FE
Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL DE LICENCIATURA

Título: "El enfoque argentino sobre Ciberseguridad y Ciberdefensa"

Que para acceder al título de Licenciado en Relaciones Internacionales presenta el alumno Edgardo Aimar Gago.

BUENOS AIRES, 29 de mayo de 2017

INDICE

INTRODUCCIÓN

Justificación de la investigación

1. Con relación al tema

· Área de Investigación: SEGURIDAD INTERNACIONAL

· Tema de Investigación CIBERSEGURIDAD Y CIBERDEFENSA.

· Tema acotado: El enfoque argentino sobre Ciberseguridad y Ciberdefensa.

2. Sobre el problema a investigar

a. Antecedentes

Se trata de un tema actual; una realidad de la que es preciso intentar entender y empezar a familiarizarse. Empieza a dominar el escenario mundial y tiene implicancias tanto en la paz como en la guerra, ya sea en las infraestructuras tecnológicas como asimismo, a causa de su gran capacidad de penetración en todo el ámbito de la actividad humana, en la vida cotidiana de cada uno de todos nosotros.

El poder de comunicación de Internet y las facilidades de nuevos desarrollos en telecomunicaciones e informática, ha permitido la interconexión de superordenadores

descentralizados e independientes en un sistema informático que procesa la información en múltiples formatos. Como una red gigante de comunicaciones trabaja a través de la conmutación de paquetes donde la transferencia de datos constituye la inmensa mayoría del tráfico y donde la transmisión de voz no es más que uno de sus servicios especializados. Tiene una complejidad de interacción creciente y pautas de desarrollo impredecibles que surgen del poder creativo de esa interacción. Debe interpretarse en términos de *intercambio* más que mera *transmisión,* ya que al decir de Kuehl (2009) "La palabra intercambio fue elegida por ser más incluyente: no se puede tener un intercambio de información sin su transmisión, y la transmisión sin recepción no tiene sentido."

Como se desprende de las palabras de Manuel Castells (2000), estamos en un proceso de transformación multidimensional y nuestra era es un periodo histórico caracterizado por una revolución tecnológica, centrada en las tecnologías digitales de la información y comunicación, asociada pero no causante, de la emergencia de una estructura social en red en todos los ámbitos de la actividad humana y con interdependencia global. La define como la "*sociedad red"*; es la nueva estructura social de la cual está surgiendo una nueva cultura: la cultura de la virtualidad real, que es simultáneamente incluyente y excluyente, dependiendo de los valores e intereses dominantes en cada país y en cada organización social.

El ex Ministro de Seguridad Interior de EEUU, Michael Chertoof (al escribir el prólogo de Carr 2012), reconoce que aunque algunos le restan importancia al ciberespacio como un dominio en el que se produzcan guerras, ciertos ataques a nivel global demuestran que los sistemas informáticos ocuparán gran parte del campo de batalla del futuro.

Una acumulación de ciberataques coordinados, o simplemente uno aislado, deberían ser una grave preocupación para los gobiernos, por lo que tendría que emplearse todo su potencial de prevención aplicado a la ciberseguridad. Las consecuencias de desatenderla pueden arrojar impactos sociales significativos, temor, incertidumbre y presión pública sobre el liderazgo político.

La percepción errónea es que el daño sólo se limita a la parte física de las redes de computadoras atacadas, pero el ambiente externo que las rodea -o les depende- puede verse afectado a largo plazo. Este es un argumento tangible de que se puede infligir daño continuado en una sociedad específica, más allá de la destrucción real de una red informática.

Debe considerarse a la ciberseguridad como un aspecto muy importante de la Seguridad Nacional, ya que en el ciberespacio una nación puede ver amenazada su libertad de acción y su seguridad. Y debe entenderse no sólo su seguridad cibernética sino toda la Seguridad Nacional. El ciberespacio debe ser un dominio estratégico y así debe ser considerado al establecer la Estrategia de Seguridad y consecuentemente, al planear la correspondiente Defensa Nacional.

En repetidas ocasiones se afirma que nuestro país no tiene hipótesis de conflicto. Incluso puede hallarse quienes argumentan que las mismas sirven para justificar la existencia de las Fuerzas Armadas. Otros a su vez, opinan que no se vislumbran amenazas que afecten intereses vitales, debido al contexto mundial y

regional imperante en la actualidad. No obstante, a los conflictos en potencia corresponde preverlos y prevenirlos para alcanzar la mejor solución posible.

