia

Cronología (Artiles, p. 191):

"Los ciberataques contra Georgia se produjeron en tres fases diferenciadas:

1. **Fase 1: Pre-conflicto armado. Junio de 2008-7 de agosto de 2008.**

Ataques de pequeña escala.

Durante este periodo se contabilizaron ataques DDoS de pequeña escala contra sitios web oficiales de Georgia. El primer ciberataque fue registrado en Junio de 2008, dos meses antes del inicio del conflicto. Estos ataques se enmarcan dentro de las tensas relaciones que mantenían Rusia y Georgia

2. **Fase 2: Conflicto armado. 8 de agosto de 2008 – 12 de agosto de 2008.**

Ataques bien organizados y coordinados.

Durante los cinco días que duró el conflicto armado se sucedieron ciberataques contra sitios web pertenecientes al Presidente de la República de Georgia, el Parlamento, Ministerios de Defensa y Asuntos Exteriores, el Banco Nacional y las principales agencias de noticias. El primer ataque a gran escala y con un alto grado de sofisticación en su ejecución se produjo coincidiendo con la primera ofensiva de las Fuerzas Rusas en territorio de Georgia.

Es importante destacar, que a medida que el conflicto armado se intensificaba, a su vez se incrementaba el número de ciberataques

Deliberadamente o no, el caso es que, los ciberataques debilitaron la capacidad de toma de decisiones del entorno político y militar de Georgia durante el conflicto; y debilitaron la capacidad de información y de comunicación entre el Gobierno y

los ciudadanos, a la vez que, a través de la ciber propaganda, trataron de influenciar en la opinión pública hacia la postura defendida por Rusia, Osetia del Sur y Abjasia.

3. **Fase 3: Post-conflicto armado. 13 de agosto de 2008 – 28 de agosto de 2008.**

Ataques de menor escala.

Coincidiendo con la finalización del conflicto armado, el 12 de agosto de 2008, las operaciones cibernéticas sufrieron una importante reducción en número e intensidad pero el conflicto en el ciberespacio, parecía no estar incluido en el acuerdo de paz y las ciberoperaciones continuaron hasta el 28 de agosto.

El fin de las operaciones cibernéticas no se debió a ningún tipo de acuerdo, sino a la falta de rentabilidad de los cibertaques. Por un lado las medidas de ciberdefensa lograron bloquear gran parte de los ciberataques y por otro, el entusiasmo de los hacktivistas iba decreciendo después de la finalización del conflicto armado."

Análisis de ambos casos

Estos casos demostraron que la guerra tradicional, no solamente cambio, sino que ha evolucionado a un nuevo espacio virtual donde la soberanía y autonomía del Estado es cada vez más vulnerada por expertos de la tecnología.

Como consecuencia de estos ataques, se han desarrollado acuerdos de cooperación en la creación de instituciones y organismos dentro de la OTAN que permitan concentrar un conocimiento especializado en esta materia tendientes a generar áreas de ciberseguridad.

La OTAN se enfrentó a este problema en la Cumbre de Bucarest de 2008, de cuya declaración se desprendían tres líneas de acción que consistían en medidas a adoptar:

- Por la propia OTAN para mejorar su capacidad de ciberdefensa;
- Por las naciones para mejorar la protección de los sistemas de información crítica desplegados en sus territorios;
- Por ambas partes, OTAN y naciones, para mejorar la coordinación, intercambio de información y el apoyo mutuo

4.1 Sobre el Nuevo Concepto Estratégico de la OTAN.

A raíz de distintas reuniones llevadas a cabo por los Ministros de Defensa de la OTAN realizadas en el marco del Nuevo Concepto de Ciberdefensa de la Alianza, la OTAN ha aprobado una Política de Ciberdefensa y un plan de acción para su implementación. El principal objetivo consiste en la protección de las redes informáticas de los Estados Miembros.

Uno de los principios fundamentales de este Concepto es el de la cooperación como pilar fundamental para poder integrar las capacidades de otros Estados y organismos internacionales en el planeamiento de la Defensa de la OTAN frente a las ciberamenazas (MINDEF, 2001) Como objetivos, la OTAN implementará un enfoque coordinado de ciberdefensa para abarcar aspectos de planificación y desarrollo de capacidades junto con mecanismos de respuesta en caso de ciberataque. Para ello la Alianza incorporará e integrará las medidas de ciberdefensa en las misiones.

Para lograr estos objetivos, la OTAN utilizará los procesos de planeamiento de la defensa para promover el desarrollo de las capacidades de ciberdefensa de los aliados, para ayudar a las naciones aliadas que lo soliciten y para optimizar la compartición de información, la colaboración y la interoperabilidad.

4.2 Capacidades de ciberdefensa.

En este aspecto, se han creado organismos especializados en materia de ciberataques. Uno de ellos es el NCIRC (Capacidad de respuesta ante incidentes informáticos de la OTAN), cuya misión principal, es la de repeler ataques en materia de ciberdelito. Al mismo tiempo, es la responsable de proteger todas las instalaciones informáticas de la OTAN, tanto civiles como militares. Para tal fin, cuenta con la logística y apoyo necesario que le rinda la organización para cumplir con tal fin.

Para aumentar las capacidades de la ciberdefensa, el Consejo de la OTAN firmó la Política de Ciberdefensa en enero de 2008 con el objetivo de aumentar la capacidad de la OTAN en respuesta a ciberataques, proteger los sistemas y redes de información y

comunicaciones de valor crítico para la Alianza frente a los ciberataques; desarrollo del concepto de ciberdefensa[22]; proceso para conseguir una capacidad operativa completa de respuesta ante incidentes informáticos-NCIRC.

4.3 Plan de Ciberdefensa

El principio que rige este plan es el "principio militar de mutua asistencia y defensa colectiva", el cual, establece que "cualquier nación miembro de la OTAN que sufra un ciberataque significativo podrá solicitar ayuda de la OTAN. La petición será considerada por el comité de gestión de ciberdefensa"

4.4 Ataques más sofisticados y principales actividades

Si bien hemos analizado algunos casos en nuestro Estado de Arte, los ataques van mutando y se han vuelto más sofisticados gracias al desarrollo de las Nuevas Tecnologías de la información generando una mayor vulnerabilidad a los actores que son atacados por este medio.

Algunos de los tipos de ataques conocidos por los organismos especializados en materia de ciberseguridad figuran en las guías CCN-CERT:[23]

- Virus: Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- Código dañino, también conocido como código malicioso, maligno o «malware» en su acepción inglesa: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.
- Bomba lógica: Segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre desencadenen a alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal.

[22] "NATO Cyber Defence Concept, MC 0571, 4-2-2008.
[23] Guía de seguridad de la STIC (CCN-STIC-401), Glosario y abreviaturas, 1 de febrero de 2010.

- Troyano: Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.
- Gusano: Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

Es importante destacar la "profesionalidad" con la que estos tipos de ataques son diseñados y ejecutados. Se requiere de un alto conocimientos en ciencias y tecnología y un alto nivel de organización para poder perpetuar en el tiempo. Las vulnerabilidades de los sistemas son el elemento fundamental de los ciberataques porque es la esencia de las capacidades ofensiva, defensiva y de inteligencia en el ciberespacio (Coleman, 2010).

Las amenazas enemigas de las infraestructuras críticas (IC) siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora ataques en tiempos de paz por ciberatacantes anónimos (Geer, 2009).

Teniendo en cuenta las características de estos ataques, la OTAN desarrolló el concepto de RRT: "Los expertos en ciberdefensa son responsables de asistir a los estados miembros que soliciten ayuda en el caso de un ataque de relevancia nacional"[24].

Para efectivizar este trabajo, se han desarrollado diferentes actividades de coordinación y asesoramiento para que las autoridades políticas y expertos de las tecnologías puedan trabajar en conjunto con la colaboración de otros organismos internacionales como la Unión Europea. Estas actividades incluyen:

- Coordinación y asesoramiento en ciberdefensa

Esta actividad será desarrollada por el campo político, militar y científico-tecnológico de la Alianza. La CDMA (Cyber Defence Management Authority) es la encargada de llevar a cabo las coordinaciones y el asesoramiento a las unidades para repeler ciberamenazas y prevenir ataques cibernéticos, como así también, evaluar los riesgos de otros actores en infiltrar las estructuras críticas de la organización y repeler las

[24] "Política de Ciberdefensa de la OTAN" – Reunión de Ministros de Defensa – Mayo 2011

vulnerabilidades que pongan en riesgo las actividades de la misma. Ante una emergencia en materia de ciberataque, se debe recurrir a este organismo.

- Asistencia a las naciones

La OTAN se rige por el principio de cooperación con otros socios regionales e internacionales puesto que la nueva modalidad de ataque permite que, desde cualquier computadora, pueda ejecutarse una infiltración a los sistemas de comunicación de los Estados Miembros. La OTAN, por tal motivo, promueve acuerdo, a través de medidas de confianza mutua con terceros para evitar riesgos o amenazas que pongan en riesgo la libertad de acción de la Alianza.

- Investigación y formación

Para el desarrollo de esta actividad, se ha creado el Centro de Excelencia OTAN de Ciberdefensa Cooperativa (Cooperative Cyber Defence Centre Of Excellence – CCDCOE) con el objetivo de llevar a cabo investigaciones en materia de ciberguerra y capacitar al personal en el conocimiento de este nuevo campo de la Defensa.

- Cooperación con los socios.

Se ha creado el Consejo para la Cooperación en Ciberdefensa con socios y organizaciones internacionales para fomentar mediadas de confianza mutua con la intención de mitigar y repeler ciberamenzas a los países de la Alianza.

El estudio sobre la apreciación estratégica de la OTAN brinda una importante experiencia ante la necesidad de un planeamiento estratégico que ha generado esta nueva modalidad de ataque para proteger los intereses vitales de una nación como así también la necesidad de fomentar la investigación y desarrollo en proyectos con capacidad de mitigar y repeler estas nuevas amenazas cibernéticas. En todos los ámbitos del Poder Nacional. “La ciberguerra es asimétrica”.

El bajo coste de los equipos informáticos puede implicar que nuestros adversarios no tengan necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a nuestras capacidades militares. Unos cuantos programadores pueden, si encuentran una vulnerabilidad a explotar, amenazar nuestros sistemas logísticos, robar nuestro planeamiento operacional o cegar nuestros sistemas de inteligencia y de mando y control. Por este motivo, muchos ejércitos están desarrollando capacidades ofensivas en

el ciberespacio y se estima que más de 100 servicios de inteligencia extranjeros llevan a cabo estas actividades.”

Evidenciamos “que la Alianza Atlántica, que fue la primera en percibir la necesidad de acomodar las respuestas tradicionales al nuevo escenario estratégico, está inmersa en un proceso de transformación profunda de sus estructuras, procedimientos y capacidades, con el fin de conseguir unas fuerzas aliadas mejor dotadas, interoperables y capaces de actuar con la máxima eficacia (…) Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar, aire y espacio, a través del ciberespacio” (Duran, P. 220).

CAPITULO 5

Estrategias en materia de Ciberdefensa

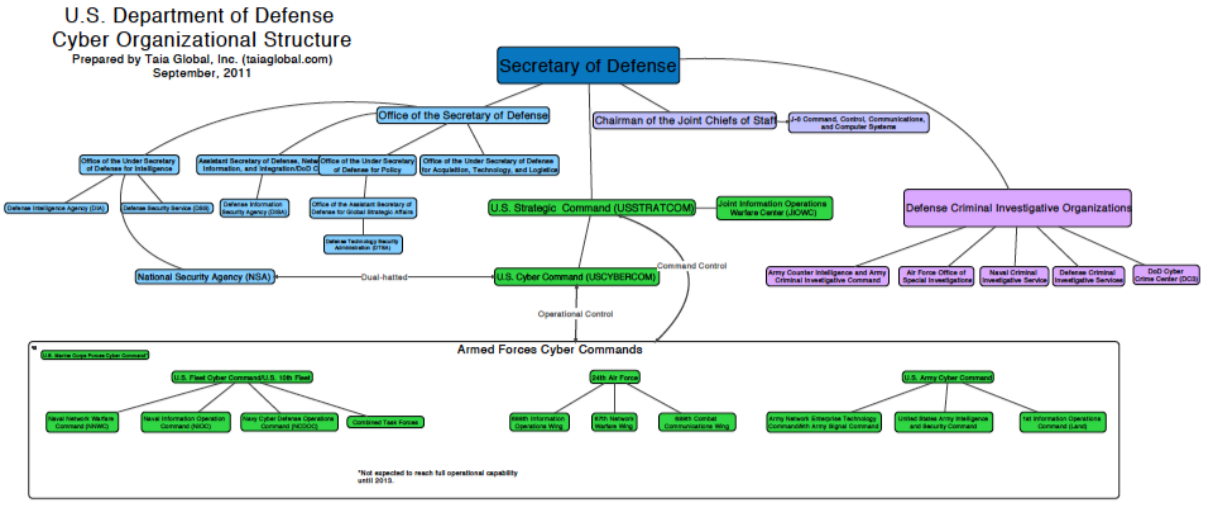
5.1 EUA crea el Primer cibercomando militar

En el año 2003, los EUA modificaron de la doctrina militar el concepto de Guerra de la Información, dejando solamente el de Operaciones de Información, entendidas como el empleo integral del corazón de las capacidades de la guerra electrónica, operaciones de redes de computadoras, operaciones psicológicas, operaciones velo y engaño y operaciones de seguridad, en concierto con las capacidades de soporte y relacionadas para influenciar, interrumpir, corromper o usurpar el corazón del proceso de toma de decisiones humanas y automatizadas del adversario, mientras que se protegen las propias.

El 21 de mayo de 2010 se anuncia la creación del Primer cibercomando en EUA (U.S. Cyber Command - USCYBERCOM) bajo el mando del Comando Estratégico militar. Su misión es planear, coordinar, integrar, sincronizar y conducir "actividades para: dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y; prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acciones a los EUA y sus aliados en el ciberespacio e impedir lo mismo a nuestros adversarios". En tal sentido, el Secretario de Defensa de ese país, Leo Panetta indicó, a mediados de Julio de 2011 que un "nuevo Pearl Harbor es un posibilidad real en el mundo actual, como resultado debemos contrarrestar esto agresivamente".

Por su parte, el General Keith B. Alexander, Comandante del USCYBERCOM, a cargo también de la National Security Agency y del Central Security Service (CHCSS), indicó en julio de 2012 que le "preocupa el paso de los ataques perjudiciales a los destructivos. Creo que están por venir", añadiendo que hay que prepararse para estos ataques (Nakashima, 2012).

Su organización, dependiente del Secretario de Defensa y a su vez del Comando Estratégico de los EUA, se interrelaciona con los los cibercomando de cada una de las fuerzas armadas.



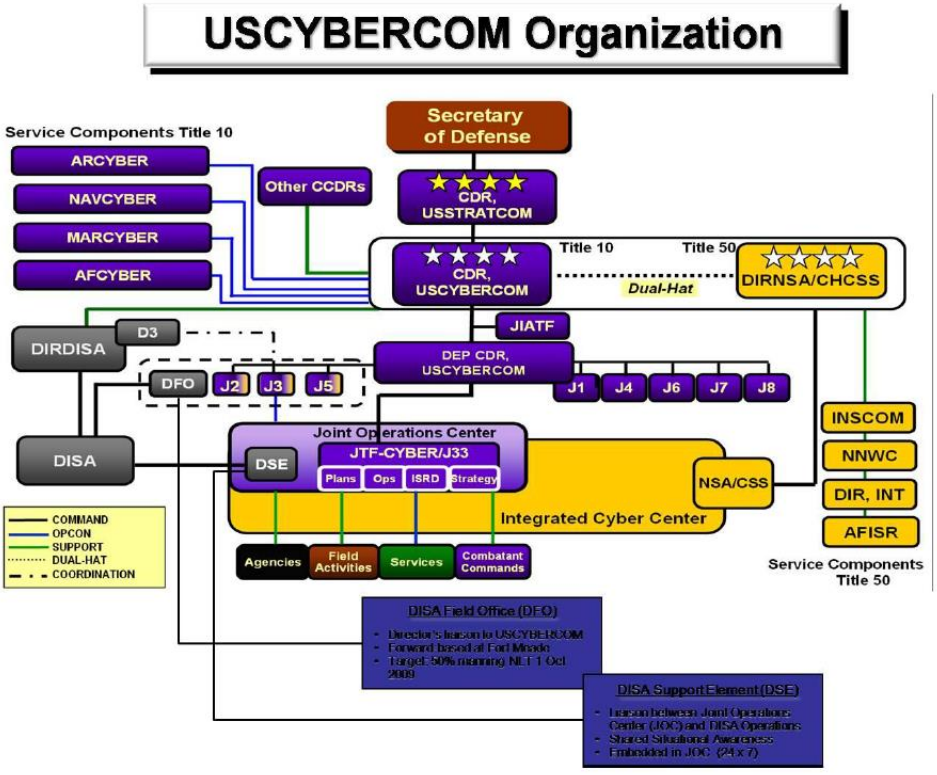


Fig. 4. USCYBERCOM Organization (http://www.govexec.com/nextgov/)

http://www.dtic.mil/dtic/tr/fulltext/u2/a525307.pdf

Así, el Ejército de los EUA, crea en octubre de 2010 el U.S. Army Cyber Command (ARCYBER) como componente dependiente del USCYBERCOM. Ubicado en el área de Washington DC, se compone de 21.000 efectivos, militares y civiles destinados en todo el mundo y tiene por misión planificar, coordinar, integrar, sincronizar, dirigir y conducir operaciones y defensa de la red de todas las redes del Ejército y conducirá operaciones en el ciberespacio en apoyo del completo espectro de las operaciones militares para asegurar la libertad de acción de los EUA y sus aliados en el ciberespacio y para rechazar el mismo a los adversarios (US Army, 2010).

A mediados de 2015, el cibercomando indicó que recibe 250.00 ataques por hora, lo que implica alrededor de 6 millones por día (Hernández, 2015).

A fines de abril de 2015, EUA dio a conocer la segunda Ciberestrategia del Departamento de Defensa (*The DoD Cyber Strategy 2015-2018)* que actualiza la original de 2011 y se encuentra coordinada con los documentos Estrategia de Seguridad Nacional de 2015 y la Revisión Cuadrienal de Defensa de 2014.

A fines de abril de 2015, EUA dio a conocer la segunda Ciberestrategia del Departamento de Defensa (*The DoD Cyber Strategy 2015-2018)* que actualiza la original de 2011 y se encuentra coordinada con los documentos Estrategia de Seguridad Nacional de 2015 y la Revisión Cuadrienal de Defensa de 2014.

Esta Ciberestrategia 2015 incluye como tres misiones principales: “defender las redes, sistemas y la información del DoD (Departamento de Defensa); defender la patria y los intereses nacionales de EUA frente a los ataques cibernéticos de significativa importancia; y proporcionar apoyo cibernético a los planes operativos y de contingencia militar”. El documento también afirma que el Departamento de Defensa busca defender al país contra cualquier adversario “durante tiempo de paz, crisis o conflicto” (US Department of Defense, 2015).

Asimismo, establece como objetivos estratégicos:

- Construir y mantener fuerzas y capacidades listas para dirigir operaciones en el ciberespacio;

- Defender las redes de información del DoD, asegurar los datos del DoD y mitigar los riegos para las misiones del DoD;
- Estar preparados para defender la patria y los intereses vitales de EUA de ciberataques destructivos y perjudiciales de consecuencias significativas;
- Construir y mantener un plan y opciones ciberespaciales (de Internet) para emplear esas opciones en controlar una intensificación del conflicto y determinar el ambiente de conflicto en todos los escenarios y etapas; y
- Construir y mantener fuertes alianzas y socios internacionales para disuadir amenazas determinadas e incrementar la estabilidad y seguridad nacional.

En apoyo a esas misiones, la Estrategia establece que el Departamento de Defensa dirige un rango de actividades “fuera del ciberespacio” como la cooperación “con agencias del gobierno, con el sector privado, y nuestros socios internacionales (Canadá, Gran Bretaña, Australia y Nueva Zelanda) para buscar información, construir alianzas y socios, y fomenta normas de conducta responsable para mejorar la estabilidad estratégica global”. La estrategia, que reemplaza a la de 2011, plantea abiertamente que EUA podrá realizar actividades de ciberguerra al afirmar que el país “debe ser capaz de recurrir a las ciberoperaciones para destruir las redes de mando y control, infraestructuras críticas o sistemas de armas de los potenciales adversarios del país”. También recuerda que las ciberoperaciones se integrarán plenamente en el planeamiento y conducción de las operaciones militares.

Al momento de presentar la estrategia, el Secretario de Defensa estadounidense Ashton Carter durante su visita a Silicon Valley donde dictó una una conferencia en la Universidad de Stanford, argumentó la obligada necesidad del Departamento de Defensa (DoD) para estar a la vanguardia de la innovación tecnológica. En la conferencia expuso que la nueva estrategia, de carácter disuasorio, expone sobre los principales riesgos y amenazas a los que se enfrenta el DoD, el gobierno y los ciudadanos de ese país en general en todo el ciberespacio. En tal sentido, la estrategia dispone que organismos implementaran esa estrategia, las principales medidas a adoptar y los objetivos hasta el año 2018.