En este trabajo se busca aportar planteos y respuestas, debido al marco jurídico de la República Argentina y su Doctrina de Seguridad y Defensa, en función del concepto de seguridad cooperativa de la Unión de Naciones Suramericanas (Unasur) y su Consejo de Defensa Suramericano (CDS).

Entre las visiones de los autores a ser citados, se tendrá en cuenta la del Coronel "VGM" Enrique Stel plasmada en su libro de 2005, quien se refirió entre otros aspectos al concepto de Guerra Cibernética, explicando un nuevo ámbito, el ciberespacio, en el cual transitan datos que permiten atacar infraestructuras críticas de los Estados, incluyendo a las redes de las FFAA. Otro autor que será tenido en cuenta es Juan Puime Maroto, en su ensayo que publicara en 2009 el Ministerio de Defensa del Reino de España.

Asimismo, se recurre al desarrollo del tema que hiciera el Doctor Roberto Uzal (2012) y que como expresión sintetizada de su pensamiento tomamos su propia expresión:

> Las agresiones que se han estado verificando entre estados-naciones, utilizando una nueva generación de armamento basada en sofisticados programas de computadoras, obligan a repensar las relaciones internacionales y a redefinir las incumbencias de lo que conceptual e instrumentalmente se entiende como Defensa Nacional.

b. Planteo o formulación del problema.

Las nuevas tecnologías de información no son las causas de la formación de una sociedad global, pero son la infraestructura indispensable para su existencia. Las nuevas capacidades desarrolladas por la actividad criminal han llevado, en algunos países de América, y más específicamente en el área de la Unasur, que algunos estados adopten un enfoque propio de seguridad que incluye no sólo la cooperación sino hasta el empleo directo de las Fuerzas Armadas en tareas de contención y represión del crimen.

Otros separan las actividades de defensa y las de seguridad pública, considerando su marco legal interno y evaluando el grado de participación que le otorga a sus FFAA, por caso, en Ciberdefensa, es decir, para hacer frente a riesgos que afecten infraestructura sensible, hidroeléctrica, de transporte, o de la propia seguridad, por amenazas en el ciberespacio.

El carácter multidimensional de los peligros que enfrenta la seguridad ha llevado a una mayor conciencia acerca de la necesidad de una acción coordinada de instituciones como el Ministerio de Defensa, de Relaciones Exteriores, del Interior, de Seguridad entre otros.

En el ámbito nacional, a partir del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad que actúa como marco regulatorio específico, se elaboró la Política Modelo de Seguridad de la Información para la

Administración Pública Nacional, quedando muchos de los incidentes cibernéticos por fuera y lejos de la órbita de la Ciberdefensa.

En el Plan de Acción 2014 del Consejo de Defensa Suramericano (CDS), se ha planteado el objetivo de avanzar en los aspectos técnicos y académicos que confluyan para delimitar las capacidades que cada país miembro posee en relación con la ciberdefensa, tal que se pueda llegar al desarrollo de herramientas que permitan enfrentar las amenazas del ciberespacio.

No alcanza únicamente con incluir el ciberespacio en la agenda política de un gobierno y que éste proclame su importancia estratégica; además, es también creciente la necesidad de toma de conciencia respecto de que es imprescindible la colaboración de toda la sociedad civil, organizada como apoyo y complemento de las acciones institucionales.

c. Justificación del problema.

Es necesario para cualquier país contar con medios y recursos humanos que permitan discernir de inmediato, ante amenazas en el ciberespacio, si se da el caso de enfrentar un *Crimen Cibernético*, o una agresión de *Terrorismo Cibernético* o se trata de un hecho originado por otro estado, o sea, que se trata de un caso de *Guerra Cibernética*.

El Estado debe ejercer el liderazgo de forma inequívoca, a través de un sistema nacional de ciberseguridad integral y dinámico, que posibilite una dirección y gestión eficiente de la seguridad y la defensa de su ciberespacio específico, porque la supervivencia misma de Estado debe ser el primero y máximo interés nacional.

En materia de ciberdefensa existen importantes dificultades fácticas para determinar de antemano si la situación se trata de una agresión militar estatal externa. Por tal motivo, dicha calificación sólo puede darse *a posteriori*, limitando las respuestas inmediatas que el Sistema de Defensa debería poder dar 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.

3. Objetivos de la investigación.

a. Objetivo general.