En este sentido, los aspectos más relevantes de esta estrategia destacó que EEUU:

- *“*… debe ser capaz de utilizar las ciberoperaciones para disrumpir las redes de mando y control, infraestructuras críticas y sistemas de armas de los potenciales adversarios del país” (Fojón Chamorro, 2105).
- integrará las ciberoperaciones plenamente en el planeamiento y conducción de las operaciones militares**,** potencializando la construcción de cibercapacidades a nivel conjunto, a partir de crear en los próximos años una ciberfuerza compuesta por 6.200 efectivos repartidos en en 133 centros operativos para reforzar el Comando Cibernético.
- seguirá financiando proyectos tecnológicos de primer nivel para dinamizar y evolucionar la industria tecnológica en el ámbito militar, creando para tal fin una iniciativa para fortalecer las relaciones entre las empresas tecnológicas y el Pentágono dentro de lo que incluirá iniciativas de capacitación con el sector privado.
- creará una Oficina del Asesor Principal en materia de Ciberdefensa del Secretario de Defensa.

Para alcanzar esos objetivos, el Pentágono ha otorgado a la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) de un presupuesto cercano a los 3.000 millones de dólares para investigación, desarrollo e innovación de nuevas tecnologías destinadas a uso militar para 2016, en especial las relacionadas con el ciberespacio. Gran parte de ese presupuesto estará destinado a mejorar las capacidades que permitan realizar:

- las denominadas *Computer Networks and Electronic Operations* (CNEO),

- satisfacer la creciente demanda de ancho de banda para la operatividad de las fuerzas armadas,

- evolucionar los sistemas no tripulados en cualquiera de sus modalidades (terrestres, acuáticas o áreas),

- avanzar en las tecnologías de miniaturización de sistemas y componentes eléctricos y electrónicos,

- mejorar las capacidades y tecnologías del Big Data para optimizar la gestión de la información, y

- avanzar en todas las disciplinas relacionadas con la inteligencia artificial, la biometría, la guerra inalámbrica o el uso avanzado de impresoras 3-D (Fojón Chamorro, 2015).

5.2 El ciber Ejército Azul de la República Popular China

Diversos investigadores de la Academia de Ciencias Militares de China, de la Universidad Nacional de la Defensa China y de la Academia de Comando de Comunicaciones de Wuhan han desarrollado en los últimos años estudios sobre la ciberguerra.

Así, dos expertos militares en electrónica de la referida Academia, los Coroneles Ye Zheng y Zhao Boaxian, han indicado que el uso de Internet en las revueltas desarrolladas en 2011 en el mundo árabe, están asociadas a acciones gubernamentales desde el exterior de esos países, por lo cual China debe erigir una “frontera de Internet” y “defender su soberanía de internet”, indicando que “igual que la guerra nuclear fue la guerra estratégica de la era industrial, la ciberguerra se ha convertido en la guerra estratégica de la era de la información y se ha convertido en una forma de batalla que es muy destructiva y concierne a la vida y la muerte de las naciones”. Así, en mayo de 2011 el Coronel Geng Yansheng, Vocero del Ministerio de Defensa Chino indicó que "China es relativamente débil en materia de ciberseguridad y ha sido a menudo víctima de ataques en internet", "actualmente, la seguridad en la red se ha convertido en un problema internacional, que no sólo afecta al ámbito social, sino también al sector militar", indicando que su país ha establecido la creación de una unidad de ciberdefensa, denominada el Ejército Azul (Ambrós, 2011).

Los expertos de este país incluyen nuevos conceptos dentro de las denominadas ciberactividades como cibermobilización, cibermanipulación, cibereclutamiento que no conforman lo que entendemos por la guerra (ataque y defensa) señala Timothy Thomas, experto estadounidense en Operaciones de Información del Foreign Military Studies Office del Ejército de ese país (Thomas, 2005).

Un informe de la empresa de seguridad informática dado a conocer en 2013 por el New York Times, indicó que unidades militares secretas de China atacan a EUA diariamente. El informe indica que los denominados Primer, Segundo, Tercer y Cuarto Departamentos, de varios decenas de miles de integrantes cada uno, dependientes del denominado Departamento General de Personal (DGP) del Ejército Popular de Liberación realizan dichas ciber operaciones. Bajo las órdenes del DGP, tres departamentos trabajan en sus campañas de espionaje para guerras no convencionales. Su Segundo Departamento se enfoca en los espías humanos e inteligencia (HUMINT). El Tercer Departamento se enfoca en ciberespionaje y señales de inteligencia (SIGINT). El Cuarto Departamento se enfoca en guerra electrónica, interceptación de datos satelitales y en inteligencia electrónica (ELINT). Asimismo, el informe señala que el DGP también supervisa las regiones militares de China, la Armada, la Marina, la Fuerzas Aérea y la Segunda Artillería, hogar de las armas nucleares chinas (Philipp, 2014).

El 26 de mayo de 2015 el Ministerio chino de Defensa Nacional dio a conocer la nueva “Estrategia militar de China”. Dado a conocer por la Oficina de Información del Consejo de Estado de la República Popular China, el documento en la materia indica que “el ciberespacio se ha convertido en un nuevo pilar del desarrollo económico y social, y un nuevo dominio de la seguridad nacional. Dado que la competencia estratégica internacional en el ciberespacio se ha ido convirtiendo cada vez más feroz, un buen número de países están desarrollando sus fuerzas militares cibernéticos. Siendo una de las principales víctimas de ataques de piratas informáticos, China se enfrenta a graves amenazas a la seguridad a su infraestructura cibernética. A medida que el ciberespacio pesa más en la seguridad militar, China acelerará el desarrollo de una fuerza cibernética, y mejorar sus capacidades de conocimiento de la situación del ciberespacio, la defensa cibernética, el apoyo a los esfuerzos del país en el ciberespacio y la participación en la cooperación internacional cibernética, con el fin de detener importante cibernético las crisis, garantizar la seguridad de redes y datos, y mantener la seguridad nacional y la estabilidad social” (República Popular China, 2015).

Asimismo, el 16 de diciembre de 2015, en la ciudad china de Wuzhen, se inició la Conferencia Mundial de Internet y organizado por la Administración del Ciberespacio

de China (CAC) contando con la presencia de dos mil representantes procedentes de un centenar de países (Fojón Chamorro, 2016).

Entre los asistentes destacaron el primer ministro ruso Dmitri Medvédev, el presidente de Pakistán Mamnoon Hussain y los vicepresidentes de Apple, IBM y Microsoft. Ver destacar que no participó ningún representante oficial de los denominados 5 Ojos, alianza constituida en materia de telecomunicaciones y seguridad electrónica por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda.

En el discurso inaugural el presidente chino Xi Jinping**,** subrayó la importancia estratégica que tiene la seguridad del ciberespacio para el desarrollo socio-económico chino, considerando que China posee una visión sobre el futuro del ciberespacio centrada en tres áreas fundamentales: gobernanza del ciberespacio, ciberseguridad y ciber-soberanía.

En relación al ciberespacio abogó por un ciberespacio regulado, pero que sean consensuadas por la comunidad internacional y no impuestas por un solo actor. En materia de ciberseguridad, expuso la necesidad de evitar la militarización del ciberespacio, e instó a la comunidad internacional a luchar contra el cibercrimen, destacando los recientes convenios suscriptos con EEUU. Asimismo, en materia de ciber-soberanía, expuso que: “el principio de la igualdad soberana consagrado en la Carta de las Naciones Unidas es una de las normas básicas en las Relaciones Internacionales contemporáneas. Cubre todos los aspectos de las relaciones entre estados, incluyendo también el ciberespacio” e indicó que “se debe respetar el derecho de cada país a elegir de forma independiente el modo en el que quiere desarrollar su ciberespacio específico, su modelo de regulación cibernética y garantizar una participación igualitaria en la gobernanza ciberespacio internacional”.

5.3 Las actividades militares de la Federación de Rusia en el Ciberespacio

A principios de 2012, el Ministerio de Defensa ruso publicó en su página web un documento titulado *“*Criterios conceptuales sobre la actividad de las Fuerzas Armadas de la Federación de Rusia en el espacio informático”, el cual establece las tendencias que

adoptarán sus fuerzas para el control, la prevención y la solución de los conflictos cibernéticos que puedan surgir (Caplan, 2012). Asimismo, el documento indica la posibilidad que ocurran ataques ofensivos contra otros países y propone que se extienda la costumbre del Derecho Internacional en materia de guerras interestatales -como el uso proporcional de la fuerza y la minimización de daños a civiles- a los conflictos en el ciberespacio. Del documento de catorce páginas, la mitad de las cuales, aproximadamente, constituye el cuerpo terminológico. La concepción de guerra, propiamente dicha, ocupa la menor parte del documento (Meschcheriakov, 2012).

En el documento no se hace mención alguna sobre la gestión por parte de Rusia de acciones bélicas ofensivas en el ciberespacio. La concepción estratégica se resume en tres acciones fundamentales: contención, prevención y autorización de los conflictos bélicos en el campo digital. En el punto 3.2.3 del documento expone que “en condiciones de escalada de un conflicto en el espacio informático y de su paso a una situación de crisis, hacer uso del derecho de autodefensa individual o colectiva mediante el empleo de cualquier procedimiento y medio elegido, que no sean contrario a las normas reconocidas universalmente y a los principios de las leyes internacionales”.

Otra disposición hace referencia a la instalación de fuerzas informáticas de seguridad en el territorio de otros estados. En tal sentido, esta instalación está permitida tanto voluntariamente como en correspondencia con la legislación internacional.

En tal sentido, Eugene Kaspersky director de la compañía rusa de seguridad informática que lleva su nombre hizo una evaluación en relación a los nuevos tipos de ataques de virus como Stuxet o Flame contra infraestructuras críticas como las centrales nucleares o refinerías petroleras. En una conferencia sobre seguridad y ciberespacio desarrollada a mediados de 2012 por la Universidad de Tel Aviv indicó "créame, tengo mucho miedo y preocupación por lo que puede provocar la ciberguerra, espero que se actúe antes de que sea demasiado tarde”. Kaspersky evaluó que para crear un virus como Flame “se necesitó menos de 100 millones de dólares" para pagar a ingenieros, expertos, analistas, técnicos, máquinas de café, etc. y que ese virus “es un ejemplo que el caber-arma es muy peligroso y puede hacer mucho daño, ya no lo llamo ciberguerra sino ciberterrorismo. No sabes dónde y cuándo será el próximo ataque y, si no se actúa rápido, las cosas irán peor. Los países no tienen suficientes defensas" y concluyó que teme "el fin

del mundo que conocemos si no hay cooperación internacional contra este peligro" (Emergui, 2012).

Asimismo, en febrero de 2013, el Ministerio de Defensa ordenó al Estado Mayor Conjunto de las FFAA de su país acelerar el plan para la creación de un cibercomando militar (Rico, 2013). El mismo se anunció como un centro donde convergerían esfuerzos militares junto a los de del Departamento K del Ministerio del Interior, responsable en investigar delitos informáticos, y al Centro de seguridad informática del Servicio Federal de Seguridad (inteligencia), responsable del accionar de grupos extremistas, organizaciones criminales y servicios secretos extranjeros que atentan contra los intereses rusos.

Al respecto, Alexander Sharavin, director del Instituto de Análisis Político y Militar, miembro de la Academia de Ciencias Militares afirmó que “hace ya diez años se plantearon en el Ministerio de Defensa propuestas para la creación de un comando de este tipo. Entonces lo discutimos intensamente y por lo que yo sé, muy pronto debe aparecer un comando así en nuestro ejército. La protección de nuestras redes cibernéticas es una tarea no sólo para nuestras fuerzas armadas, es una tarea de todo el Estado, de todas nuestras administraciones encargadas de la seguridad nacional. La guerra cibernética ya es una realidad por eso comandos de este tipo tienen la tarea no sólo de defender sino también, si fuera necesario responder a los ataques” (Petrova, 2013).

Por su parte, Anatoli Tsiganov, director del Centro de Análisis Militares, y profesor de política mundial en la Universidad Estatal de Moscú (MGU) expuso que “la idea del uso de armas cibernéticas fue planteada hace unos seis o siete años. Actualmente estas armas ocupan el segundo lugar en importancia, tras las armas nucleares”, ya que “las armas cibernéticas son usadas de manera generalizada en conflictos militares, el ejemplo más reciente tuvo lugar en el transcurso de la intervención norteamericana en Libia, donde se controló no sólo el espacio aéreo (...) sino también las redes de comunicaciones. Se introdujeron en las redes de televisión libias, transmitiendo para la población local”.

Tsiganov estima que Israel es el país donde más está desarrollada la ciberdefensa y en segundo lugar EUA y los países europeos terceros.

En agosto de 2013, se aprueba el documento "Fundamentos de la política estatal de Rusia en la esfera de la seguridad informática por un período hasta 2020" en el que se expone la visión rusa del problema de la seguridad informática internacional y se dan lineamientos a futuro en la materia.

El documento identifica cuatro amenazas cibernéticas para Rusia:

1) El uso de tecnologías informáticas y de comunicación como arma informativa con fines político-militares para llevar a cabo actos hostiles y de agresión.

2) El empleo de tales tecnologías por parte de terroristas.

3) El incremento de los cibercrímenes, particularmente en cuanto al acceso ilegal a la información computarizada, la creación y difusión de programas dañinos.

4) El empleo de tecnologías de Internet para "inmiscuirse en los asuntos internos de estados", "perturbar el orden público" y "hacer propaganda de ideas que inciten a la violencia".

El documento propone para enfrentar dichas amenazas, establecer mayor cooperación con sus aliados, en primer lugar con la Organización para la Cooperación de Shanghái, la Organización del Tratado de Seguridad Colectiva y el grupo BRICS (Brasil, Rusia, India, China y Sudáfrica). Posteriormente, estas intenciones planteó Rusia en oportunidad de la cumbre BRICS en Fortaleza, Brasil, en julio de 2014. Cabe destacar que este documento no refiere a posibilidades de reacción militar a los ataques cibernéticos, dejando esta cuestión al ámbito específico del Ministerio de Defensa. (Kóbzev, 2013).

5.4 Las Fuerzas de Defensa de Israel (FDI) y la ciberdefensa

Desde 2010, el Gobierno Israelí cuenta con una "Ciber Iniciativa Nacional". (Tabansky, 2013) a cargo de la Autoridad Nacional de Seguridad de la Información.

Asimismo, las FDI cuentan con un sólido organismo de ciberdefensa integrado desde 2009. (Raska, 2015, pp. 21)

En la mencionada Conferencia de Tel Aviv de 2012, el entonces Ministro de Defensa isarelí, Ehud Barak, indicó que su país desarrolla acciones tanto la defensa como el ataque en el ciberespacio, expresando que "a diferencia de la guerra convencional, en

este tipo de lucha es más importante invertir en la defensa que atacar al enemigo". Asimismo, indicó que *"*debemos cambiar a un sistema proactivo, en que no solo reaccionemos ante ataques*",* agregando que la ciberdefensa *"*es más importante y más difícil*"* que los ciberataques, señalado que Israel desde aspirar a convertirse en líder mundial en ciberdefensa, a niveles militar y civil (Emergui, 2012).

El Gobierno israelí estableció a mediados de 2012 un Comité Nacional para desarrollar la defensa de la infraestructura crítica, sistemas financieros y otros activos. Por su parte, las FDI cuentan con componentes específicos frente a ataques tecnológicos contra su país. En abril de 2012, alrededor de 30 efectivos de las FDI se graduaron del su primer curso de los ciber-defensores, desarrollado para brindar capacidades para prevenir los ciberataques contra las redes propias. En el curso estrenaron un nuevo sistema de simulación de ciberguerra denominado Elbit. El simulador, desarrollado para el gobierno, instalaciones militares e instalaciones civiles de infraestructura crítica, permite la formación personal y grupal de los diferentes usuarios en la localización, manejo y gestión de diversos eventos de la guerra cibernética y los ataques que esta trae aparejados. Asimismo ofrece capacitación en prevención de los episodios de guerra cibernética, mediante la simulación de escenarios de redes de protección.

5.5 El Consejo Superior del Ciberespacio y el Ejército cibernético de Irán

En octubre de 2011, el general Gholam Reza Jalali, Director de la Organización de Defensa Pasiva de Irán, anunció en la conferencia de Defensa Cibernética celebrada en Teherán que para contrarrestar posibles amenazas externas sobre sus instalaciones nucleares, Irán había puesto en marcha un "cibercomando" dedicado a luchar contra posibles ataques de piratas informáticos contra las redes del país, que tendría como misión "vigilar, identificar y contraatacar cuando se produzcan amenazas informáticas contra las infraestructuras nacionales".

Jalali indicó que "los Estados Unidos está reduciendo el tamaño de su Ejército para poder tener un infraestructura de defensa cibernética más grande. Pues, países como Irán tienen que instalar y modernizar sus sedes de defensa cibernética e incluso (constituir) un Ejército cibernético". El general iraní expresó también que Irán es uno de

los países que más ha sido objeto de ciberataques a lo largo de los últimos dos años. En este sentido, recalcó que los centros atacados no salieron afectados y de momento Irán es en gran medida inmune de este tipo de ataques (Hispantv, 2012). A principio de marzo de 2012, el líder iraní ayatolá Ali Jamenei, anunció la creación del Consejo Superior del Ciberespacio, conformado por el Presidente del país y los jefes del Parlamento y el Poder Judicial, el secretario del Consejo Supremo de Seguridad Nacional, varios ministros y mandos militares y policiales.

5.6 La ciberdefensa en Reino Unido de Gran Bretaña (RUGB)

En un informe de julio de 2010 presentado al Parlamento Británico por el director del Centro de Comunicaciones Gubernamental (GCHQ), se apreciaba que las amenazas cibernéticas son reales y creíbles e indicaba que el RUGB debe prepararse para participar en una serie de operaciones ofensivas cibernéticas para proteger sus intereses.

Correspondiente a ello, la Estrategia de Seguridad Británica, publicada en octubre de ese año, identificará por vez primera a la amenaza cibernética, entendida como un ataque hostil sobre el ciberespacio nacional por otros Estados o por el crimen organizado como uno de los cuatro riesgos de nivel I (de mayor probabilidad e impacto), junto a acciones del terrorismo internacional, un accidente importante o un desastre natural que precisa una respuesta nacional, una pandemia o una crisis militar internacional entre estados, afectando al país y sus aliados, así como a actores estatales y no estatales.

Asimismo, protegerse frente a un ataque hostil sobre el ciberespacio nacional (IEEE, 2010).

En tal sentido, el RUGB cuenta con el Programa Nacional de Seguridad Cibernética, tendiente a ampliar los sistemas de protección de la seguridad cibernética, en el aseguramiento de la información (Information Assurance); en mejorar la detección y análisis de los ataques cibernéticos; en aumentar la cooperación con países aliados; y en la creación de una unidad cibernética conjunta en colaboración con el Ministerio de Defensa para desarrollar nuevas tácticas, técnicas y planes relativos a las operaciones militares.

Quien lleva adelante el Programa Nacional de Seguridad Cibernética, es una unidad cibernética conjunta entre el Ministerio de Defensa y el Centro de Comunicaciones Gubernamental (GCHQ). Asimismo, en noviembre de 2011 publicó su estrategia: *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world* (RUGB, 2011).

La Oficina de CiberSeguridad del Reino Unido ha expuesto que *“así como en el Siglo XIX tuvimos que consolidar la presencia en los mares para nuestra seguridad nacional y prosperidad y en el Siglo XX tuvimos que consolidar el aire, en el Siglo XXI tendremos que garantizar nuestra superioridad en el ciberespacio.”* (RUGB, 2011).

5.7 La ciberdefensa en Francia

El Libro Blanco sobre Defensa y Seguridad Nacional de Francia, aprobado por el Presidente de la República en junio de 2008, puso de relieve como nueva amenaza, el ciberespacio, centrándose en la seguridad de los “sistemas de información, centros nerviosos reales de nuestra sociedad”, donde “todos los sectores de actividades, ya sean estatales, industrial, financiero o comercial, dependen más de la tecnología y redes de comunicaciones electrónicas” se verían muy afectados por distinto tipo de disfunciones.

Esa apreciación distingue tres escenarios principales:

- Un ataque contra los sistemas informatizados que gestionan infraestructuras críticas como plantas nucleares, red ferroviaria o aeropuertos: para los militares, es plausible pensar que puedan provocar "en los próximos quince años", provocando destrozos similares o superiores a un bombardeo físico.
- Un ataque contra la parte visible de Internet, esto es, las webs y las intranets de administraciones clave, como presidencia, policía, impuestos y hospitales. El hundimiento de esas páginas provocaría caos y desprestigio de un Estado ante sus ciudadanos y ante las potencias extranjeras.
- la integración de cualquiera de esos ataques informáticos en el marco de una secuencia clásica de guerra convencional.