Este trabajo tratará de identificar y exponer el enfoque que otros actores internacionales tienen en los campos de la Ciberseguridad y la Ciberdefensa, que les permite estar en capacidad de actuar con la celeridad que impone la realidad de una dimensión en continua mutación; indagando al mismo tiempo sobre el enfoque que la República Argentina ha adoptado, de tal forma que se aprecie si existe la necesidad de adecuarlo. Todo sobre la factibilidad de lograr real integración de las Fuerzas Armadas de la Unasur para actuar en Ciberdefensa, teniendo en cuenta la cuestión relativa a las diferencias existentes en los conceptos en seguridad y defensa entre los países integrantes del CDS y las dificultades que podrían derivar de tales diferencias.

b. Objetivos específicos

Objetivo Particular Nro 1: Caracterizar la significación otorgada por otros actores a los conceptos Ciberespacio, Ciberseguridad, Ciberdefensa y sus relacionados, así como a la Seguridad y la Defensa.

Objetivo Particular Nro 2: Indagar sobre cuál es la tendencia generalizada para la gestión integral de la Ciberseguridad de otros actores Estados, su posición frente a la cooperación y el intercambio de información, así como las herramientas y procedimientos que disponen.

Objetivo Particular Nro 3: Describir el marco legal vigente en el ámbito nacional que establece los órganos que se emplean en Ciberseguridad y Ciberdefensa.

4. Formulación de la Hipótesis – Problema

¿El enfoque argentino es compatible con la política de defensa común de cooperación regional de la Unasur y su CDS?

5. Marco Teórico.

Para señalar cuál es el marco teórico del tema elegido, en primer lugar se cree necesario recurrir a los principios de la corriente de pensamiento denominada Realismo. Nos aproximamos desde la posición sostenida por Hans Morgenthau, la cual está caracterizada por una concepción pesimista de la naturaleza humana y de la política internacional, donde ésta carece de criterios morales y conlleva la defensa de los intereses nacionales de los Estados como objetivo principal y en la búsqueda de influir desde la óptica estado-centrista. Esta personificación se sustenta en la idea de Raymond Aron, que en su libro implica que los Estados están dotados de inteligencia. (Aron, 1985).

Gustavo Palomares Lerma (2006) caracteriza a Morgenthau como el autor más destacado del realismo político norteamericano, que en sus estudios intenta formular una teoría general de la política sin hacer distinciones entre política interna e internacional y que en sus reclamos, por un cambio hacia una nueva producción teórica, impulsó el desarrollo de las Relaciones Internacionales.

Según el concepto de Morgenthau (1986), la Política Exterior de un país es la expresión de las medidas que el Estado implemente, para lograr sus intereses nacionales dentro del concierto de las naciones. Destaca además que "el elemento principal que permite al realismo político encontrar el rumbo en el panorama de la política internacional es el concepto de interés definido en términos de poder", y a esto agrega que "sin este concepto, cualquier teoría política, internacional o interna, sería totalmente imposible".

Desarrolló un modelo que corresponde al período de la Guerra Fría, circunscripto al enfrentamiento entre las dos superpotencias. Su teoría internacional se caracteriza por seis principios:

- Concepción pesimista de la naturaleza humana y de la política.

- Interpretación de la centralidad y equilibrio del poder.
- Defensa del "Interés Nacional" como principal objetivo de la política exterior.
- Inexistencia de criterios morales en la política internacional.
- Exclusividad de las normas y leyes políticas.
- Interés definido en términos de poder y del incremento de éste.

Se entiende por poder, a la capacidad o habilidad de un Estado para influir en el comportamiento de otro, persuadiendo o disuadiendo para que haga o deje de hacer, a fin de obtener determinados objetivos (conforme a su propio interés nacional), los que deberían ser proporcionales a las capacidades reales del Estado.

En cuanto al objeto pretendido para el desarrollo de este trabajo, se busca atraer la atención acerca del hecho que los Estados son semejantes respecto de las tareas con las que se enfrentan, pero no en sus posibilidades para llevarlas a cabo, con lo cual las diferencias están dadas por la capacidad.

Partiendo de esa premisa, se recurre además al Realismo-Sistémico-Estructural enunciado por el Doctor Luis Dallanegra Pedraza (2008), que considera a las instituciones internacionales, como "el producto de una estructura de poder que las implementa para cristalizar un orden alcanzado de hecho, resultado de un proceso de "pugna" entre los actores del sistema, en forma asimétrica, y no como las generadoras de ese orden".

Se refiere además al "*poder de ser*", íntimamente relacionado con la "*existencia*" básica para la supervivencia, señalándolo como el "*interés nacional mínimo*" al que ninguna Nación o pueblo puede dejar de aspirar para satisfacer la necesidad básica imperiosa: sobrevivir o desaparecer.

El realismo, (en su posición definiendo al poder bajo la influencia política que un actor ejerce sobre otro), requiere de los gobiernos una prudencia política y un actuar de manera estratégica para alcanzar autonomía en un contexto en el que –según el concepto de *sistema* de Morton Kaplan (1957) –, el contexto internacional se caracteriza por ser un "sistema político sin fuerza legal" que no puede exigir el cumplimiento de normas acordadas ni tampoco sancionar los incumplimientos.

La definición de Kaplan se basa en el concepto de *soberanía,* por el cual las *"*reglas especifican el ámbito de jurisdicción de todas las restantes unidades de decisión*".* Considera que la existencia de un gobierno es un síntoma empírico inequívoco de la existencia de un sistema político, donde la *Política* es el ámbito de competencia para asumir funciones de decisión que permitirán escoger entre diferentes objetivos políticos, o para cambiar las reglas esenciales de esos sistemas.

Particularmente en las relaciones internacionales se presta gran atención al dinamismo, al cambio. Considerado un factor desordenador, se generan mecanismos reequilibradores para conservar el *statu quo* y el orden, a través de los más poderosos que operan como árbitros.

Nos encontramos en un momento decisivo, caracterizado por la consolidación de nuevas potencias. Asistimos a un cambio de centro de gravedad estratégico global hacia la zona Asia-Pacífico y la profundización del retroceso de la Unión Europea, a lo que debe agregarse la presencia cada vez mayor de actores estatales y no-estatales con

capacidades bélicas que aprovechan la dependencia tecnológica vigente en nuestras sociedades y sus riesgos asociados para la seguridad.

Al efectuar el análisis, en la idea de estar ante una amenaza en la agenda de Seguridad Internacional, adscribimos a la teoría del Constructivismo que el Doctor Mariano Bartolomé (2006) define para analizar la variable Amenaza Transnacional. En ella interactúan múltiples actores, al tiempo que la dinámica propia de sus acciones dificultan la soberanía de los estados afectados.

A partir de la interdependencia compleja, algunos pensadores liberales como el politólogo y profesor de la Universidad de Harvard, Joseph Nye, (en una confluencia con algunos aspectos del realismo), admiten que el Estado continúa siendo el principal actor de la escena internacional. Pero al mismo tiempo apuntan con sus críticas a los realistas, al concluir que éstos le quitan importancia a todo otro actor relevante que no sea un Estado. (Nye, 1988b).

La interdependencia compleja reordena los temas de la agenda internacional al considerar que no existe jerarquía entre ellos. Le otorga un rol menor al poder de naturaleza militar a la hora de concretar acciones políticas, quitándole preeminencia a la fuerza militar como poder de decisión del Estado. Este a su vez tiene que enfrentar el desafío de ir viendo que el poder estatal se va difuminando, influido por los grandes avances tecnológicos en detrimento del Estado y en beneficio de otros actores no estatales.

Nye (2011), en su clasificación del concepto poder, señala tres tipos de poderes:

- el poder duro (*hard power*), basado en la coerción al usar los recursos militares y económicos;

- el poder suave (*soft power*), que utiliza lo que podría llamarse un tipo de seducción, atrayendo a los demás sin necesidad de fuerza, aunque se puede insinuar su uso y que utiliza factores como valores, cultura, la influencia y la cooperación, la conveniencia y legitimidad de las acciones; y

- el poder inteligente (*smart power*), una noción mixta, una mezcla adaptada a cada circunstancia de la combinación de los otros dos tipos de poderes ya mencionados. El poder inteligente no es ni duro ni blando, es ambos.

Según este autor, la importancia del poder está en los resultados que se obtengan y en la máxima proximidad que éstos alcancen con los objetivos que se buscan, y no propiamente en los recursos utilizados para hacerlo valer. Dice que combinando todas las facetas del poder es posible maximizar el poder que tienen los Estados, pero al mismo tiempo recuerda que no solamente los tipos de poder han cambiado; también cambia el contexto internacional donde los Estados conviven con otros actores no gubernamentales.

Enmarcado en lo que se dio a llamar el "Tercer Debate"[1], entre realistas y los defensores de las concepciones transnacionalistas o globalismo, Stanley Hoffmann (1978) esgrime su concepto de sociedad transnacional, señalando que ésta coexiste junto al plano interestatal, constituida por las relaciones protagonizadas por los individuos o los grupos que trascienden las fronteras de las unidades políticas de los Estados. Situado

[1] Primer Debate entre realismo Vs idealismo y el Segundo Debate entre tradicionalismo Vs cientificismo.

dentro del realismo existencial expresa que tener el poder no necesariamente implica que se esté en condiciones de usarlo.