Frente a esta amenaza creciente y aún más insidiosa, el Libro Blanco destacó la necesidad de dotar a Francia con una capacidad de defensa equipo activa, capaz de

detectar y contrarrestar los ataques, recomendando crear agencia nacional responsable. Así, a mediados de 2009 se crea, dependiente del el Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) la Agencia Nacional para la Seguridad de Sistemas de Información (ANSSI) con la misión de proteger los sistemas nacionales de información y proponer las normas que deben aplicarse para la protección de los sistemas estatales y verificar la aplicación de las medidas adoptadas. Por medio del Centro Operacional de la Seguridad de Sistemas de Información (COSSI), se detectan y responden ataques y se vigilan las redes más sensibles de la administración y se desarrollan nuevas capacidades defensivas.

Por su parte el SGDSN mantiene dos planes de trabajo: el Plan Vigipirate de vigilancia, prevención y protección, cuyo principal objetivo es la preparación del Estado para la protección de la población, su infraestructura y sus instituciones, y el Plan de Piranet, complementario del anterior, en respuesta a amenazas o ataques a gran escala utilizando medios específicos de agresión o que afectan a los entornos particulares, donde se requiere la intervención del estado en una grave crisis, constituyéndose así en uno de los pilares de la estrategia de esa defensa (SGSN, 2014). Cabe destacar que en 2012 se anunció que en la escuela interarmas del Ejército francés Saint-Cyr Coëtquida se estableció un centro de conocimientos de ciberdefensa (Defense Systems, 2012).

En febrero de 2011, la ANSSI presentó la Estrategia nacional de Ciberseguridad de Francia que establece objetivos que procurarán convertir a Francia "*en una potencia mundial en defensa cibernética con mantenimiento de su independencia estratégica*", cooperando con naciones líderes en la defensa cibernética; salvaguardar la capacidad del país para tomar decisiones protegiendo las comunicaciones en crisis, proteger las infraestructuras nacionales críticas, evitando ataques (ANSSI, 2011).

Desde 2011 en materia de ciberdefensa el denominado Oficial General de la Ciberdefensa es el encargado de coordinar las acciones del ámbito de la Defensa y sirve de interfaz principal en caso de producirse una crisis cibernética.

En 2013, el Gobierno francés dio a conocer su actualización del Libro Blanco sobre Defensa y Seguridad Nacional y la Ley de Programación Militar, documentos los cuales determinan la orientación estratégica del sistema de defensa del país para el periodo 2014 a 2019. Como amenazas y riesgos consecuentes de la globalización:

aprecian los movimientos de bienes, mercancías y/o personas, los riesgos para la seguridad marítima en el marco del aumento de la piratería, los riesgos terroristas y, entre otros "el incremento exponencial de los riesgos mediante ciberataques contra las infraestructuras digitalizadas y las amenazas que pueden dirigirse contra el espacio extra-atmosférico" (Fuente Cobo, 2016).

El 16 de octubre 2015 se dio a conocer la Estrategia Nacional para la Seguridad en el Ámbito Digital. El documento, coordinado por la ANSSI establece y actualiza objetivos para el Secretario de la Defensa y la Seguridad Nacional, respondiendo a los nuevos desafíos que nacen de la evolución de los usos digitales y amenazas (ANSSI, 2015).

Cabe destacar que, tras los atentados terroristas de París, el Presidente Hollande en su mensaje a la Asamblea Nacional del 16 de noviembre de 2015, expuso que "*el ejército francés aumentará su despliegue en ciberdefensa durante los próximos cuatro años, hasta 2019*" y que se aumentará las medidas en torno al control de las comunicaciones electrónicas, ya que no se puede luchar en estado de guerra contra lo que se tenía hace años.

5.8 La ciberdefensa en Alemania

Desde 2006, el sistema de defensa de ese país posee una unidad militar de operaciones de red de computadoras (Computer Network Operations Unit - CNO) que está subordinada al comando estratégico de inteligencia militar, con sede en Bonn y centrada en la guerra cibernética, logrando capacidad inicial para operar en redes hostiles y desarrollando simulaciones de ataques en un ambiente de laboratorio cerrado. El desarrollo de la capacidad alemana de ciber-defenderse y ciber-atacar debe ser considerado a la luz de ataques realizados contra redes gubernamentales durante los últimos años y que el país procura estar al nivel de otros países de la OTAN, como EUA, Francia y Gran Bretaña.

En 2011, el Gobierno a alemán dio a conocer su Estrategia de Ciberseguridad de Alemania**.** Por medio de la misma, se crea Centro Nacional de Ciberdefensa (NCA) que analizará los ataques recibidos por la Red de Internet y asistirá al Gobierno sobre la mejor

forma de combatirlos. El CNA supervisará en lo atinente a su misión las telecomunicaciones del Gobierno federal y tendrá la asistencia de otros organismos públicos en lo tecnológico, jurídico y policial (BMI, 2011).

En agosto de 2016, el Gobierno alemán dio a conocer su nuevo Libro Blanco de la Defensa, el cual realiza recomendaciones para mejorar las capacidades de ciberdefensa y mejorar la resiliencia de la población civil frente a crisis de seguridad.

5.9 La ciberdefensa en España

El 28 de enero de 2010 se aprueba el documento “Visión de la Ciberdefensa Militar", el cual orientará la definición, desarrollo y empleo de las capacidades militares del país para garantizar la eficacia en el uso del ciberespacio en las operaciones militares. Resultado de ello, en julio de 2011 se aprobará el “Concepto de Ciberdefensa Militar”, que definirá principios, objetivos y retos de la ciberdefensa en el ámbito militar y un año después de anunciará el “Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar”, el cual comenzará la coordinación de los esfuerzos entre el ámbito conjunto y específicos a partir del aprovechamiento de las estructuras existentes (MCCD, 2011).

El 19 de febrero de 2013, el Ministro de Defensa establece la creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) “*responsable de realizar el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional*” (Villanueva Barrios, 2014). Asimismo, el MCCD dirige y coordina la actividad de los centros de respuesta a incidentes de seguridad de la información del Ejército de Tierra, del Ejército del Aire y de la Armada, y el centro de operaciones de seguridad de la información del Ministerio de Defensa.

Formas de Acción del MCCD:

- De defensa: “… *protección de los sistemas de información y telecomunicaciones, y la información que manejan, frente a ciberataques y su recuperación en caso de fallo o inutilización, parcial o total*”.

- De explotación. “… *obtención de información sobre las capacidades cibernéticas de potenciales adversarios y agentes hostiles.”*

- De respuesta. “… *realización de acciones ofensivas como respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional*”.

Por su parte, el 5 de diciembre de 2013, el Consejo de Seguridad Nacional aprueba la Estrategia de Ciberseguridad Nacional de España.

La misma entiende que de los doce riesgos y amenazas para la seguridad nacional identificados, la ciberamenaza es una de las más recientes pero se ha convertido en una de las más preocupantes, donde “el ciberespacio es un nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, pero también ha diluido las fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas. La creciente dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito” (Caro Bejarano, 2013).

La estrategia expone como objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, así como la gestión de las infraestructuras críticas.

La estrategia española define el ciberespacio y sus características como un nuevo dominio global y dinámico que está compuesto por las infraestructuras TIC (Tecnologías de la Información y la Comunicación). Estas características de los ciberataques incluyen su bajo coste, la ubicuidad y fácil ejecución, su efectividad e impacto, y el reducido riesgo para el atacante. Asimismo, identifica como riesgos y amenazas a la Ciberseguridad Nacional aquellos provenientes de: individuos aislados, hacktivistas, amenazas internas, delincuentes, terroristas, estados extranjeros que se suman a los problemas causados por causas técnicas o fenómenos naturales.

Como principios rectores plantea: la unidad de acción; la anticipación y prevención; la eficiencia y sostenibilidad en el uso de los recursos; y la resiliencia o capacidad de resistencia y recuperación, para lo cual se requiere el liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional.

Define como objetivo global en el ámbito de la ciberseguridad “Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques”, para lo cual se requerirá una actualizada Política de Ciberseguridad Nacional.

En materia de Defensa expone la necesidad de “ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional”, consolidando la implantación del Mando Conjunto de Ciberdefensa y potencializando su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés así como las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional (Gobierno de España. 2013).

Cabe destacar que a fines de mayo de 2016, en la Base de Retamares de España, se desarrolló el I Foro Iberoamericano de Ciberdefensa organizado por el Mando Conjunto de Ciberdefensa (MCCD). Al mismo asistieron representantes de los diferentes organismos de Ciberdefensa de Argentina, Brasil, Chile, Colombia, España, México, Perú y Portugal. Tambien estuvieron invitados representantes de Ecuador y Paraguay los cuales no pudieron asistir por problemas de agenda.

En el encuentro se identificaron actividades de colaboración y apoyo en materia de capacitación, ejercicios, intercambio de información, investigación y desarrollo e innovación en materia de Ciberdefensa. Estas propuestas fueron plasmadas en una Carta de Intenciones, suscripta por los representantes de todos los países asistentes, lo que constituyó el inicio de programa multilaterial en la materia.

5.10 La ciberdefensa en Naciones Unidas

En Julio de 2015, el Grupo de Expertos Gubernamentales da a conocer un informe ante la Asamblea General titulado Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

El grupo expuso que las TICs han producido profundos cambios en las economías, las sociedades y las relaciones internacionales. Así, el ciberespacio afecta a todos los aspectos de la vida, otorgando innumerables ventajas pero también generando grandes riesgos. El ciberespacio solo podrá ser un entorno estable y seguro por medio de la cooperación internacional, sustentado en el derecho internacional y los principios de la Carta de las Naciones Unidas.

Los expertos de 20 países concluyeron que existen tendencias preocupantes en el entorno mundial de las TIC, fundamentalmente debido al aumento de incidentes relacionados por el uso malintencionado de Estados o particulares lo que puede incidir en la paz y la seguridad internacional lo que atañe al posible desarrollo de conflictos entre Estados mediante el uso de las TICs.

En materia de ciberataques apreciaron el ataque a infraestructuras críticas estatales, especialmente con fines de terrorismo, lo que podría amenazar la paz y la seguridad internacional dado que además existen diferencias en los niveles de capacidad que tienen los Estados en la esfera de la seguridad de las TIC, lo que puede aumentar la vulnerabilidad en un mundo interconectado. Asimismo, el Grupo tomó nota de la propuesta de China, la Federación de Rusia, Kazajstán, Kirguistán, Tayikistán y Uzbekistán de un código internacional de conducta para la seguridad de la información

El Grupo de expertos brindó recomendaciones para el examen por los Estados de normas, reglas y principios voluntarios y no vinculantes de comportamiento responsable de los Estados con miras a promover un entorno abierto, seguro, estable, accesible y pacífico en la esfera de las TIC:

a) Los Estados, en consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, deberían colaborar en la elaboración y aplicación de medidas para incrementar la estabilidad y la seguridad en el

uso de las TIC y evitar las prácticas en la esfera de las TIC que se consideran que son perjudiciales o que pueden poner en peligro la paz y la seguridad internacionales;

b) En el caso de incidentes relacionados con las TIC, los Estados deberían tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías, así como la naturaleza y el alcance de las consecuencias;

c) Los Estados no deberían permitir deliberadamente que su territorio fuera utilizado para la comisión de hechos internacionalmente ilícitos mediante la utilización de las TIC;

d) Los Estados deberían estudiar cuál es la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines terroristas o delictivos y aplicar otras medidas de cooperación para hacer frente a tales amenazas. Quizás los Estados deberían considerar si existe la necesidad de elaborar nuevas medidas a este respecto;

e) Los Estados, para garantizar la utilización segura de las TIC, han de acatar las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión;

f) Un Estado no debería realizar ni apoyar de forma deliberada actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañaran intencionadamente infraestructuras fundamentales que prestan servicios al público o dificultaran de otro modo su utilización y funcionamiento;

g) Los Estados deberían tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, teniendo en cuenta, la resolución 58/199 de la Asamblea General sobre la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales y otras resoluciones pertinentes;

h) Los Estados deberían atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales fueran objeto de actos malintencionados relacionados con las TIC. Los Estados también deberían atender las solicitudes

apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía;

i) Los Estados deberían adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro con miras a que los usuarios finales confiaran en la seguridad de los productos relacionados con las TIC. Los Estados deberían tratar de evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC, así como el uso de funciones ocultas y dañinas;

j) Los Estados deberían alentar la divulgación responsable de las vulnerabilidades relacionadas con las TIC y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o infraestructuras dependientes de esas tecnologías;

k) Los Estados no deberían realizar ni apoyar de forma deliberada actividades que dañaran los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias cibernéticas o equipos de respuesta a incidentes de seguridad informática) de otro Estado. Un Estado no debería utilizar equipos autorizados de respuesta a emergencias para participar en una actividad internacional malintencionada.

5.11 OEA - Estrategias Hemisféricas frente a la PIC y la ciberseguridad.

Diversos acuerdos celebrados en los últimos años por los países del Hemisferio en la Organización de los Estados Americanos (OEA) han definido una concepción común, estableciendo (Ortiz, 2008):

- Un “Enfoque Multidimensional de la Seguridad Hemisférica”. Las amenazas, preocupaciones y otros desafíos a la seguridad en el Hemisferio son de naturaleza diversa y alcance multidimensional y el concepto y los enfoques tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales.

A los fines de este enfoque, entre las nuevas amenazas se identifican el ciberterrorismo y "los ataques a la seguridad cibernética". Se acuerda desarrollar una estrategia integral sobre seguridad cibernética para responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas. (OEA, 4 de junio de 2002)

- Contar con "diferentes medios de alerta anticipada que permitirían actuar tratando de evitar atentados a la seguridad y la consiguiente generación de inestabilidad", y fortalecer la coordinación interinstitucional e intergubernamental y de los regímenes de seguridad y defensa en la región que permitan la protección de la población y la estabilidad y la paz", V Conferencia de Ministros de Defensa de las Américas (Santiago de Chile, noviembre de 2002).

- Establecer una lista de medidas para el fomento de la confianza en materia de seguridad para ser adoptadas a nivel bilateral, subregional y regional, que incluye medidas políticas, diplomáticas, educativas y culturales, militares y otras no militares, Comisión de Seguridad Hemisférica de la OEA (2003).

- Definir la existencia de amenazas a la seguridad cibernética hemisférica. Comité Interamericano contra el Terrorismo (CICTE) (julio de 2003).

- Proteger la Infraestructura Crítica para salvaguardar las telecomunicaciones y redes de computadoras, Seminario sobre Seguridad Cibernética de la OEA (Buenos Aires, julio de 2003).

- Aprobar una Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernetica que establece la necesidad de conformar una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones y sus redes y sistemas de información en respuesta a los ciber-incidentes (OEA, 8 de junio de 2004).

- Crear de una “Red Interamericana de Seguridad Cibernética”, por medio de grupos nacionales de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSRITs) para identificar y luchar contra las amenazas emergentes creando una red interamericana de vigilancia y alerta sobre seguridad cibernética (OEA, 2005).

- El Grupo sobre Ciberseguridad y las Infraestructuras de Información esenciales regional de la Comisión Interamericana deTelecomunicaciones (CITEL) publicó en el año

2005 el “Libro Azul: Políticas de Telecomunicaciones para las Américas” donde expone que la cooperación internacional es un elemento clave para proteger las infaestructuras de información esenciales” necesitándose la coordinación de sistemas de alerta temprana, analizar información sobre vulnerabilidades, amenazas o incidentes y coordinar investigaciones sobre ataques contra dichas infaestructuras de conformidad con las leyes nacionales.

- Definir “la Infrestructura Crítica en el Hemisferio”. La OEA definió como infraestructura crítica a "entre otras, en aquellas instalaciones, sistemas, y redes, así como servicios y equipos físicos y de tecnología de la información cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, la gobernabilidad democrática, o el eficaz funcionamiento del gobierno de un Estado miembro" (Panamá, 1 de marzo de 2007).

- Identificar infraestructuras críticas. El 14 de marzo de 2007, Arístides Royo, representante de Panamá ante la OEA y Presidente del CICTE, indicó que ese organismo presentará pronto su plan de trabajo para que se identifiquen las áreas relativas a la infraestructura crítica, tanto desde la perspectiva física, portuaria etc, como de los denominados espacios virtuales, para brindar seguridad al comercio y transporte global.

- “Declaración de Fortalecimiento de la Seguridad Cibernética en las Américas” de 2012, donde se expone la importancia que los Estados Miembros participen en la Red de Seguridad Hemisférica de los CSIRT y de Autoridades en Seguridad Cibernética, así como que aumenten el intercambio de información entre los Estados Miembros y la cooperación relacionada con la protección de infraestructura de información crítica, y para la prevención y respuesta a incidentes de ciber seguridad y la importancia de reforzar la seguridad y la resistencia de tecnologías de infraestructura crítica de información y comunicaciones (TIC) ante las ciber amenazas, con especial énfasis en las instituciones gubernamentales críticas así como en los sectores críticos para la seguridad nacional, incluyendo los sistemas de energía, financieros, transporte y telecomunicaciones.

Asimismo, los Estados miembros se comprometen a continuar desarrollando estrategias nacionales de seguridad cibernética integrales e involucrar a todos los actores pertinentes en su desarrollo e implementación y promover la cooperación del sector

público con el privado y académico para fortalecer el resguardo y la protección de dicha infraestructura crítica de información y comunicaciones.

- Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas de 2015 el cual indica que los ataques a la infraestructura crítica se han convertido en una importante preocupación para los gobiernos y proveedores privados de todo el mundo – ya sean ataques cometidos por criminales cibernéticos que buscan tener ganancias financieras o por hackers como actos políticos que buscan socavar la credibilidad de los gobiernos y las compañías. El reporte expone que los ataques a la infraestructura crítica se han vuelto más comunes y sofisticados y continuarán creciendo en el futuro inmediato y que la gestión y el monitoreo de los sitios ha mejorado en las instalaciones de la infraestructura crítica gracias a que éstas se conectan cada vez más agresivamente a Internet. Sin embargo, advierte que "la conveniencia de la conectividad ha convertido la superficie de ataques una vez limitada de estas industrias en un campo fértil para los ataques cibernéticos".

Una encuesta realizada por la OEA para este informe y a nivel hemisférico indica un incremento específico de los ataques a la infraestructura crítica (43%) mientras que un alarmante 31% dijo que no estaban seguros de haber sido atacados. Asimismo, la sofisticación de los ataques (76% dicen que se están volviendo más sofisticados) los cuales son difíciles de detectar.

Cabe destacar que a partir de 2016, la Junta Interamericana de Defensa (JID), dependiente de la OEA, ha incorporado el tratamiento de la temática de ciberdefensa en sus actividades al apreciar que "la seguridad en el hemisferio se ve afectada por amenazas de naturaleza transnacional que requieren respuestas del sector público y del sector privado en coordinación con la sociedad civil" que incluye la necesidad de conformar programas de capacitación común en la materia, conforme lo expuesto por el propio Vicepresidente del Consejo de Delegados de la JID, General Jaime González Avalos, al expresar en un reportaje que desarrollarán los mismos en materia de "desminado humanitario con las autoridades de la organización de las Naciones Unidas y tenemos previsto presentar y desarrollar estos ejercicios en toda la temática de amenazas complejas, o sea, desastres naturales, cambio climático, impactos en el medio ambiente, crimen organizado, ciberdefensa, derechos humanos" (Ommati, 2016).

5.12 Ciberseguridad en América Latina y el Caribe

En marzo de 2016, el Observatorio de la Ciberseguridad en América Latina y el Caribe, coordinado en conjunto por la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo publicaron el informe “Ciberseguridad, ¿estamos preparados en América Latina y el Caribe?” (BID, 2016).

El mismo, estima que los delitos cibernéticos cuestan a América Latina y el Caribe alrededor de 90.000 millones de dólares al año. Asimismo, al costo económico se le agrega la creciente vulnerabilidad de nuestra privacidad en línea y nuestros datos personales.

El reporte aprecia los avances en el diseño de estrategias, pero entiende que se requiere de una respuesta urgente y, dado que no reconoce fronteras, de forma coordinada entre los países de la región.

Al respecto, destaca que de la región, solo dos países han adherido a la Convención de Budapest, solo seis han adoptado estrategias de seguridad cibernética, contando solo uno de cada tres con un centro de comando y control de ciberseguridad. Por tal motivo, hay carencia de mecanismos formales para denunciar incidentes y los mecanismos formales de intercambio de información.

América Latina presenta no solo una infraestructura terrestre informacional, sino también submarina por lo que todo lo referido a “los cables submarinos es fundamental, porque plantea las problemáticas tradicionales de la organización de las infraestructuras de comunicación en América Latina y su vínculo con una serie de riesgos importantes” (Martín, 2015, pp 9 a 15), conforme se presenta en el siguiente mapa de los cables submarinos de comunicación:

Tomado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

Así, la seguridad en la región presenta grandes desafíos, sea por la misma infraestructura y su gran área de desenvolvimiento como así también por parte de las medidas gubernamentales. En tal sentido si bien hubo avances en la materia, todavía no existe un catálogo completo de identificación de infraestructuras críticas, contramedidas preventivas frente ataques a ellas así como estudios pormenorizados y sistemáticos que permitan “ilustrar la complejidad actual del ejercicio de medición de riesgo cibernético para América Latina” donde además habría que “detenida y separadamente la situación específica presentada por cada zona geográfica del continente latinoamericano” (Martín, 2015, pp 15 a 16).

5.13 Unión de Naciones Suramericanas (UNASUR)

En 2012, la UNASUR aprobó el Plan de Acción correspondiente a ese año, donde en el eje de “Políticas de Defensa” abarca, en su punto 1.F, la “conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa”, siendo responsable la República del Perú en el marco de aportes a las políticas de defensa que implementa el Consejo de Defensa Suramericano (CDS).

Asimismo, el Plan de Acción del 2013, en materia de “Políticas de Defensa”, postuló como actividad a desarrollar por el referido el grupo de trabajo la posibilidad de “establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa”.

Por su parte, en la I Declaración de Paramaribo, Surinam, del 30 de agosto del año 2013, los países miembros instruyeron “al Consejo de Defensa Suramericano y al COSIPLAN a evaluar la cooperación con otros consejos ministeriales competente y avanzar en sus respectivos proyectos de defensa cibernética y la interconexión entre redes de fibra óptica en nuestros países con vistas a tornar más seguras nuestras telecomunicaciones.

Promover el desarrollo de tecnologías regionales y la inclusión digital. Saluda el interés del MERCOSUR en estrechar su coordinación con la UNASUR sobre esos temas e instruye al CDS y al COSIPLAN a trabajar regularmente en coordinación con el recién creado Grupo de Trabajo de MERCOSUR, responsable por asuntos de telecomunicaciones, y a enviar un informe con las recomendaciones sobre posibles avances en la materia durante la Reunión Ordinaria de la UNASUR”

En 2014, en la V Reunión Ordinario del Consejo de Defensa Suramericano se ratificó la necesidad de avanzar en las coordinaciones regionales en materia de ciberdefensa y aprobaron el Plan de Acción 2014, el cual incluye por vez primera una actividad de capacitación en materia de defensa cibernética, mediante la realización de un Seminario Regional de Ciberdefensa.

El Seminario, desarrollado en Buenos Aires[25], del 14 al 16 de mayo de 2014, contó con expositores expertos de países de la región, y de España, Italia y EUA, quienes trataron temas en materia de infraestructuras críticas y seguridad de la información, a los ecosistemas de computación en la nube, a la seguridad de las comunicaciones y a las tecnologías de la información y de las comunicaciones.

En concordancia con el Seminario se desarrolló la tercera reunión del Grupo de Trabajo de Ciberdefensa del Consejo de Defensa Suramericano, el cual, por consenso, anunció la necesidad de desarrollar cuatro puntos básicos:

1. Crear un foro regional del Grupo de Trabajo de Ciberdefensa de los Estados Miembros, a fin de intercambiar conocimientos, experiencias y procedimientos de solución.
2. Establecer una red de contactos de autoridades competentes para el intercambio de información y colaboración de manera permanente.
3. Definir la plataforma y procedimientos de comunicaciones de la red de contactos.
4. Profundizar y sistematizar la reflexión sobre definiciones conceptuales de ciberdefensa y ciberseguridad (Declaración de Cartagena del Consejo de Defensa Suramericano, 2014).

5.14 Situación en materia de ciberdefensa en algunos países de la región.

Brasil

En América Latina, además de los desarrollos en Chile y Colombia, se destaca la República Federativa de Brasil.

La Estrategia de Defensa Nacional de Brasil de 2008, ya promovía y desarrollaba tres sectores de importancia estratégica: el espacial, el cibernético y el nuclear.

En cuanto al eje cibernético, la directriz ordena que las capacidades militares relativas a la ciberdefensa se dirijan a los ámbitos industrial, educativo y militar. Como

[25] Tres integrantes del equipo de investigación, participaron junto al Secretario de Investigación de la ESG del Seminario Regional de Ciberdefensa de la UNASUR.

prioridad, se incluirán las tecnologías de la información entre todos los contingentes de las Fuerzas Armadas para garantizar su actuación en red. En el año 2009, el Ministerio de Defensa, por medio de la Directriz Ministerial N° 14, designó para cada sector estratégico una fuerza responsable, con el fin de lograr una coordinación de acciones entre los mencionados sectores. Entonces, la Marina pasó a ser la encargada del área correspondiente a las actividades nucleares, la Fuerza Aérea se ocuparía del ámbito espacial, y el Ejército Brasilero del ambiente cibernético.

En 2010 el Departamento de Seguridad de la Información y Comunicaciones publicó la Guía de Referencia para la Protección de Infraestructuras Críticas de Información y el Libro Verde de Seguridad Cibernética en Brasil.

Por su parte, ese mismo año, el Ministerio de Defensa del país dispuso la creación en el ámbito del Ejército el Centro de Defensa Cibernética (CDCiber) con la misión de profundizar las amenazas, establecer una doctrina nacional sobre el tema y perfeccionar los medios de defensa contra esas amenazas. El mismo comenzó a desarrollar sus actividades de modo estratégico a partir de septiembre de 2012. Asimismo, la nueva Estrategia de Defensa Nacional del año 2012 reafirmará la significación de continuar desarrollando el sector cibernético detentado por las Fuerzas Armadas.

El 27 de diciembre de 2012, Brasil publicó su Política Cibernética de Defensa, la cual fue en previsión de brindar seguridad en ese campo al normal desarrollo del Campeonato Mundial de Futbol de 2014 y a los Juegos Olímpicos previstos para 2016.

El documento expone la actividad del cibercomando en el nivel estratégico y en los niveles operativos y tácticos así como el monitoreo respecto de la consecución de los objetivos, para “asegurar la utilización del espacio cibernético impidiendo o minimizando los efectos de ciberataques contra los intereses del país” y entendiendo que la ciberdefensa consiste en adoptar acciones defensivas, exploratorias y ofensivas, en el marco de una planificación militar, con el fin de proteger los sistemas de información, obtener datos para producir conocimiento e inteligencia, y eventualmente causar daños a los sistemas de información enemigos.

Asimismo, propicia la “Producción de Conocimiento de Inteligencia” para crear “Estructuras de Inteligencia Cibernética” para detectar amenazas, reales y potenciales de carácter interno o externo. Entre las medidas se destacan la creación bajo la

responsabilidad del EMC del Comando de Defensa Cibernética y de la Escuela Nacional de Defensa Cibernética. Asimismo, la Secretaría General del Ministerio de Defensa será responsable de decidir acerca de los recursos presupuestarios y de personal e infraestructura. Por su parte, el Ejército desarrollará la activación del Núcleo de Comando de Defensa Cibernética.

En enero de 2015 se aprueba la Estrategia General de Tecnología de la Información y las Comunicaciones (EGTIC) que incluye como instrumento para su gestión el establecimiento de la Dirección de Tecnología de la Información y Comunicaciones (TIC).

En mayo de 2015 el Gabinete de Seguridad del Gobierno de Brasil presenta la Estrategia de Seguridad de la Información y las Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal 2015-2018. Esta estrategia determina las atribuciones de los órganos del Estado en la elaboración de políticas y acciones en materia de protección de infraestructuras críticas gubernamentales y de la industria en general, especialmente en materia de empresas de defensa.

Actualmente, Brasil posee diversos Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que van desde entidades administradas por el gobierno a equipos del sector privado o académicos. El Comité Gestor de Internet en Brasil (CGI.br) es el encargado de coordinar todas las iniciativas de servicios de Internet en el país y el Centro de Información de la Red Brasileña (NIC.br) trabaja para implementar este tipo de iniciativas.

Asimismo, el equipo Nacional de Respuesta a Incidentes Informáticos de Brasil (CERT), que opera bajo el CGI.br y el NIC.br, tiene a su cargo la respuesta y coordinación a incidentes, capacitación y campañas de concientización. En materia de Administración Pública, el Departamento de Seguridad de Información y Comunicaciones posee otro Centro en respuesta a incidentes en ese sector.

Colombia

El 11 de abril de 2016, el Consejo Nacional de Política Económica y Social de Colombia (CONPES), dio a conocer la nueva Política Nacional de Seguridad Digital que

actualiza su antecesora de 2011, que había fijado política a 2015 y otorgaba responsabilidades al ejército y la Policía colombiana. La misma fue elaborada por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación.

El documento expresa “la ausencia de una visión estratégica basada en la gestión de riesgos” ya que considera que “actualmente el país no cuenta con una instancia de coordinación nacional en seguridad digital que optimice la gestión de los recursos destinados a esta materia”. Por tal motivo, se hace imposible tener “una visión estratégica, que articule las funciones y actividades de la institucionalidad existente en torno a los objetivos nacionales en seguridad digital”, lo que redunda en duplicar esfuerzos y tener menor eficiencia. (CONPES, 2016)

Por tal motivo, la nueva Política incluye y obliga a todas las entidades del Estado y todos actores los involucrados a comenzar a prevenir y mitigar los riesgos informáticos. Para tal fin, el Ministerio de TIC realizará una guía para que todas las áreas del Estado sepan identificar, clasificar y gestionar su riesgo informático.

Asimismo, plantea desarrollar campañas de concientización a los ciudadanos sobre los riesgos informáticos y la forma de prevenirlos. Otro tema que prevé es aumentar las capacidades técnicas de ciberdefensa y desarrollar el Ministerio de Defensa una estrategia de protección de la infraestructura crítica para los sistemas energético y financiero. De esta manera, Colombia sigue liderando el ámbito regional. En 2014, el índice mundial de ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), ubicaba al país se ubicaba en el quinto lugar del ranking de países avanzados en materia de ciberseguridad y ciberdefensa a nivel regional, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay.

Cabe destacar, que siguiendo a Brasil, en 2015, el Ministerio de Defensa Nacional elaboró la Guía para la Identificación de Infraestructura Crítica Cibernética.

Para las autoridades, el año 2015 marcó el inicio de un cambio significativo hacia nuevas amenazas cibernéticas más difíciles de detectar, “lo que significa una mayor incertidumbre frente a la seguridad digital a nivel global”. Por tal motivo, se suman como riesgos asociados a dicha incertidumbre (bases de datos o sistemas de información), “la

infraestructura física nacional, como hidroeléctricas, redes de energía, sistemas portuarios, sistemas de defensa, o armamento de guerra, entre otros, que utilizan redes de comunicaciones como base para su funcionamiento. Lo que se conoce como infraestructuras críticas nacionales”. En tal sentido, el documento refiere a la posibilidad que terroristas puedan apagar la captación de agua de una hidroeléctrica o tomar el control de aviones no tripulados, armas y sistemas de orientación de las fuerzas militares para causar daño a la población o, incluso, a las mismas instalaciones militares.

La Política dispone que ente entre junio y octubre de 2016, el Ministerio de Defensa Nacional elaborará “un plan de fortalecimiento que permita al sector Defensa generar una autonomía cibernética conducente a identificar, detectar y atender posibles amenazas en contra del Estado y su infraestructura critica”, procurando mejorar las capacidades de las Unidades Cibernéticas de las Fuerzas Militares e incluirá dos estudios de viabilidad técnica para la conformación de un Centro de operaciones cibernéticas de las Fuerzas Militares, y de un Centro nacional de protección y defensa de infraestructura crítica cibernética nacional.

Chile

El 10 de abril de 2015 el gobierno de Chile dispuso la creación del Comité Interministerial de Ciberseguridad (CIC), constituido entre otros, por el Ministerio del Interior, el Ministerio de Justicia, el Ministerio de Relaciones Exteriores y el Ministerio de Defensa. Por medio de la disposición, el Ministerio de Defensa, tiene a su cargo la Secretaría Ejecutiva del CIC, a cargo del Subsecretario de Defensa. Asimismo, el CIC está conducido por el Subsecretario del Interior (Koch Merino, 2015).

El 21 de mayo de 2016, la Presidenta de Chile, Dra. Michelle Bachelet realizó la exposición Cuenta Pública, donde se refirió a los logros y planteó los objetivos de su gobierno.

En materia de política de defensa y, específicamente en relación a la ciberdefensa, el documento Cuenta Pública Sectorial, Ministerio de Defensa, indica que como principales logros alcanzados a mayo de 2016 en materia de ciberdefensa se destaca que se intensificó junto con otros ministerios “la participación en instancias internacionales

relativas a ciberseguridad y ciberdefensa, tanto a nivel bilateral, como multilateral, con el objeto de ampliar la cooperación y diálogo en este ámbito, y de participar más activamente en los debates sobre conflictos internacionales en el ciberespacio”. Asimismo indica que la Subsecretaría de Defensa “tuvo a su cargo la Secretaría Ejecutiva del Comité Interministerial creado con el fin de diseñar una Política Nacional de ciberseguridad y cuyo borrador fue preparado con la participación de diversos actores públicos, privados y de la sociedad civil”. Asimismo el documento indica que “se dio inicio al proceso de diseño de planes y políticas en materia de ciberseguridad para la Defensa Nacional, que servirá, entre otras cosas, para contar con una política de ciberdefensa que oriente la actualización y mejora de las capacidades de protección a la información y redes computacionales del Ministerio de Defensa y las Fuerzas Armadas” (Ministerio de Defensa de de Chile, 2016).

En el mismo sentido, el documento refiere a que “el Estado Mayor Conjunto inició el proceso para levantar el proyecto de ciberdefensa, el que se encuentra en la etapa final de diseño de perfil, la que señala un diagnóstico actual del escenario del Sistema de Seguridad Cibernética en la Defensa Nacional” y, a tal efecto, “se elaborará una política sectorial de ciberdefensa, que permita enfrentar los riesgos y amenazas propias del ciberespacio de acuerdo con las obligaciones constitucionales y legales de la Defensa Nacional”. Asimismo indica que “con la cooperación de las Fuerzas Armadas, y de las subsecretarías de esta cartera de Estado, se consolidará el trabajo en materias de ciberdefensa, para avanzar” en la etapa de factibilidad de un sistema de Mando y Control del Estado Mayor conjunto de las Fuerzas Armadas (Ministerio de Defensa de de Chile, 2016).

En ese marco, se ha presentado para el debate público el documento del gobierno “Propuesta de Política Nacional de Ciberseguridad de Chile (PNCS) 2016-2022”. El documento expone que la Subsecretaria de Defensa del Ministerio de Defensa, es “responsable de generar y mantener actualizada la planificación primaria y políticas correspondientes para enfrentar los desafíos que la ciberseguridad plantea para la Defensa Nacional, y de asegurar la correspondencia de la planificación secundaria con ésta” (Ministerio de Defensa de de Chile, 2016).

Por su parte, el documento indica que el Estado Mayor Conjunto y Fuerzas Armadas posee un rol “preventivo y reactivo” y su misión es “proteger su propia insfraestructura de la información, además de colaborar en las tareas de ciberseguridad que correspondan en relación con la seguridad nacional y el sistema nacional de inteligencia”. Es asimismo responsable “como organismo de trabajo y asesoría permanente del Ministro de Defensa Nacional en materias que tengan relación con la preparación y empleo conjunto de las Fuerzas Armadas, y está a cargo de elaborar y mantener actualizada la planificación secundaria de la Defensa, junto con otras tareas relevantes para la ciberseguridad del país. Las Fuerzas Armadas, por su parte, están a cargo, acorde a la planificación realizada, de los planes institucionales y operativos que correspondan”.

La propuesta de política nacional estable en materia de defensa los siguientes aspectos:

- Política nacional de ciberdefensa: “Dado que las redes y sistemas de información de la Defensa Nacional constituyen una infraestructura crítica para la seguridad exterior y el ejercicio de la soberanía del país, y a las atribuciones constitucionales y legales de la Defensa Nacional, el Ministerio de Defensa, durante el año 2016 preparará y publicará políticas específicas de ciberdefensa, que contemplen las definiciones políticas en torno a cómo serán protegidas estas redes, y cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro, democrático y resiliente para el país” (Gobierno de Chile, 2016).
- “Política internacional para el ciberespacio: “es imprescindible que el país integre estos objetivos con otros tales como el desarrollo, los derechos humanos, la defensa y otros relacionados, para consolidarlos e integrarlos en la política exterior de Chile. Para ello, la presente política contempla una medida específica vinculada con la elaboración de una estrategia en estas materias por parte del Ministerio de Relaciones Exteriores, lo que a su vez es consistente y pone en marcha la medida Nº11 de la Agenda Digital 2020, que apunta a generar una visión país sobre gobernanza de internet”. La misma prevé contar con equipos de respuesta a incidentes de ciberseguridad y, entre los CSIRTs sectoriales, enfatiza que “se reforzará el actual de Gobierno y se creará uno específico para la Defensa Nacional. Por otra parte, deberá evaluarse la pertinencia de crear un CSIRT de

infraestructuras críticas” y el desarrollo de una industria de la ciberseguridad (Gobierno de Chile, 2016).

Uruguay

En la República Oriental del Uruguay, es responsable de la seguridad y defensa cibernética del país la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) dependiente de la Presidencia de la República, a través del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy).

Por su parte, dependiente del Ministerio del Interior, la Unidad de Delitos Cibernéticos de la Policía Nacional es el organismo que tiene a su cargo la investigación de los delitos cibernéticos.

Asimismo, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) creada en diciembre de 2005 es la oficina responsable de la implementación del Gobierno Electrónico del país de la cual dependen áreas de gestión de seguridad de la información, identificación electrónica y el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) creado en 2008.

Cabe destacar que en abril de 2015 se creó Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT), dependiente del Ministerio de Defensa Nacional (Camps. 2016).

Venezuela

Desde 2008 Venezuela dispone de un Sistema Nacional de Gestion de Incidentes Telematicos VenCERT con la finalidad de: “prevenir, detectar y gestionar los incidentes generados en los sistemas de informacion del Estado y en las infraestructuras críticas de la Nacion, a traves del manejo de vulnerabilidades e incidentes de seguridad informatica”. (Torres, 2015)

En mayo de 2015 por medio de la Resolución Nº 9722/15, el Ministerio de la Defensa del país desactivó la Dirección Conjunta de Seguridad Informática de la Fuerza Armada Nacional Bolivariana y por medio de la subsiguiente Resolución Nº 9723/15 crea la nueva Dirección Conjunta de Ciberdefensa (Dicociber) de la Fuerza Armada Nacional Bolivariana, adscrita al Comando Estratégico Operacional.

La Resolución prevé estructurar la nueva organización con los siguientes elementos: Director conjunto, Subdirector conjunto, Gestión administrativa, División de operaciones ciberdefensa, División de gestión de seguridad informática, Gestión de investigación y desarrollo y, División de redes sociales.

Argentina

El desarrollo de las TI en Argentina no es reciente. De hecho en los años 60 se destacó la incorporación en el Instituto del Cálculo de la Facultad de Ciencias Exactas de la Universidad de Buenos Aires el primer equipo de computación del país, basamento para el desarrollo de la primera carrera de estudios en la materia. Años después será el Centro Único de Procesamiento Electrónico de Datos (CUPED) instalado en el Ministerio de Bienestar Social en primer desarrollo a nivel gubernamental donde comenzaron a capacitarse investigadores y profesionales, único en su tipo de Hispanoamérica. Asimismo el desarrollo de la calculadora CIFRA bajo el auspicio de la empresa FATE y resultado de investigaciones de la Facultad de Ingeniería de la UBA constituyó el inicio del uso del microchip. Por su parte en el ámbito de la defensa a partir del establecimiento de la Junta de Investigaciones Científicas y Experimentales de las Fuerzas Armadas en 1958 se iniciarán desarrollos nacionales en ese sector.

En 1964 el Ingeniero Horacio Regnini realizó la primera conexión de una computadora entre Buenos Aires y el Instituto Tecnológico de Massachusetts (MIT), siendo una suerte de antecedente de la actual Internet. A partir de los años 80 se da inicio al consumo de hardware, destacándose la ampliación de uso de PC tipo "Comodore". Tras la caída del Muro de Berlín, Argentina debió adecuarse rápidamente al proceso de globalización, desarrollándose la desregulación de las telecomunicaciones propiciada

desde la Organización Mundial del Comercio a partir del entonces Plan de Liberalización de las Telecomunicaciones elaborado por la Secretaría de Comunicaciones el 10 de marzo de 1998, el cual contemplaba: telefonía Pública (desde marzo de 1998), telefonía Rural (desde junio de 1998), transmisión de datos con el Mercosur (1999), llamadas Locales, Larga Distancia e Internacionales (desde noviembre de 1999) y operadores de nuevas licencias (desde noviembre del 2000).

Esa primera etapa posibilitó el ingreso masivo de tecnología de comunicaciones de punta aunque muchos analistas identificaron la falta de una visión estratégica de los intereses nacionales y de la ciudadanía plasmado en normativas legales frente a inversiones que por su peso estratégico requerían de resguardos. Este andamiaje jurídico posibilitó el incremento del desarrollo de la web en el país.

En mayo de 1995 se venden las primeras conexiones comerciales a Internet en Argentina. Para el año siguiente más de 45.000 personas y 500 compañías navegaban por Internet. A fines de 1998 230.000 argentinos se conectaban a Internet. En diciembre de 2002 se estimaban en 4,1 millones los usuarios nacionales de Internet.

Según el estudio realizado en diciembre de 2014 por *Prince Consulting* para la OEA, indicaba que Argentina se encontraba entre los primeros países de la región en términos de adopción de las Tecnologías de Información y Comunicación (ITC).

El informe indicaba que las conexiones móviles que incluyen computadoras y tabletas conectadas, así como teléfonos inteligentes y otros aparatos celulares con paquetes de servicio de datos o Wi-Fi gratuito habían crecido a una tasa exponencial, llegando a 20 millones de conexiones a finales de 2014. Datos de la OEA y el BID de marzo de 2016, ampliaron esa cifra a alrededor de 28 millones de personas con acceso a internet y más de 66 millones de abonos a telefonía celular[26].

En tal sentido, Argentina se conecta cada vez más a Internet, tanto a nivel privado, individual y empresarial como gubernamental. Se destaca que la Administración Nacional de la Seguridad Social (ANSES) y la Administración Federal de Ingresos Públicos (AFIP) han digitalizado muchos de sus servicios al tiempo que muchos procedimientos y transacciones del Estado se realizan actualmente por Internet.

[26] Tomado de: http://observatoriociberseguridad.com/country/ar

Para fines de 2014, en el país existían 758 proveedores de servicios de Internet (ISP) y la industria de la telefonía móvil había cuadriplicado su tamaño desde 2003. Durante 2013, las autoridades nacionales observaron un aumento en el robo de identidad y el fraude a través de las redes sociales, el correo electrónico y la banca electrónica, deformaciones de sitios web y amenazas persistentes avanzadas (ATPs)

Esta infraestructura informacional proyectas desarrollo al tiempo que crea riesgos y vulnerabilidades. Argentina cuenta con un sistema nacional frente a estos desafíos.

El informe denominado "El estado de la banda ancha 2015", elaborado por la UIT con el respaldo de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco), fue publicado en Ginebra, Suiza, y reúne los datos de 191 países.

Según la UIT, Argentina es el segundo país de la región con mayor proporción de usuarios de Internet, con un 64,7%, sólo superado por Chile (72,4%), y seguido por Uruguay (61,5%) y Brasil (57,6%). Argentina también se encuentra entre los países latinoamericanos con mayor cantidad de personas conectadas a la banda ancha móvil, con un 53,6%, por detrás de Brasil (78,1%) y Uruguay (59,8%), y por delante de Chile (50,5%). Asimismo, el informe muestra que Argentina ocupa el cuarto puesto en la región (y 29 en el mundo) respecto de la cantidad de hogares conectados a la red, con el 52%. En este ranking es antecedido por Uruguay (57,4%), Costa Rica (55,1%) y Chile (53,9%), pero precede a Brasil, donde las conexiones hogareñas de banda ancha representan al 48 por ciento del total de hogares. Para fines del 2015, al menos un 65% de los argentinos accede a Internet y un 54% lo hace desde su teléfono celular, mientras que el 52% de los hogares del país se encuentran conectados por banda ancha, según un informe publicado por la Unión Internacional de Telecomunicaciones (UIT).

Por su parte, el informe resalta el desarrollo del Plan Nacional de Telecomunicaciones Argentina Conectada, lanzado en 2010, y que al presente construyó más de 30.000 kilómetros de fibra óptica en su Red Federal, alcanzando a más de 1.800 localidades del país.

En cuanto a la velocidad de conexión, en Argentina actualmente es de 3 megas, y se estima que se alcanzará en breve 8. Sin embargo, el promedio mundial, es de 34 megas, y el de América Latina, que es de 12 megas. Del 2011 al 2016 Chile pasará de tener 6,1 megas a 17 megas, mientras que Brasil de 4,9 megas a 14 megas.

La Coordinación de Emergencias en Redes Teleinformáticas (ArCERT)

La ArCERT, creada en mayo de 1999 en el ámbito de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros, es la unidad de respuesta (CSIRT) fue una de las primeras oficinas destinadas a centralizar y coordinar los esfuerzos para el manejo de los incidentes de seguridad que afectaren los recursos informáticos de la Administración Pública Nacional, ante cualquier ataque o intento de penetración a través de sus redes de información.

Desde ese entonces, la ArCERT difunde información con el fin de neutralizar dichos incidentes, en forma preventiva o correctiva, y capacita al personal técnico afectado a las redes de los organismos del Sector Público Nacional y centralizó los reportes sobre incidentes de seguridad en el sector público tendiente a facilitar el intercambio de información para afrontarlos, así como un servicio especializado de asesoramiento en seguridad de redes y coordina con otros organismos la prevención, detección, manejo y recuperación de incidentes de seguridad, poseyendo respuestas en materia de técnicas de defensa, dictando en noviembre de 1999 el primer curso de seguridad en redes.

ArCERT definió conceptualmente que las amenazas a la seguridad de la información atentan contra su confidencialidad, integridad y disponibilidad. Existen amenazas relacionadas con falla humanas, con ataques malintencionados o con catástrofes naturales. Mediante la materialización de una amenaza podría ocurrir el acceso modificación o eliminación de información no autorizada; la interrupción de un servicio o el procesamiento de un sistema; daños físicos o robo del equipamiento y medios de almacenamiento de información.

La Oficina Nacional de Tecnologías de Información (ONTI)

Por su parte, desde el año 2003, la Oficina Nacional de Tecnologías de Información (ONTI), dependiente de la Jefatura de Gabinete de Ministros, es el organismo responsable en la formulación de políticas y en la implementación del proceso

de desarrollo e innovación Tecnológica para la transformación y modernización del Estado, debiendo, entre otras acciones, entender en los aspectos relativos a la seguridad de la información digitalizada y electrónica del Sector Público Nacional, teniendo bajo su área Arcert.

La ONTI, el 3 de agosto de 2005, aprobó la primer "Política de Seguridad de la Información Modelo para el Sector Público" la cual establecía:

- Desarrollar una Política de Seguridad en cada Organismo, ISO/CEI 17799
- Asignar responsabilidades en materia de seguridad dentro del Organismo,
- Aumentar del nivel de seguridad en los Organismos del Estado.
- En materia de doctrina de Seguridad de la Información ya definía:

Información “a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro”.

Sistema de información “a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procesos, tanto automatizados como manuales”.

Incidente de Seguridad es “un evento adverso en un sistema de computadoras, o red de computadoras que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes, desarrollados por la Infraestructura de la Seguridad de la Información”. (ONTI, 2005)

Desde hace unos años, la División Delitos en Tecnología y Análisis Criminal de la Superintendencia de Investigaciones Federales de la Policía Federal Argentina (PFA) conforma un cuerpo de auxiliares de la Justicia especializados en telecomunicaciones y delitos en telemática.

Cabe destacar que en 2010 un ciberataque contra el sitio web de la Administración Federal de Ingresos Públicos (AFIP) produjo un fallo en la validación de datos y el acceso a los datos personales de los contribuyentes, tales como copia del DNI, firma y huella digital.

Marco Legal.

La Ley 25.326 de Protección de Datos Personales es la ley marco que regula la protección de los datos personales en Argentina, procurando garantizar el derecho al honor, a la privacidad y a la intimidad de la personas, y el acceso a la información que pueda registrarse sobre estas. Asimismo, establece los derechos de los titulares de los datos, las responsabilidades ligadas a los archivos y bancos de datos, los mecanismos de control, las sanciones y los procedimientos pertinentes.

Por su parte, obliga a los responsables o usuarios de datos a adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales; y prohíbe el registro de datos personales en archivos, registros o bancos que no reúnan las condiciones técnicas de integridad y seguridad necesarias y prohíbe la transferencia de datos personales a países u organismos internacionales que no proporcionen niveles de protección adecuados y sus respectivas excepciones.

En otro orden, obliga a los bancos de datos (públicos y privados) a estar registrados y a informar los medios utilizados para garantizar la seguridad de los datos y se encuentra sujetos ante la ley aquellos datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los archivos de las Fuerzas Armadas.

Por su parte, la Ley 26.388, promulgada el 24 de junio de 2008, modifica el Código Penal (CP), introduciendo los delitos informáticos, ya que modifica, sustituye e incorpora figuras típicas a diversos artículos del CP, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el CP, incorporando diversos delitos informáticos: distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

Así, tipifica, entre otros, los siguientes delitos informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP);
- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP);

- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP);
- Acceso a un sistema o dato informático (artículo 153 bis CP);
- Publicación de una comunicación electrónica (artículo 155 CP);
- Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP);
- Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP);
- Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data);
- Fraude informático (artículo 173, inciso 16 CP);
- Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP).

Las penas establecidas por la Ley son: a) prisión; b) inhabilitación (cuando el delito lo comete un funcionario público o el depositario de objetos destinados a servir de prueba); c) multa (ej. art. 155). Cabe destacar que el artículo 10 indica “incorporase como segundo párrafo del artículo 183 del Código Penal, el siguiente: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños”.

Asimismo, el 13 de noviembre de 2013 por medio de la Ley N° 26.904 se incorpora al Código Penal el siguiente artículo 131: “Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma”.

El Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad.

La Resolución 580/2011 establece el Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC) indicando la importancia del ciberespacio y las infraestructuras críticas para el Sector Público Nacional y el sector privado frente a “a constantes amenazas” “por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas”.

El Programa tiene como finalidad impulsar la creación y adopción de un “marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos inter jurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías”.

Para llevar adelante este proceso, el ICIC conformó cuatro grupos de trabajo:

- El Equipo de Respuesta ante Emergencias Teleinformáticas (CERT), a los efectos de brindar asistencia y asesoramiento en el análisis de los incidentes y formula recomendaciones para su tratamiento.
- El Grupo de Acción Preventiva (GAP), responsable del estudio de posibles fallas de seguridad y las acciones preventivas que posibiliten la reducción de incidentes de seguridad informática, propendiendo a desarrollar Políticas de Seguridad, de conformidad a las normas ISO 27.001 y 27.002.
- El grupo INTERNET SANO, para concientizar y capacitar en materia de ciberseguridad, especialmente entre niños y jóvenes (Justribó, Gastaldi y Fernández; 2014, pp 1 a 17).
- El Grupo de Infraestructuras Críticas de la Información (GICI), “responsable del relevamiento, identificación y clasificación de las infraestructuras estratégicas y criticas de información, del monitoreo de los servicios que el Sector Público Nacional brinda a través de Internet, de la coordinación de los ejercicios de respuesta ante un intento de vulneración de tales infraestructuras críticas, así como también de brindar asesoramiento sobre tecnologías de la

información y propiciar la articulación con el sector privado" (Justribó, Gastaldi y Fernández, 2014, pp 1 a 17).

Nueva Política de Seguridad de la Información de la ONTI - 2013

Por medio de la disposición 3/2013 se aprobó la nueva "Política de Seguridad de la Información. Modelo", la cual de conformidad a los Lineamientos Estratégicos del Plan Nacional de Gobierno Electrónico y los Planes Sectoriales de Gobierno Electrónico establece el alcance, especifica el para qué y qués es la seguridad de la información, sus requerimientos, evaluación de los riesgos de seguridad, factores críticos de éxito, términos y definiciones, recursos físicos y humanos, entre otros. (ONTI, 2013)

Atribuciones en la materia a la Agencia Federal de Inteligencia (AFI)

La Ley 27.126, sancionada el 3 de marzo de 2015, que crea la referida AFI, establece en su Artículo 7° que "será el organismo superior del Sistema de Inteligencia Nacional y dirigirá el mismo, abarcando los organismos que lo integran".

En su Artículo 6º, sustituye el artículo 8° de la ley 25.520 por el siguiente texto: Artículo 8°: "Las funciones de la Agencia Federal de Inteligencia serán las siguientes: La producción de inteligencia nacional mediante la obtención, reunión y análisis de la información referida a los hechos, riesgos y conflictos que afecten la defensa nacional y la seguridad interior, a través de los organismos que forman parte del sistema de inteligencia nacional" y "la producción de inteligencia criminal referida a los delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, ciberdelitos, y atentatorios contra el orden económico y financiero, así como los delitos contra los poderes públicos y el orden constitucional, con medios propios de obtención y reunión de información".

Asimismo, el Decreto PEN Nº 1311/15 aprueba la nueva Doctrina de Inteligencia Nacional, la cual contempla como otras acciones que atentan la seguridad interior las cuestiones referidas a la ciberseguridad.

La Ciberdefensa en la Defensa Nacional

La Ley 23.554 de 1988 define a la Defensa Nacional como la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes.

La responsabilidad primaria de las Fuerzas Armadas es la defensa ante agresiones militares estatales contra la soberanía e integridad territorial de la Nación. Se destaca que la ley 24.059 de Seguridad Interior determina el empleo de las fuerzas policiales y de seguridad de la Nación frente a acciones de naturaleza delictiva y establece que las Fuerzas Armadas solo pueden eventualmente, y cuando lo requiera el sistema de seguridad interior, enfrentar amenazas de naturaleza no militar (Sibilla, 2007).

A fines de 1998, el Ministerio de Defensa publica el "Libro Blanco de la Defensa Nacional" versión 1998, donde ya se analizaba que con la "revolución de los asuntos militares" (RMA) se supera el criterio de masa numérica como factor decisivo y surgía el concepto de "soft power", con tres ejes: información militar espacial, su procesamiento (sistemas C3I2) y armamento de precisión. Estos cambios generan un nuevo peligro: la amenaza sobre los sistemas informáticos propios. Posteriormente, en el año 2001 el Ministerio presenta la Revisión de la Defensa, que actualiza el documento anterior y

analiza perspectivas futuras de la Defensa Nacional, considerando que RMA está transformando el "arte de la guerra" donde tiene mayor protagonismo la tecnología informática. Esto implica la necesidad de cambios profundos en la tecnología utilizada para el desarrollo de sistemas de armas, las doctrinas militares, en el plano logístico, reservas y la forma de organización.

El documento establecía la necesidad de integrar los sistemas de C4I2 (comando, control, comunicaciones, computación, información e informática) de nivel estratégico nacional, militar y operacional, que permitan la conducción de las operaciones terrestres, navales y aéreas; intervenir en lo relativo a sistemas satelitales con aplicación en el área de la Defensa e integrar los sistemas de guerra electrónica de niveles estratégico nacional, militar y operacional y realizar operaciones terrestres, navales y aéreas de guerra electrónica.

Dependiente del Ministerio de Defensa, el entonces denominado Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas (CITEFA) (actualmente CITEDEF) desde hace décadas realiza investigación y desarrollo (I+D) en materia de comunicaciones, electrónica y defensa y seguridad informática, provee capacidades para el análisis de redes, pruebas de vulnerabilidad, configuración de servidores seguros, implementación de firma digital, configuración de firewalls, así como Proyectos de Investigación en Sistemas de Detección de Intrusiones. En el año 2004 es creado en el seno del entonces CITEFA el Laboratorio de Investigación y Desarrollo en Seguridad Informática (Si6)**.** Actualmente el Si6 desarrolla proyectos de investigación en: Detección, Clasificación e Identificación de Intrusos, Honeypots, Análisis de Patrones, Redes Privadas Virtuales (VPN), Firewalls, Firma Digital y Penetration Tests, entre otros.

En 2006, se comienza a atender a la ciberdefensa como política de defensa mediante distintas disposiciones. Así, el Decreto 727/06, fortalece el rol del Estado Mayor Conjunto de las Fuerzas Armadas (EMCO) como principal ejecutor de las decisiones estratégicas determinadas por la conducción civil y como último órgano militar encargado de ejercer las funciones de comando y organización de las fuerzas armadas. Su Jefatura VI - C3I2 (Comando, Control, Comunicaciones, Interoperabilidad e Informática) tiene como misión desarrollar y monitorear políticas, planes, programas y proyectos relacionados con los sistemas de C3I2 Conjuntos y Combinados. Desde la

década de los 80 existe una Doctrina Militar Conjunta en materia de Comunicaciones y Guerra Electrónica.

En actualizado Libro Blanco de la Defensa Nacional de 2010, en materia de ciberdefensa ya se planteaba la necesidad de una “estrategia de carácter defensivo”, “frente a una eventual agresión militar estatal externa, y para desarrollar eficazmente la conducción de las operaciones militares y repeler con éxito dicha agresión”, para lo cual era necesario desarrollar tecnologías “para mantener la continuidad operativa del ciberespacio que configura una nueva dimensión operacional” asegurando el uso y el control del “ciberespacio específico de los componentes del Sistema de Defensa Nacional, y aquellos ámbitos de interés estratégico asociados ante agresiones externas contra el ciberespacio nacional (ciberguerra)”.

Como se indicó al inicio, a fines de diciembre de 2014, el Ministerio de Defensa, mediante el Decreto Decreto 2645/14, pública la Directiva de Política de Defensa Nacional, donde entiende ciberespacio como:

> “**…** los usos militares de las novedosas tecnologías asociadas a la robótica, cibernética, sensores remotos, entre otros desarrollos en materia de ciencia y tecnología, han impulsado nuevas formas de librar la guerra que exhiben un salto cualitativo hacia un nuevo paradigma tecnológico. … Otro aspecto asociado al nuevo paradigma tecnológico y a las tecnologías de la información es la importancia que está adquiriendo el ciberespacio para el desarrollo de las operaciones militares. La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la ‘guerra real’ y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también el ciberespacial. Éste no constituye un ‘espacio en sí mismo’, sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias”.
>
> La misma PDN expone que:

“los usos militares de las novedosas tecnologías asociadas a la robótica, cibernética, sensores remotos, entre otros desarrollos en materia de ciencia y tecnología, han impulsado nuevas formas de librar la guerra que exhiben un salto cualitativo hacia un nuevo paradigma tecnológico. El empleo de aviones no tripulados en los teatros de operaciones es el ejemplo más cabal de esta tendencia. De igual modo, estos cambios traen aparejados también modificaciones sustanciales sobre la profesión militar, en el sentido de representar no sólo novedosas técnicas en el empleo de los sistemas de armas, sino también al modificar la tradicional configuración del campo de batalla, el rol del soldado y de las operaciones” ... “Otro aspecto asociado al nuevo paradigma tecnológico y a las tecnologías de la información es la importancia que está adquiriendo el ciberespacio para el desarrollo de las operaciones militares. La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la “guerra real” y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también al ciberespacial. Éste no constituye un “espacio en sí mismo”, sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias. Si bien las acciones de ciberguerra poseen su origen en el ámbito virtual de las redes de comunicación y sistemas informáticos, sus efectos impactan sobre el mundo físico, pudiendo afectar, por ejemplo, el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, entre otros. Dentro de la amplia gama de operaciones cibernéticas, sólo una porción de éstas afectan específicamente el ámbito de la Defensa Nacional. En efecto, en materia de ciberdefensa existen dificultades fácticas manifiestas para determinar a priori y ab initio si la afectación se trata de una agresión militar estatal externa. Por tal motivo, resulta necesario establecer dicha calificación a posteriori actuando como respuesta inmediata el Sistema de Defensa únicamente en aquellos casos que se persiguieron objetivos bajo protección de dicho sistema, es decir que

poseen la intención de alterar e impedir el funcionamiento de sus capacidades" (Ministerio de Defensa de la República Argentina, 2014).

En materia de Planeamiento para la Defensa, la PDN determina que "durante el segundo Ciclo de Planeamiento de la Defensa Nacional, el planeamiento estratégico militar continuará elaborándose en base al conjunto de factores oportunamente establecidos para el ciclo recientemente concluido, a saber:
a) la vigencia de una concepción, posicionamiento y actitud estratégica de naturaleza defensiva y una disposición de carácter cooperativo;
b) la contribución al control efectivo de los espacios territoriales soberanos de la REPÚBLICA ARGENTINA en sus ambientes terrestre, marítimo, aeroespacial y su transversal dimensión ciberespacial;
c) la determinación final de aquellos aspectos y factores del INSTRUMENTO MILITAR que no fueron concluidos durante el primer Ciclo de planeamiento de la Defensa Nacional, orientándose dicho proceso a partir de toda la normativa vigente, en particular, por los instrumentos específicos ya sancionados de referencia inmediata en la materia (Resolución MD N° 414/11 y disposiciones pertinentes a tal efecto materializadas en el Plan de Capacidades Militares —PLANCAMIL 2011—); y
d) el desarrollo de capacidades operacionales en la dimensión ciberespacial con el objeto de adquirir competencias en los ambientes terrestre, naval y aéreo, así como de ciberseguridad de redes pertenecientes al Sistema de Defensa Nacional y respecto de los objetivos de valor estratégico que oportunamente sean definidos por el Nivel Estratégico Nacional. Asimismo, la DPN dispone que el Ministerio de Defensa "elaborará las normas para la creación de una instancia de naturaleza operacional en materia de Ciberdefensa, de acuerdo a lo previsto en el Plan de Capacidades Militares (PLANCAMIL 2011)" y "se procederá a la adhesión del MINISTERIO DE DEFENSA al "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad" de la OFICINA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN (ONTI) de la JEFATURA DE GABINETE DE MINISTROS". La DPN también ordena al "ESTADO MAYOR

> CONJUNTO DE LAS FUERZAS ARMADAS la elaboración de un Plan de Desarrollo de Ciberdefensa para el período 2014-2018". Por último establece que "en función del marco normativo y doctrinario del Sistema de Defensa Nacional de la REPÚBLICA ARGENTINA, se entenderá por "Ciberdefensa" a las acciones y capacidades desarrolladas por el INSTRUMENTO MILITAR en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo" y que en función de la "dimensión ciberespacial de los ambientes operacionales terrestre, naval y aéreo, según surge de la presente Directiva, el ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS deberá elaborar, por instrucción del MINISTERIO DE DEFENSA, un Plan de Desarrollo de la Ciberdefensa para el período 2014-2017. (Ministerio de Defensa de la República Argentina, 2014)

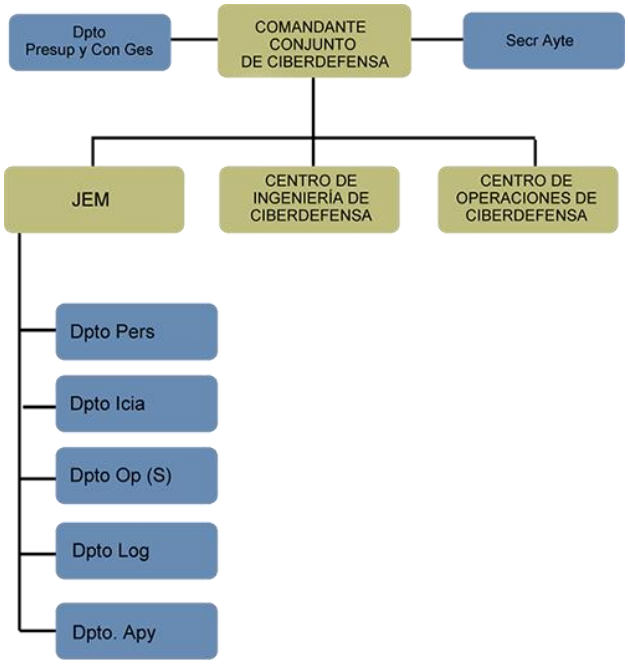
El Comando de Ciberdefensa

El 14 de mayo de 2014, el Ministerio de Defensa dispone la creación del Comando de Ciberdefensa dependiente del Estado Mayor Conjunto de las Fuerzas Armadas. En los considerandos de la Resolución, se dispone que el nuevo Comando como misión "ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el planeamiento estratégico militar y desarrollar capacidades frente a los ciberataques contra las infraestructuras críticas de la información y los activos del sistema de Defensa Nacional y de su Instrumento Militar". Asimismo, se instruye a los Jefes de los Estados Mayores de las tres FFAA para desarrollar capacidades de ciberdefensa en orden a contribuir con el referido Comando.

Las actividades desarrolladas por el comando se han centrado principalmente en:

- Determinar necesidades de equipamiento, comunicaciones y redes;
- Relevamiento de capacidades de cada fuerza,
- Análisis de proyectos de investigación y desarrollo en la materia; y

- Coordinación de los cursos de capacitación vinculados.



La ciberdefensa en el Libro Blanco de la Defensa 2015.

El nuevo Libro Blanco de la Defensa 2015, publicado por el Ministerio de Defensa a fines del mes de octubre, dedica varios espacios a la temática, entendiendo que el ciberespacio:

- "se convirtió en un nuevo dominio, creado por el hombre, en donde ocurren cada vez con mayor frecuencia interacciones sociales y donde el conflicto armado internacional, como fenómeno social, podría desarrollarse".

- "no es un ámbito militar operacional específico, sino que es una dimensión operacional transversal a los ambientes operacionales tradicionales en el que pueden desarrollarse operaciones de naturaleza militar, lo cual requiere un planeamiento militar conjunto".

- adquiere importancia "para el desarrollo de operaciones militares. Este ámbito artificial y sin precisa locación física no constituye un ambiente operacional específico sino otro, con medios y reglas propias, que atraviesa a los espacios terrestres, marítimos y aeroespaciales".

- por la potencialidad de afectarse infraestructuras críticas "demanda una rápida adaptación de los sistemas de defensa y el desarrollo de capacidades específicas en este singular ámbito operacional" (Ministerio de Defensa, 2015).

En el referido documento, el Ministerio de Defensa indica como principales lineamientos políticos en la materia: la coordinación de las diferentes capacidades y unidades especializadas generadas en el Ministerio, el EMCO y en las Fuerzas Armadas; mejorar los niveles en infraestructura y seguridad, incluyendo la normalización y aspectos técnicos; desarrollar vínculos de intercambio y cooperación a nivel nacional y promover las relaciones específicas en la materia tanto a nivel CDS - UNASUR, como a nivel bilateral con los países que la conforman, así como con la OEA y con países de la Unión Europea.

La Subsecretaría de Ciberdefensa del Ministerio de Defensa

Asimismo, el 4 de febrero de 2015 por Decisión Administrativa JGM N° 15/2015, se aprueba la estructura organizativa en de la Dirección General de Ciberdefensa dependiente del Ministerio de Defensa[27]. Su responsabilidad será la de intervenir en "el planeamiento, formulación, dirección, supervisión y evaluación de las políticas de ciberdefensa para la jurisdicción del Ministerio de Defensa y su instrumento militar dependiente". (Gobierno Argentino, 2015)

También establece diversas acciones a partir de su responsabilidad primaria en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar y en asistir en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa. Cabe destacar que el Comando Conjunto de Ciberdefensa y la Dirección General de Ciberdefensa, funcionan integradamente y tienen por sede principal el Centro de Ciberdefensa.

Cabe destacar que el 13 de septiembre de 2013 se suscribió la Declaración de Buenos Aires, una declaración conjunta entre los Ministros de Defensa de Argentina y Brasil, a través de la cual decidieron impulsar la cooperación en ciberdefensa y la creación de un grupo de trabajo bilateral, el cual posteriormente acordó una agenda de trabajo en áreas de capacitación, métodos y sistemas tecnológicos, desarrollo de doctrina combinada, investigación científica e intercambios entre los CSIRT de ambos Ministerios para incrementar la seguridad cibernética.

Cabe destacar que mediante el Decreto 42/2016 del 07/01/2016 se dispuso un reordenamiento de las dependencias del Ministerio de Defensa y, en tal sentido, en materia de defensa cibernética, se dispuso crear la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa (Gobierno Argentino, 2016).

Así, dentro de los objetivos de la Secretaría en la materia, tendrá los de:

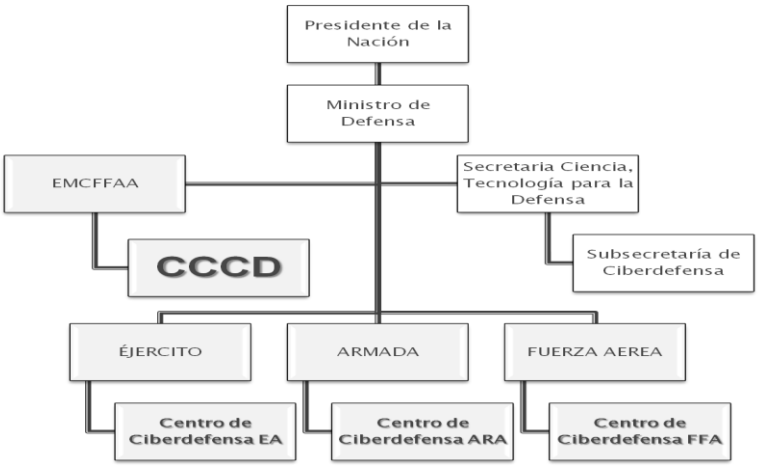
- Entender en la formulación, aprobación y supervisión del cumplimiento de las políticas y programas de los organismos de investigación y desarrollo del sector Ciberdefensa.
- Entender en la coordinación y conbducción superior de los organismos científicos y tecnológicos del área Ciberdefensa.
- Entender en el impulso y promoción del intercambio de formación técnica relacionada con la Ciberdefensa a nivel extrajurisdiccional.

Por su parte, la nueva Subsecretaría de Ciberdefensa tendrá por acciones:

1. Asistir al Secretario de Ciencia, Tecnología y Producción para la Defensa en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar.
2. Entender en la coordinación con los organismos y autoridades de los distintos Poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica.
3. Intervenir en la orientación, dirección y supervisión de las acciones en materia de ciberdefensa ejecutadas por los niveles Estratégico Nacional y Estratégico Militar.
4. Ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas.

5. Intervenir en la evaluación y aprobación de los planes militares de desarrollo de capacidades de ciberdefensa, en la Doctrina Básica y en las publicaciones militares pertinentes, cualquiera sea su naturaleza.
6. Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.
7. Fomentar políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado.
8. Promover vínculos sistemáticos de intercambio y cooperación en materia de ciberdefensa con los ámbitos académico, científico y empresarial.
9. Impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados.
10. Asistir en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa de conformidad a los lineamientos del Ciclo de Planeamiento de la Defensa Nacional.

    De este modo, el organigrama de responsabilidades en la materia a nivel nacional queda estructurado de la siguiente manera (Mato, 2016):



CAPITULO 6

Proyecciones educativas en el ámbito de la defensa.

6.1 Situación en Hispanoamérica

España

En el ámbito hispanoparlante, se destaca el dictado del Master en Ciberdefensa de la Universidad Alcalá de Henares[28]. Con el apoyo del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas de España, el mismo está dirigido a ingenieros y graduados relacionados con el sector de las TIC y profesionales de las Fuerzas Armadas que necesiten incrementar su conocimiento en el área de Ciberdefensa y que deseen adquirir u obtener un marco de referencia en una de las áreas tecnológicas con más proyección del sector de la seguridad.

Entre los docentes y expositores del programa, además de académicos y profesionales civiles, se destacan oficiales del Estado Mayor del Mando Conjunto de Ciberdefensa, del ámbito telecomunicaciones de las tres fuerzas armadas, de la guardia civil y del European Security and Defence College.

Entre las competencias a adquirir por parte del egresado del Master se destacan:

- Comprender las diferencias y similitudes entre el concepto de Ciberdefensa y Ciberseguridad, sus antecedentes y las diversas iniciativas de normativa y doctrina a nivel internacional y mundial.
- Conocer y saber aplicar los diferentes aspectos doctrinales relacionados con las capacidades de Ciberdefensa: explotación, defensa y respuesta.
- Comprender y saber aplicar el concepto de Defensa en Profundidad, así como las principales técnicas de defensa frente a controles de Ciberdefensa, que las organizaciones deberían implementar para obtener un nivel alto de seguridad.
- Conocer y saber aplicar diversas técnicas y herramientas de detección de ataques cibernéticos y actividades maliciosas, prevención, recuperación y mitigación de

[28] Tomado de: http://masterciberdefensa.in-nova.org/

ciberataques, evaluación dinámica del riesgo, conciencia de la situación, toma de decisiones en tiempo oportuno, colaboración y compartición de información.

- Conocer y saber analizar los aspectos más importantes que conllevan los ataques y sus herramientas.
- Conocer las técnicas de detección y análisis de malware avanzado tipo Amenaza Avanzada Persistente (APT) como Stuxnet, Flame, etc.
- Tener la capacidad para realizar auditorías de seguridad.
- Conocer los diferentes sistemas de control industrial y de información que controlan las infraestructuras críticas.
- Adquirir la capacidad de realizar Análisis Forense Digital.

Bolivia.

La Escuela de Altos Estudios Nacionales (E.A.E.N.), vinculada a la Universidad de las Fuerzas Armadas del Estado Pluinacional de Bolivia desarrolla desde el año 2016 una Diplomatura en Ciberdefensa y Ciberseguridad a distancia [29].

El objetivo general del programa es capacitar a profesionales frente a las amenazas latentes a la seguridad de un Estado o una organización. La diplomatura está dirigida a cursantes bolivianos y a extranjeros residentes en ese país.

La currícula tiene como módulos: la Ciberdefensa, la Ciberseguridad y la Ciberguerra; Ataques cibernéticos; Estrategias de Ciberseguridad y de Ciberdefensa; Plan Nacional de Ciberseguridad y Ciberdefensa.

Brasil.

Mediante un Decreto del Ministerio de Defensa de octubre de 2014,se establece la creación de la Escuela Nacional de ciberdefensa (ENaDCiber) de Brasil.

[29] Tomado de:
http://www.eaen.edu.bo/pdf/PROG_DIPLOMADO_CIBER_DEFENSA_Y_SEGURIDAD.pdf

El proyecto, encargado a la Universidad de Brasilia (UnB) fue entregado en julio de 2015. El profesor Jorge Fernandes, director del Centro de Informática de la UnB, ha expresado que esos estudios, conjuntamente con otros estarán concluidos en octubre de 2016[30].

El mismo se integra al Programa de Defensa Cibernética de la Defensa Nacional y su objetivo será la formación de recursos humanos e investigación en materia de ciberdefensa de Brasil. Aunque la ENaDCiber tendrá una oficina física, los cursos se desarrollarán en todo el territorio nacional, en colaboración con las universidades y centros técnicos especializados.

Cabe destacar que esta nueva institución educativa especializada prevé implementar un sistema de Certificación y Homologación de Productos y Sevicios de Defensa Cibernética (SHCDCiber) para el análisis de seguridad de adware y software utilizados por los organismos de defensa cibernética. En tal sentido, la idea es montar una red de laboratorios para analizar la seguridad de los productos y certificar los mismos.

Colombia.

Desde el año 2010, la Escuela Superior de Guerra de Colombia (ESDEGUE)**,** desarrolla un proyecto de investigación sobre nuevas amenazas para preparar la ciberdefensa.

Posteriormente, en 2013 la ESDEGUE abrió la cátedra de ciberguerra**,** dirigida a los alumnos de los Cursos de Altos Estudios Militares (CAEM) y Curso de Estado Mayor (CEM) con el fin de prepararlos hacia un conocimiento más profundo del tema y generar la cultura de la seguridad informática y de la ciberdefensa[31].

[30] Tomado de: http://oglobo.globo.com/sociedade/tecnologia/brasil-tera-escola-nacional-de-defesa-cibernetica-15914957
[31] Tomado de: http://www.siliconweek.com/cloud/el-mintic-se-une-al-ejercito-para-crear-armas-de-ciberdefensa-en-colombia-49059

Asimismo, a principios de 2014, las autoridades de la Escuela y del Ministerio de Tecnologías de la Información, suscribieron un Acuerdo Interinstitucional sobre Ciberguerra y Ciberdefensa que busca trabajar de manera conjunta en "el diseño, planeación y ejecución de programas académicos entre las Fuerzas Militares y las entidades públicas con el fin de unificar criterios y optimizar los recursos del Estado en pro de la seguridad y defensa de la nación".

Recientemente, la Escuela Superior de Guerra del Ejército de Colombia en coordinación con el Ministerio de Tecnologías de la Información y las Telecomunicaciones "MinTIC", dicta dos programas académicos, uno de posgrado: el Magister en Ciberseguridad y Ciberdefensa[32] y otro de extensión: la Diplomatura en Ciberseguridad y Ciberdefensa.

El Magister en Ciberseguridad y Ciberdefensa, aprobado a mediados de 2015, dio inicio a su primer cursada en 2016. El objetivo general del mismo es formar posgraduados que integren conceptos, prácticas, y procedimientos propios de la seguridad de la información, las telecomunicaciones y el riesgo operacional; capaz de formular políticas, diseñar estrategias, tomar decisiones y gestionar conocimiento propio, para garantizar el cumplimiento de la misión de una organización y su resiliencia.

El posgrado está destinado a profesionales en áreas de ingeniería de sistemas, electrónica, mecatrónica, de telecomunicaciones e industrial, administradores de empresas, públicos, logísticos, aeronáuticos y policiales, graduados en ciencias militares, ciencias navales y ciencias militares aeronáuticas, profesionales en criminalística, abogados, que tengan experiencia en el área de tecnologías de la información, seguridad informática, asesores en Seguridad y Defensa Nacional, Inteligencia Militar y/o Policial, investigadores policiales, analistas de riesgos, asesores jurídico-operacionales o de telecomunicaciones.

El perfil del egresado se orienta a lograr:

- identificar recursos cibernéticos a través del desarrollo de la capacidad para determinar los elementos, recursos y actores de infraestructura crítica, públicos y privados, para la construcción de un modelo integrado de seguridad cibernética.

[32] Tomado de: http://www.esdegue.mil.co/node/5656

- evaluar planes y programas de Ciberseguridad y Ciberdefensa, permanentemente, para garantizar su efectividad.
- diseñar planes, programas, y proyectos de Ciberseguridad y Ciberdefensa, ajustados a la normatividad pertinente, para la prevención, detección, análisis e investigación de ciberamenazas y ciberataques.
- definir políticas y lineamientos en materia de Ciberseguridad y Ciberdefensa, para el sector de desempeño, que propendan por la seguridad de la organización y la continuidad del negocio, ante un ciberataque.
- formular estrategias en Ciberseguridad y Ciberdefensa, que garanticen el uso seguro del espacio cibernético, la seguridad de los datos y la minimización del riesgo.
- tomar decisiones en Ciberseguridad y Ciberdefensa, a partir de modelos simulados de ataques contra la infraestructura crítica, para establecer el riesgo operacional y financiero del sector y/u organización, además de garantizar la continuidad del negocio.
- modelar, con capacidad de crear esquemas de simulación, a partir de procesos de investigación, para generar conocimiento propio y aplicable a la Ciberseguridad y Ciberdefensa

Por su parte, la Diplomatura es destinada a oficiales y funcionarios públicos que intervienen en la administración de plataformas tecnológicas, infraestructura crítica y sistemas de seguridad en el país. El perfil de los cursantes es el de profesionales graduados en el área de Ingeniería de Sistemas, Electrónica, Telecomunicaciones o afines, relacionados con el sector de las TIC, administradores de plataforma tecnológica o encargados de seguridad de la información.

El objetivo es la formación y capacitación para mejorar la seguridad y privacidad de las tecnologías de la información en el Estado colombiano frente a las amenazas cibernéticas, "buscando fomentar la participación de funcionarios civiles y militares encargados de la administración judicial y del manejo de plataformas tecnológicas en el sector Defensa, para Incentivar la creación de redes de conocimiento e investigación que permitan trabajar de manera conjunta, coordinada e interagencial a favor de la seguridad y y defensa de la Nación"[33].

[33] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia: http://www.mintic.gov.co/portal/604/w3-article-7684.html

La diplomatura de 160 horas, es desarrollada en dos fases, una virtual de 5 módulos de aproximadamente un mes de duración y luego una etapa presencial de 5 días intensivos.

Los temas que se desarrollan son: regulaciones cibernéticas, el estudio del ciberespacio, actores y roles en el panorama nacional e internacional, las leyes que cobijan el accionar de los organismos de defensa frente a los ataques informáticos, conceptos operacionales y guerra electrónica, políticas y lineamientos en seguridad de la información y debate en torno a una estructuración conjunta de una estrategia de ciberseguridad y ciberdefensa.

Chile

Desde hace unos años, la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) juntamente con la Subsecretaria de Defensa del país, desarrolla el Seminario Ciberseguridad y Ciberguerra. En el mismo se tratan temáticas como: "Elementos Fundamentales de la Seguridad de la Información", "Conceptos básicos sobre infraestructura de red" y "Ciberespacio", "Ciberseguridad" y "Tecnologías de Ciberseguridad para la Defensa", "Aspectos conceptuales legales y doctrinarios", "Regulación del ciberespacio", "El ciberespacio y la Defensa" y "Nuevas tendencias y desafíos". (ANEPE, 2015)

Ecuador

Durante 2015, la Facultad de Ciencias Físico-Matemáticas y Naturales de la Universidad Nacional de San Luis, Argentina y la Universidad Nacional de las Fuerzas Armadas (ESPE) de Ecuador desarrollan un programa tendiente a establecer una Maestría en Ciberdefensa y en Ciberseguridad con orientaciones aspectos operativos y en aspectos forenses en la materia[34].

[34] Tomado de: http://desd.espe.edu.ec/wp-content/uploads/2015/06/ESPE-UNSL-Borrador-de-la-estructura-de-la-Maestria-en-Ciberdefensa-y-en-Ciberseguridad-Version-3.0.pdf

Perú.

El Centro de Altos Estudios Nacionales, Escuela de Posgrado del Estado Peruano, adscrita a la Presidencia del Consejo de Ministros, cuyo objetivo es capacitar y perfeccionar a los profesionales del sector público y privado, para la toma de decisiones eficaces en la gestión estratégica en las áreas de seguridad, desarrollo y defensa nacional de ese país, dicta una Diplomatura en Ciberseguridad[35].

El objetivo de la misma es:

- fortalecer el conocimiento del plan de seguridad de la información en redes y sistemas del ciberespacio Conocer y aplicar técnicas Antihacking, a fin de estar en condiciones de incrementar las medidas de protección a las redes y sistemas de información.
- conocer el funcionamiento y aplicación de procedimientos técnicos usados en un CERT.
- plantear esquemas defensivos eficaces para la gestión de riesgos frente a la intrusión no autorizada a los sistemas de información, que garanticen el uso seguro del ciberespacio.

La misma está dirigida a oficiales de Seguridad de la Información (CISO) del sector público y privado, ingenieros que administran sistemas informáticos, consultores de empresas de seguridad, miembros de las fuerzas armadas y policiales interesados en obtener una certificación para fortalecer sus conocimientos de seguridad informática y ser capaces de proteger sus instalaciones de amenazas de ciberataques o intrusión o interna y/o externa.

Los módulos de estudio son: el Contexto internacional de la ciberseguridad: Ciberinteligencia y ciberdefensa; la Gestión de Riesgos; la Gestión de la Ciberseguridad; la Gestión de la Continuidad de Negocios; las Técnicas de Anti hacking; la Gestión de ciberincidentes y operación de ciberseguridad; la Ciberseguridad en infraestructuras críticas nacionales y la gestión de CERTs.

El perfil del egresado propicia que el egresado estará en condiciones de:

[35] Tomado de: http://www.caen.edu.pe/wordpress/posgrados/diplomados/i-diplomado-en-cibeseguridad/#tab-1-521347101

- Gestionar, planificar, diseñar e implementar los procedimientos necesarios para optimizar la ciberseguridad de los diferentes activos de la empresa, teniendo en cuenta las actuales amenazas de ataques o intrusiones a las redes y sistemas informáticos.
- Gestionar la seguridad de un departamento de servicios de tecnologías de información y comunicación y la seguridad en sistemas SCADA.
- Brindar servicios de consultoría y auditoría en una empresa especializada en seguridad de la información.

República Argentina

En el ámbito de la Escuela Superior Técnica "Grl Manuel Savio" (EST) del Ejército Argentino, se dicta la Especialización en Criptografía y Seguridad Teleinformática[36]. Propende a capacitar para el desarrollo de proyectos de alta complejidad en el ámbito de la Criptografía y las Ciencias de la Computación vinculadas con la Seguridad de los Sistemas Teleinformáticos en un marco donde la seguridad teleinformática y sus disciplinas asociadas se encuentra enmarcado internacionalmente por crecientes factores de riesgo y amenazas a las organizaciones e instituciones civiles de las naciones, en todos los órdenes, y con particular énfasis en ataques a sus sistemas informáticos y teleinformáticos (Ortiz, 2004).

Este postgrado brinda a graduados en informática, telecomunicaciones y electrónica el conocimiento y la profundización de los conceptos fundamentales que hacen a los sistemas de seguridad utilizados para resguardar la información, así como las herramientas teóricas y prácticas que es necesario utilizar, tanto durante su procesamiento, como durante la fase de transmisión.

Posee como objetivos:

- Proporcionar conocimientos teóricos / prácticos sobre Criptografía y Seguridad Teleinformática, relacionados especialmente, a los Sistemas de Información y a las Redes de Computadoras, sobre las que estos sistemas utilizan para su vinculación.
- Dar a conocer las técnicas y los protocolos que se emplean habitualmente para asegurar un reparto seguro y confiable de la información, y un acceso controlado a la misma en instalaciones de uso compartido.

[36] Tomado de: http://www.est.iue.edu.ar/?page_id=133

- Facilitar el dominio práctico de los algoritmos más importantes que se emplean para cifrar la información con la finalidad de asegurar una transmisión confiable, a costo mínimo.
- Dar a conocer los algoritmos y sistemas de autenticación, protección y privacidad más utilizados, así como con las tácticas más comunes de criptorruptura de cifrados.
- Posibilitar en los graduados la actualización de nuevos enfoques técnico-metodológicos y marcos teóricos relativos a las ciencias de la computación vinculada con la Seguridad Informática.
- Enseñar las problemáticas actuales emergentes de los paradigmas fundamentales de los Sistemas de Información y las Redes Teleinformáticas.
- Caracterizar la vinculación de los problemas que genera la necesidad de tener Sistemas Teleinformáticos con la operación eficaz de las Redes de Computadoras y los costos consecuentes.
- Articular teoría y práctica desde los conocimientos específicos para un aprovechamiento integrado de la práctica profesional.
- Facilitar el análisis, en sus múltiples dimensiones, de las características de los modelos criptográficos formales en sus diferentes lógicas y sus algoritmos de encriptamiento.
- Integrar marcos teóricos y estrategias de acción, con la finalidad de abordar satisfactoriamente modelos de estudio de costos y factibilidad de Sistemas Informáticos de Seguridad.

Actualmente, en la mayoría de los casos luego de procesar la información, es necesario transportar los datos obtenidos a otros lugares geográficos, locales o remotos, para su uso o posterior reprocesamiento. Estas nuevas especialidades típicas de nuevos escenarios de la realidad cotidiana, si bien tienen desarrollos con un sesgo claramente tecnológico, también requieren del estudio de temas claramente vinculados con lo puramente matemático.

Tanto por el lenguaje utilizado, como por los métodos de desarrollo (construcción de algoritmos, uso generalizado de la abstracción y conocimiento

expresado en la forma de teoremas) es necesario, también, el conocimiento de aspectos particulares de la matemática aplicada.

Uno de los procedimientos más aptos para proveer soluciones tecnológicas a los distintos problemas de seguridad en cualquiera de sus niveles está vinculado con las técnicas criptográficas, de cifrado ó de encriptación. Su disposición y aplicación requiere de conocimientos especiales asociados en primer término con las ciencias matemáticas, y en segundo término, con los adelantos tecnológicos que acompañan específicamente a los sistemas criptográficos.

Asimismo, la EST desarrolla cursos de capacitación en materia de seguridad informática y de las comunicaciones, guerra electrónica, etc. Estas capacidades también se encuentran en los institutos de formación de la Armada Argentina y en la Fuerza Aérea Argentina[37].

[37] Tomado: http://www.ingenieriaest.iese.edu.ar/

Conclusiones

Conclusiones

A partir del fenómeno de la globalización se habla de un nuevo tipo de sociedad, denominada pos industrial, posmoderna y del riesgo global.

Uno de los rasgos más sobresalientes de este tipo de sociedad es la llamada revolución de las comunicaciones; fenómeno reciente y en marcha, centrado a partir del desarrollo y utilización de tecnologías y redes de información a escala global, cuyos alcances multidimensionales afectan todas las expresiones de la sociedad humana. Lo anterior nos remite a la identificación de un nuevo espacio o "dominio" virtual (ciber), construido como un escenario de interacción humana con sus propias realidades, modalidades y disputas y actores virtuales. En otras palabras, observamos la creación de una dimensión de conducción y nuevas formas de expresión política.

Desde esta perspectiva, las relaciones internacionales no están ajenas a estos desafíos, de momento en que la expansión de un espacio inédito internacional impacta y tensiona al sistema interestatal tradicional. Entre estos, cabe mencionar, los desafíos y amenazas inesperadas y desconocidas a la seguridad nacional y los efectos transformadores del sistema internacional al partir del acceso al ciberespacio de distintos actores desde el estado a aquellos de la sociedad civil transnacional.

La utilización de Internet y las actividades ejercidas por diversos actores en el ciber espacio brinda un lugar estratégico para poder cometer acciones sociales desestabilizantes. Desde esta perspectiva el conocimiento acerca de quiénes son estos actores se ha vuelto un tema de preocupación recurrente entre actores individuales, grupos, empresas y gobernantes.

En este escenario los estados no tienen exclusividad en estas interacciones, hay grupos de especialistas – informáticos o hackers que actúan distorsionando y complejizando el acontecer de los ataques virtuales. Esto refleja que hay una especie de desjerarquización

en el poder internacional, donde los Estados no tienen necesariamente más poder que ciertos grupos o individuos que pueden provocar inestabilidad, incertidumbre y situaciones críticas de diversa índole a través de una computadora.

La era de la información posee un nuevo "espacio" informacional y una infraestructura "crítica" que lo soporta, demandando esfuerzos en igual sentido.

Los nuevos conflictos de esta era han dado lugar a la denominada guerra de la información, donde se ataca el nudo o "nodo" que hace a la comunicación, administración, comercialización, etc. esto es las redes informáticas y las infraestructuras que las soportan.

No se trata solamente de atacar un pozo petrolero para evitar el flujo de combustible, o como era un ataque en la transición de la era industrial a la nueva era. Se trata de atacar un centro financiero, un sistema de comunicaciones o infectar una red de sistemas civiles o militares, afectando así la totalidad de los sistemas de una nación, y ya no necesariamente en términos de guerra clásica, el otro sistema de defensa de la nación.

La complejidad que presenta este nuevo tipo de amenaza por la asimetría entre sus actores, multidimensionalidad de los escenarios e intangibilidad de la propia información, requiere capacidades altamente entrenadas y permanentemente actualizadas.

Identificar, desarrollar y asegurar las Infraestructuras Críticas Informacionales, neutralizando las acciones en su contra y detectar a futuro otras, son medidas continuas y constantes que demandan eficacia y eficiencia en su resolución.

Toda organización pública o privada, que precie su identidad, que quiera mantener movilidad y aplicar influencia en términos de poder, en un mundo globalizado deberá prepararse, adiestrándose, reconfigurándose en el entendimiento del nuevo ambiente estratégico del ciberespacio que posee lógica propia y afecta directa o indirectamente los

otros ambientes (terrestre , marítimo, aéreo y especial) toda vez que las infraestructuras críticas se desenvuelven en ellos y dependen de su operatividad a partir del ciberespacio.
Por tal motivo se requiere actualizar permanentemente la doctrina en la materia para entender su complejidad, identificarla, generar métodos, técnicas y entrenamiento.
Es necesario incorporar a las organizaciones como un nuevo concepto estratégico el concepto de Infraestructuras Críticas, especialmente las Informacionales.

Se requieren cada vez más mecanismos de cooperación público-privado, a nivel nacional, bilateral y multilateral frente a una amenaza multidimensional y global.
Han transcurrido 40 años desde los primeros desarrollos que dieron lugar a Internet y, aproximadamente 25 años desde su desarrollo propiamente dicho. En estos años, se ha desplegado su uso, afectando todos los órdenes, inclusive y, cada vez más el militar. En tal sentido, la Defensa Cibernética constituye un nuevo ítem en la agenda de defensa nacional y seguridad regional e internacional de los Estados, individualmente y de los organismos regionales e internacionales globalmente.

Las respuestas organizacionales comenzaron a plantear una dicotomía conceptual entre ciberseguridad y ciberguerra, llegando a fragmentar su entendimiento frente a una operatoria que era unívoca pero que se percibía solo por los efectos sin considerar las causas. Esta concepción significó la fragmentación de la utilización de los recursos de los respectivos estados en atención a esta nueva amenaza.

No obstante ello, desde mediados de la pasada década, comienzan a establecer políticas, estrategias y planes de carácter nacional, tendientes a poseer primeramente una visión de conjunto del problema, entendiendo que se requiere una respuesta coordinada entre todos los organismos de cada estado con competencia directa o indirecta en la materia.
Así, el grado de afectación de las amenazas cibernéticas ha posicionado a la Defensa Cibernética en una dimensión estratégica para los gobiernos nacionales así como para organismos regionales e internacionales.

En tal sentido, los gobiernos en general, han adoptado políticas y estrategias específicas en materia de ciberdefensa, contemplando el establecimiento de ámbitos de conducción político-nacionales a nivel ministerial, así como estructuras de coordinación conjunta en el ámbito de las Fuerzas Armadas. Esta nueva constitución de organismos responsables en los distintos niveles en distintos países, constituye una respuesta clara al grado de alta valoración que se le asigna cada vez más a la problemática de la ciberdefensa. En tal sentido, se aprecia una carrera por desarrollar capacidades de conducción, a la vez de atención ante las amenazas a la ciberdefensa. Así, el factor capacitación ha comenzado a ser cada vez más considerado, desarrollándose a tal efecto cursos y programas de formación específicos en la materia.

Los países más desarrollados desde hace menos de una década comenzaron a constituir Cibercomandos de carácter civil, policial y, principalmente militar para atender eficazmente los desafíos que se presentan.

Desde la constitución efectiva del Cibercomando por parte de los EEUU y sus buenos resultados, seguido de otros países desarrollados, ha propiciado que el resto de otros Estados conformen organizaciones militares conjuntas en atención a esa tendencia.

En el marco regional, Brasil y Colombia son los países que se presentan innovadores desarrollos en materia de ciberdefensa. No obstante ello, Argentina en los últimos años ha ido adecuando su perfil de conformidad a los requerimientos y estándares internacionales en la materia. La constitución del Comando de Ciberdefensa de carácter Conjunto y la coordinación de políticas y estrategias desde el ámbito Ministerial han brindado un marco adecuado para el desarrollo efectivo de capacidades.

En virtud a la complejidad del fenómeno, determinado tanto por el avance tecnológico en contante cambio crean una la dinámica permanente a las acciones de los gobiernos, caracterizada por la cooperación bilateral y, recientemente la multilateral en el entendimiento que el ciberespacio carece de fronteras y las infraestructuras críticas,

aunque nacionales por la interconectividad de las TICs, crean dependencias con otras que trascienden los espacios nacionales.

En tal sentido, comienza a surgir un capítulo referido a la ciberdefensa en torno a los nuevos requerimientos de Gobernanza entendida como “el arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía” (RAE, 2016).

Así, al concepto de Gobernanza en general se correlaciona la Gobernanza de Internet, entendida esta como los procesos y normas que afectan la forma en que se gestiona Internet entendida como una plataforma abierta y confiable para la innovación a partir de un enfoque descentralizado, colaborativo entre las múltiples partes interesadas hacia la gobernanza de Internet. (Internet Society, 2015)

Por último, la gobernanza de Internet contempla también los aspectos de seguridad, donde se aprecia el resguardo frente a eventuales sucesos, accidentales o incidentes provocados, lo que requiere no solo la prevención sino la previsión de efectuar una rápida resiliencia de los sistemas afectados.

Esta concepción puso necesariamente en conexión a la esfera gubernamental, tanto en sus ámbitos administrativos, judiciales, policiales y de defensa entre ellos y con los ámbitos empresariales y académicos.

En lo atinente a la Ciberdefensa, se destaca en los distintos países una correlación de desarrollos organizacionales tanto en las respectivas fuerzas armadas individualmente y en su accionar conjunto, así como en la administración de los Gobiernos a partir de la conformación de estructuras ministeriales con responsabilidad política efectiva en la conducción de la misma.

Así, los Cibercomandos específicos se interrelacionan con Cibercomandos Conjuntos y estos, bajo la dirección y conducción gubernamental en los Ministerios de Defensa con responsables específicos de fijar políticas en la materia.

En cuanto a la formación de capacidades se abre un amplio abanico de propuestas en distintos países. En el ámbito regional se destaca que todavía los programas, cursos y carreras (especialmente a nivel posgrado) se encuentran enmarcados en institutos de capacitación de las Fuerzas Armadas. El caso más significativo es Brasil, con la constitución de un instituto educativo militar específico en Ciberdefensa. A diferencia de ello, otros países, como EEUU o España, además de contar con programas de capacitación propios de las Fuerzas Armadas, también coordinan esfuerzos, desarrollando programas de capacitación entre los institutos militares conjuntamente con Universidades públicas o privadas.

No obstante ello, se destaca en la región el inicio de acciones bilaterales y multilaterales en materia de capacitación e intercambio, lo que crea un clima propicio para el desarrollo de acciones coordinadas ante la previsión de ciberaccidentes y/o ciberataques masivos a nivel regional.

Desde el ámbito académico puro, si bien la Ciberdefensa comienza a ser tratada como una cuestión gravitante, todavía subsiste una lógica percepción signada por concepciones de carácter tecnológico e inclusive bajo las entendibles consideraciones de reserva al momento de analizarla en su conjunto. Por tal motivo, el análisis y seguimiento de la temática resulta algo dificultoso. Sin embargo, la cada vez mayor constitución de organizaciones de carácter político y estratégico a nivel gubernamental, comienzan a posicionar la temática en una dimensión más propia del análisis estratégico, lo que comenzaría a facilitar un seguimiento de la temática tanto en ámbitos académicos como a través de los medios de comunicación públicos y privados, al tiempo que su estudio en el nivel académico.

BIBLIOGRAFIA

- Ambros, Isidre (2011). *China - anuncia la creación de un ´ejército azul´ para la ciberguerra.* Corresponsal en Pekín. Portal de noticias. Off News. 30/05/11 URL: http://www.offnews.info/verArticulo.php?contenidoID=31344
- ANEPE (2015). *Seminario Ciberseguridad y Ciberguerra*. Academia Nacional de Estudios Políticos y Estratégicos. Santiago de Chile. URL: http://www.anepe.cl/seminario-ciberseguridad-y-ciberguerra-en-la-anepe/
- ANSSI (2011). *Information systems defence and security France's strategy*. Agence Nationale de la Sécurité des Systèmes d'information du la Republique Françoise. París. Versión en inglés. URL:https://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf
- ANSSI (2015). *Strategie nationale securite numerique*. Agence Nationale de la Sécurité des Systèmes d'information du la Republique Françoise. París. URL:http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
- Arcángeles, Mario. (1983) *Historia de la Guerra Electrónica*, Madrid, 1983
- Arozarena Gratacos, M., Fonseca, C., Ortiz, J.U. y Perdomo, I. (2014). *El Manual de Tallin y la aplicabilidad del Derecho Internacional a la ciberguerra.* Revista de la ESG, Ejército Argentino. Sep-Dic 14, Nº 588, pp. 129-148.
- Arpagian, Nicolás (2009). *La Cyberguerre, la guerre numérique a commencé*, Ed. Vuilbert, París.
- Arquila, J y Ronfeldt, David (2001). *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica, CA: National Defense Research Institute, RAND Corporation, USA.
- Arquila, J., y Rondfeld, D. (2003). *Redes y guerras en red. El futuro del terrorismo, el crimen*. Alianza Editorial, España.
- Artiles, Nestor (2011). *La Situación de la ciberseguridad en el ámbito internacional y en la OTAN*. Instituto Español de Estudios estratégicos. Cuaderno de estrategia N° 149. Pág. 167

- Banco Mundial. *Internet users (per 100 people).* 2016.
- Bejarano, María José. (2010) *Alcances y ámbito de la seguridad nacional en el ciberespacio*. Instituto Español de Estudios Estratégicos. Cuaderno de Estrategia N° 149.
- BID (2016). *Ciberseguridad, ¿estamos preparados en América Latina y el Caribe?*. Banco Interamericano de Desarrollo (BID) Washington DC.
  URL: https://publications.iadb.org/handle/11319/7449?locale-attribute=es
- BMI (2011). *Estrategia de Ciberseguridad*. Ministerio del Interior de la Rep. Federal de Alemania.
  URL: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
- Camps, Pablo. (2016) *Ciberdefensa y ciberseguridad, nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en ese ámbito*. Centro de Altos Estudios Nacionales (CALEN), Montevideo.
  http://www.calen.edu.uy/pdf/investigacion/2016-1-Ciberseguridad-Camps.pdf
- Cano, Jeimy. (2011) *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*.
- Caro Bejarano, María José (2013). *Estrategia de Ciberseguridad Nacional.* Instituto Español de Estudios Estratégicos. Cuaderno de Estrategia N° 65, Madrid, 09 diciembre de 2013.
  URL: http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf
- Cargnelutti, Hugo (2002). *Conceptos sobre Guerra de Información*. Revista de la Comisión del Arma de Comunicaciones. Número 27. Pag 11.
- Castells, Manuel. (2002) *La Guerra Red*. Diario El País, España.
- Castel, Robert (2002) *Metamorfosis de la cuestión social*. Barcelona, Paídos.
- Castells, Manuel (1999). *La Era de la Información, Volumen II: El poder de la identidad*. Editorial Siglo XXI, México.

- Castells, Manuel (1998). *¿Hacia el Estado Red?: Globalización económica e instituciones políticas en la era de la información*, Seminario Internacional Sociedade e a Reforma do Estado, ponencia en Brasil, San Pablo.
- Coleman, Kevil (2010). *The weaponry and strategies of digital conflict*. Security and Intelligence Center at the Technolytics Institute, USA.
- CONPES (2016). *Política Nacional de Seguridad Digital de Colombia*. Bogotá. URL: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- Caplan, Sergio (2012). *Los peligros de la ciberguerra*. Russia Beyond the Headlines, Moscú. 03/07/12
  URL: http://es.rbth.com/articles/2012/07/03/los_peligros_de_la_ciberguerra_17711
- C.A.R.I. (2013). *Ciberdefensa-Ciberseguridad Riesgos y Amenazas*..
- Cavelty, V. Mauer y S. F. Krishna-Hensel. (2007) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace,* Burlington, VT: Ashgate,
- CEDN - Centro de Estudios para la Defensa Nacional (2015). *Ciberdefensa*, Universidad de Belgrano. Año 2, Nro 13.
  URL: http://www.ub.edu.ar/centros_de_estudio/cedef/13_diciembre_2015.pdf
- Clarke, Richard y Knake, Robert K. (2010). *Cyber War. The Next Threat to National Security and What to Do About It,* New York, Harper Collins.
- Clarke, R. Knake R. (2011). *Ensayos*. En Clarke, R. & Knake, R. *Guerra en la red: Los nuevos campos de batall*, Barcelona. Editorial Planeta.
- Consejo Nacional de Política Económica y Social de Colombia (2016). *Política Nacional de Seguridad Digital*. Colombia.
- Defense Systems (2012). *France moves to boost cyber warfare skills among officer corps.* 05/07/2012.
  URL: https://defensesystems.com/articles/2012/07/05/agg-france-cyber-warfare-officer-training.aspx
- Delmas, Philippe (1995). *El Brillante porvenir de la Guerra*. Chile. Editorial Andrés Bello.

- Durán, Juan José Diaz (2011). *La ciberseguridad en el ámbito militar*. Instituto Español de Estudios Estratégicos. Cuaderno de Estrategia N° 149, Madrid.
- DoD (2016). *Department of Defense Dictionary of Military and Associated Terms* Department of Defense. Washington DC. USA.
  URL: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
- Ejército argentino (2001). *Historia de las Communicaciones del EA*, Comisión de Comunicaciones Libro II.
- Emergui, Sal (2012). *Kaspersky avisa que la ciberguerra "puede acabar con el mundo que conocemos".* 07/10/12. Diario El Mundo, España.
  URL: http://www.elmundo.es/elmundo/2012/06/07/navegante/1339045745.html
- Flores, Héctor (2015). *Ciberguerra y Derecho Internacional en los conflictos armados*. Revista Manual de informaciones del Ejército Argentino, buenos Aires, Nro 4, Vol LVI, Octubre – Noviembre de 2014.
  URL:
  http://www.manualdeinformaciones.ejercito.mil.ar/archivos2/Ciberguerra.pdf
- Fojón Chamorro, Enrique y Sanz, Ángel (2010), *Ciberseguridad en España: una propuesta para su gestión*, Análisis del Real Instituto Elcano, ARI Nº 101.
- Fojón Chamorro, Enrique (2015). *La nueva estrategia ciber del Pentágono: innovar y potenciar la industria.* Real Instituto El Cano. Madrid, 27/04/2015
  URL: http://www.blog.rielcano.org/la-nueva-estrategia-ciber-del-pentagono-innovar-potenciar-la-industria/
- Fojón Chamorro, Enrique (2015). *La transversalidad del campo de batalla cibernético.* Real Instituto El Cano. Madrid, 04/03/2015
  URL: http://www.blog.rielcano.org/la-transversalidad-del-campo-de-batalla-cibernetico/
- Fojón Chamorro, Enrique (2015). *La cibersoberanía china.* Real Instituto El Cano. Madrid, 20/01/2016
  URL: http://www.blog.rielcano.org/la-ciber-soberania-china/
- Forno, Richard y Baklarz, Ronald (1999).*The Art of Information Warfare: Insight into the Knowledge Warrior Philosophy*. Universal Publishers, USA.

- Fuente Cobo, Ignacio (2016). *La Política de Defensa en Francia: ¿El fin de la independencia estratégica?* Instituto Español de Estudios Estratégicos. Ministerio de Defensa del Reino de España. Madrid URL:http://www.ieee.es/Galerias/fichero/docs_analisis/2016/DIEEEA14-2016_Revision_Defensa_Francesa_IFC.pdf
- Fukuyama, Francis (1992). *El fin de la historia*. Ed. Planeta. Buenos Aires.
- Giudici, Daniel (2013). *Lineamientos para la seguridad cibernética en Teatro de Operaciones*. Trabajo Integrador. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Buenos Aires.
- Gobierno Argentino (2016). *Decreto 42/2016 del 07/01/2016*, por el cual se crea la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa URL:http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm
- Gobierno Argentino (2015). *Decisión Administrativa JGM N° 15/2015* que aprueba la estructura organizativa en de la Dirección General de Ciberdefensa dependiente del Ministerio de Defensa URL:http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/244566/norma.htm
- Gobierno de Chile (2016). *Propuesta de Política Nacional de Ciberseguridad* (PNCS) 2016-2022. URL: http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-P%C3%BAblica-PNCS.pdf
- Gobierno de España (2013). *Estrategia de Ciberseguridad.* URL:http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf
- Gómez Abutridy, Alejandro (2014). *Ciberseguridad y Ciberdefensa, dos elementos de la Ciberguerra*. Memorial del Ejército de Chile, Nro 492, agosto 2014.

- Gómez de Agreda, Ángel (2012). *El Ciberespacio como escenario de conflictos. Identificación de las amenazas,* Centro Superior de Estudios de la Defensa Nacional, Monografía CESEDEN nº 126, febrero 2012.
  URL:http://docplayer.es/3396647-El-ciberespacio-nuevo-escenario-de-confrontacion.html
- González Cussac J. L. (2007). *Nuevas amenazas a la seguridad nacional: el desafío del nuevo terrorismo*, en Retos de la política criminal actual, Revista Galega de Seguridade Pública (REGASP)«, nº 9, Xunta de Galicia.
- Grünschläger, Ricardo (2015). *Global Commons*. Revista de la Escuela de Guerra Naval (ESGN) Nº 61/ Diciembre 2015
  URL:http://www.cefadigital.edu.ar/bitstream/123456789/334/1/4_Revista_61_Global_Commons_w4.pdf
- Hernández, J. Jaime (2015). *Ciberguerra, las batallas del Siglo XXI*. El Universal, México, 16/08/15
  URL: http://www.eluniversal.com.mx/articulo/mundo/2015/08/16/ciberguerra-las-batallas-del-siglo-xxi
- Hispantv (2012). *Irán construye su primer Ejército cibernético.* 21/02/12
  URL: http://www.hispantv.com/noticias/iran/166880/iran-construye-su-primer-ejercito-cibernetico
- Howard D. y Longstaff, T. (1998). *A Common Language for Computer Security Incidents* (Sandia Report SAND98-8667), Alburquerque, NM y Livermore, CA: Sandia National Laboratories.
- Huyghe, François-Bernard (2001) *L'Ennemi à l'ère numérique: Chaos, information, domination,* Broché, Defense, París
- Ibáñez Muñoz, Joseph, (2010) *Internet, Política y poder en la sociedad pos internacional*. Barcelona, Curso de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz. España
  URL:http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2010/2010_6.pdf
- IEE (2010). *La Estrategia Nacional de Seguridad Británica "una nación ponderosa en una era de incertidumbre".* Instituto Español de Estudios

Estratégicos. Ministerio de Defensa del Reino de España. Madrid, diciembre 2010.

URL: http://www.ieee.es/Galerias/fichero/docs_analisis/2010/DIEEEA18-2010EstrategiaNacionalSeguridadBritanica.pdf

- Internet Society (2015). *Gobernanza de Internet*. Informe de la Internet Society. Suiza.

  URL: http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-InternetGovernance-20151030-es.pdf
- Justribó, Candela; Gastaldi, Sol y Fernández, Jorge (2014). *Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo,* Informe de Investigación, Escuela de Defensa Nacional, Octubre/2014, Buenos Aires.

  http://www.edena.mindef.gob.ar/docs/PERFIL_DOCUMENTOS/GASTALDI_1.pdf
- Keyworth G. y otros, *The Digital State: How State Governments are Using Digital Technology*, Executive Summary (Washington, DC: The Progress and Freedom Foundation, September 1998).
- Kóbzev, Artiom (2013). *Rusia refuerza su seguridad cibernética.* 02/08/13. Radio La Voz de Rusia.

  URL: http://mundo.sputniknews.com/spanish_ruvr_ru/2013_08_02/Rusia-Putin-seguridad-cibernetica-defensa/
- Koch Merino, Sebastián (2015). *La política de ciberdefensa de Chile.* Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile (CEEAG). 03/06/15.

  URL: https://articulo30.org/2015/06/03/ciberdefensa-chile/
- Libicki. Martin C. (2009) *Cyberdeterrence and Cyberwar*, Santa Mónica, RAND Corporation.

- Llongueras Vicente, Adrianna (2011). *La Ciberguerra; la guerra inexistente*. Tesina del Doctorado en Paz y Seguridad Internacional. Instituto Universitario General Gutiérrez Mellado, España.
- Lucero, (2015), *La Dimensión Desconocida.* Revista Visión Conjunta, Nro 12/2015. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Buenos Aires.
- Lyns III, William J, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, vol. 89, nº 5, septiembre/octubre de 2010, pp. 97-103.
  URL: www.foreignaffairs.com/articles/66552/williamj-lynn-iii/defending-a-new-domain
- Machiandiarena, Tabeada y Gaidano. (2003). *El empleo en el EA de los sistemas de información en el contexto de la IW*, ESG, 2003. Trabajo Final Licenciatura en Estrategia y Organización (ESG-IESE).
- Martin, Paul-Edouard (2015). *La inseguridad cibernética en América Latina*. Boletín Electrónico del Instituto Español de Estudios Estratégicos. Ministerio de Defensa de España. Nº 79/2015 24 de julio de 2015
  URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf
- Mato, Óscar Ricardo (2016). *Exposición del Comodoro Óscar Ricardo Ramón Mato del Comando Conjunto de Ciberdefensa de las FFAA de Argentina: Operaciones Militares en el Ciberespacio*. Mando Conjunto de Ciberdefensa de España, 23 al 26 de mayo. Kinépolis Madrid.
  URL: https://jornadasciberdefensa2016.es/ponentes/es
- MCCD (2011). *Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar*. Mando Conjunto la Ciberdefensa. Estado Mayor de la Defensa. Ministerio de Defensa del Reino de España.
  URL: http://www.emad.mde.es/CIBERDEFENSA/
- Meschcheriakov, Vladislav (2012). *Rusia crea una estrategia de ciberguerra.* Russia Beyond the Headlines, Moscú. 21/03/12.

URL:
https://es.rbth.com/articles/2012/03/21/rusia_crea_una_estrategia_de_ciberguerra_16580

- Ministerio de Defensa (2014). *Directiva de Política de Defensa*, Decreto 2645/14 URL:http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/240966/norma.htm
- Ministerio de Defensa (2015). *Libro Blanco de la Defensa Nacional.*
  URL:
  https://www.oas.org/csh/spanish/documentos/libro%20blanco%20de%20defensa.doc
- Ministerio de Defensa de de Chile (2016). Cuanta Pública del Ministerio de Defensa. Mayo de 2016. Santiago de Chile.
  URL: http://www.gob.cl/cuenta-publica/2016/sectorial/2016_sectorial_ministerio-defensa-nacional.pdf
- Ministerio de Defensa de España (2011). *La Política de Ciberdefensa de la OTAN* Dirección General de Relaciones Internacionales. Instituto Español de Estudios Estratégicos Documento informativo del IEEE 37-2011.
- Miranda, Sergio (2014). *La Ciberguerra como amenaza a los sistemas de defensa integrados y basados en redes del teatro de operaciones*. Trabajo Integrador Curso Nivel I. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Buenos Aires.
- Molina Mateos, José María (2013). *Ciberseguridad, un reto para la libertad*. Madrid
  URL: http://molinamateos.com/content/ciberseguridad-un-reto-para-la-libertad
- NATO, reportes e informes.
- Nakashima, Ellen (2012) *Cybersecurity chief urges action by Congress*. Washington Post.
  URL: https://www.washingtonpost.com/blogs/2chambers/post/cybersecurity-chief-urges-action-by-congress/2012/07/09/gJQAP4gMZW_blog.html
- Nye, Joseph. S. (2003). *La paradoja del poder norteamericano*, Barcelona: Taurus,

- Nye, Joseph. S. (2012) *Ciberguerra y Ciberpaz*. Proyect Syndicate. 2012.
- OEA (2004). Estrategia Interamericana Integral de Seguridad Hemisférica. URL: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf
- Ommati, Marcos (2016). *La Junta Interamericana de Defensa se transforma para enfrentar nuevos desafíos*. Reportaje al General de Brigada Jaime González Ávalos, Vicepreseidente de la Junta de Delegados de la JID. Revista Diálogo de las Américas. Florida, EEUU. 12 de mayo de 2016. URL: https://dialogo-americas.com/es/articles/junta-interamericana-de-defensa-se-transforma-para-enfrentar-nuevos-desafios
- ONTI (2005). *Política de Seguridad de la Información. Modelo*. Oficina Nacional de Tecnologías de Información (ONTI), Jefatura de Gabinete de Ministros, Buenos Aires, Argentina. URL: http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf
- ONTI (2013). *Política de Seguridad de la Información. Modelo*. Oficina Nacional de Tecnologías de Información (ONTI), Jefatura de Gabinete de Ministros, Buenos Aires, Argentina. URL: http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219163/norma.htm
- Ortiz, Javier Ulises (1999). *La Era de la Información "Glocal".* Revista de la ESG del Ejército Argentino. Jul-Sep99, Nº 534.
- Ortiz, Javier Ulises (2003). *La necesidad de un Nuevo pensamiento estratégico en la era de la información*, Revista de la ESG, Ejército Argentino. pp. 59-80, Número Especial de 2003.
- Ortiz, Javier Ulises (2004). *Intelligence Profesionalism in the Americas*. R. Swanson Comp. Center for Hemispheric Defense Studies.Washinton DC.
- Ortiz, Javier Ulises (2008). *Argentine: The Challenge of Information Operations.* IOSPHERE. US Joint Information Operations Warfare Command. International Seminar. FMSO. Fort Leavenworth, Kansas. (Pags 57 a 63). URL:http://webcache.googleusercontent.com/search?q=cache:0HDVsk_AwX0J:fmso.leavenworth.army.mil/documents/Special-Edition-iosphere.pdf+&cd=2&hl=es-419&ct=clnk&gl=ar

- Ortiz, Javier Ulises (2012). *Estrategia de Defensa Cibernética en la Era de la Información.* Revista de la ESG del Ejército Argentino. Sep-Dic 12, Nº 582.
- Paez, Eduardo (2014). *La guerra ciebernética en un Teatro de Operaciones*. Trabajo Final Integrador. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Buenos Aires.
- Philipp, Joshua (2014). *Gran red de unidades militares secretas de China ataca EEUU a diario.* El Ojo Digital. 27/11/14
  URL: http://www.elojodigital.com/contenido/13906-gran-red-de-unidades-militares-secretas-de-china-ataca-eeuu-diario
- Petrova, Anastasia (2013). *Rusia prepara sus tropas cibernéticas.* Russia Beyond the Headlines, Moscú. 17/07/13
  URL:
  http://es.rbth.com/cultura/technologias/2013/07/17/rusia_prepara_sus_tropas_ciberneticas_30137
- Pritz, Roberto. (2005). *El Dislocamiento estratégico operacional en las nuevas guerras: IW, ciberguerra, sistemas C4I, nuevas armas y tecnologías*. Escuela Superior de Guerra "Tte Grl. L. M. Campos" del Ejército Argentino.
- RAE (2016). *Definición de Gobernanza*. Diccionario de la Real Academia Española.
  URL: http://dle.rae.es/?id=JHRSmFV
- Raska, Michael (2015). *Israel Evolving Cyber Strategy*. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. Singapur. Policy Report. January, 2015
  URL:https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf
- Rico, Juan (2013). *Rusia acelera la creación de un cibercomando militar.* Genbeta. 15/02/13.
  URL: http://www.genbeta.com/activismo-online/rusia-acelera-la-creacion-de-un-cibercomando-militar
- Repetto, Guillermo (2001). *Cyberwar*, EGN, Instituto de Publicaciones Navales, N° 51, Dic, 2001. Bs. As.

- República Popular China (2015). *Document: China's Military Strategy*. USNI News. May 26, 2015
  URL: https://news.usni.org/2015/05/26/document-chinas-military-strategy#SGA
- RUGB (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.* London
  URL:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
- Sánchez Medero, Gema (2010) *Los Estados y la Ciberguerra*. Boletín de Información, ISSN 0213-6864, Nº. 317, 2010, págs. 63-76.
- SGDSN (2014). *Le Plan Vigipirate.* Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), antigua Secretaria ministerial de la Defensa (SGDN), París, Francia.
  URL: http://www.sgdsn.gouv.fr/site_rubrique98.html
- Schmitt, Michael. (2002). *La guerra de la información: los ataques por vía informática y el jus in bello*. Comité Internacional de la Cruz Roja.
  URL: http://www.icrc.org/web/spa/sitespa0.nsf/html/5TECG3
- Sibilla, Gustavo (2007). *Modelo argentino de modernización del Sistema de Defensa*. Cuadernos de Defensa Nª 1. Consejo de Defensa Suramericano CDS-UNASUR. Quito, Ecuador.
  URL: http://www.ceedcds.org.ar/Espanol/09-Downloads/Cuadernos-Defensa-n1.pdf
- Stell, Enrique. (2005). *Guerra Cibernética*. Editorial Círculo Militar, Biblioteca del Oficial Volumen 791, Buenos Aires, pág. 17 y 27.
- Szafranski, Richard (1997). *Una Teoría de la Guerra de Información: Preparación para el año 2020*,
  URL: http://www.afcea.org.ar/publicaciones/teoria.htm. Véase también, *Sun Tzu and Information Warfare*, ed. Robert E. Neilson (Washington, DC: NDU Press,
- Tabansky, Lior (2013). *Cyberdefense Policy of Israel: Evolving Threats and Responses*. Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University, Israel January 2013 – Article n° III.12

URL:http://www.chaire-cyber.fr/IMG/pdf/article_3_12_-_chaire_cyberdefense.pdf

- Thomas, Timothy (2005). *Cyber Silouettes. Shadow Over Information Operations*. FMSO. Fort Leavenworth.
- Tomassini, Luciano (1995). *Política Internacional en un Mundo Posmoderno*. Buenos Aires: Grupo Editor Latinoamericano.
- Toffler, Alvin y Hedi. (1994) *Las Guerras del Futuro, la supervivencia en el alba del siglo XXI*. Barcelona. Plaza & Janes.
- Torres, Douglas E. (2015). *Ciberseguridad y ciberdefensa en Venezuela.* 11o Congresso Brasileiro de Sistemas: O Pensamento sistemico e a interdisciplinaridade: debates e discussoes. Anais. Franca, 29 e 30 de outubro de 2015
  URL en cache:
  www.isssbrasil.usp.br/ocs/index.php/cbs/11cbs/paper/download/85/67
- Torres, Manuel R. (2011). *Los dilemas estratégicos de la ciberguerra*, Revista Ejército de España, No 839, 2011, pp. 14-19.
  URL:http://www.seguridadinternacional.es/?q=es/content/los-dilemas-estrat%C3%A9gicos-de-la-ciberguerra
- Thomas, Timothy. (2005) *Cyber Silouettes. Shadow Over Information Operations*. Foreign Military Studies Office (FMSO). US Army. Fort Leavenworth, Kansas.
- Unión Internacional de Telecomunicaciones (2010). *Decisiones destacadas de Guadalajara*, Revista Actualidades de la UIT, 9 de noviembre de 2010 URL: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf
- US Army (2010). *Army establishes Army Cyber Command.* Fort Belvoir, Va. (Oct. 1, 2010) URL: http://www.army.mil/article/46012/army-establishes-army-cyber-command
- US Department of Defense (2015). *The DoD Cyberstrategy*. Washington DC. Abril 2015.
  URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

- Uzal, Roberto (2012). *Guerra Cibernética: ¿un desafío para la Defensa Nacional?* Revista Visión Conjunta. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Buenos Aires. Año 4, Nro 7, 2012.
  URL: http://esgcffaa.mil.ar/numero7/40.html
- Villaescusa González, Sergio (2016): *Ensayo sobre la vulnerabilidad cibernética*. Centro de Formación Interactiva para la Cultura de la Defensa (CFICD), España.
  URL: http://cisde.es/observatorio/18718
- Villanueva Barrios, (2014) Exposición Seminario CDS sobre Ciberdenfesa. Coronel Roberto Villanueva Barrios. Jefe de Estado Mayor y 2º Comandante del MCCD, - UNASUR, Buenos Aires Mayo 2014.
  URL: http://www.ciberdef.mindef.gob.ar/content/pdfs/bsas/Villanueva.pdf
- We are Social (2016). *Digital Yearbook*. London Singapure.
  URL: http://www.slideshare.net/wearesocialsg/2016-digital-yearbook