En un artículo periodístico, Hoffmann recalcó que es preciso que el especialista en relaciones internacionales se esfuerce por entender los sucesos, pero al mismo tiempo debe dar su opinión acerca de lo que debiera hacerse:

> Es porque el futuro no es ni descifrable ni determinado, y porque el presente es tan poco tranquilizador que el especialista en Relaciones Internacionales tiene dos misiones y no una sola. Debe intentar comprender lo que pasa, pero también debe presentar sus opiniones sobre lo que convendría que hicieran los que toman las decisiones, las élites y los simples ciudadanos. Hoffmann (2002).

6. Metodología empleada.

Será del tipo de investigación de carácter descriptivo, es decir, analizando las características y procesos en relación con determinados actores y procedimientos o situaciones vinculados con el tema elegido, acotando la investigación al conjunto de autores señalados en la bibliografía.

La propuesta de esta investigación consiste en abordar por una parte, los aspectos relacionados con el modo en que se encara el tema en otros países en relación con la Ciberseguridad y Ciberdefensa, y por la otra, la posición adoptada por el Gobierno que ha sido plasmada en una serie de normativas de carácter nacional.

c. La descripción de la estrategia de prueba.

Se busca identificar las definiciones conceptuales desde una perspectiva que incorpore, de forma articulada, las dimensiones externa e interna, para una provechosa dirección y coordinación de la Política Nacional en materia de Ciberseguridad, que permita gestionar correctamente las situaciones de crisis de ciberseguridad que por su dimensión o carácter transversal desborden las capacidades de respuesta.

Se desarrolla un estudio exploratorio-descriptivo, tal que proporcione un orden a los conceptos centrales y sus interrelaciones necesarias para el análisis, tal que permita inferir las posibles respuestas al problema planteado.

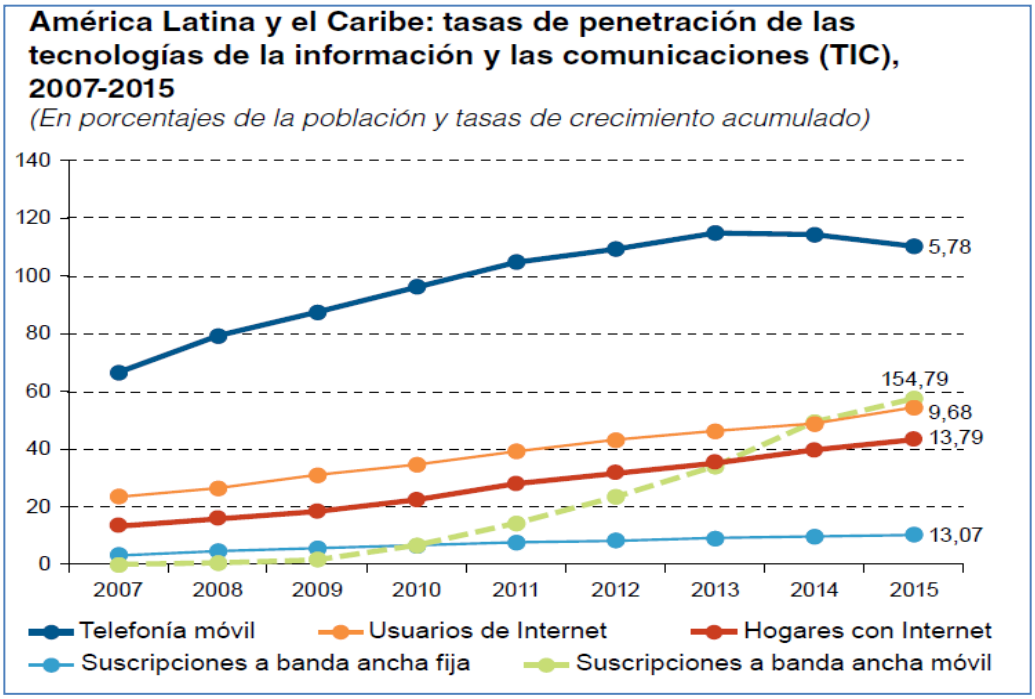
CAPÍTULO I
Definiciones y Conceptos

Sección 1
Ciberespacio

El ciberespacio, denominado el quinto dominio detrás de tierra, agua, aire y espacio exterior, ha surgido tras el desarrollo de las Tecnologías de la Información y la Comunicación (TIC). Estas se han convertido en una parte integral de las sociedades actuales, al tiempo que nuestra dependencia se incrementa constantemente y cuanto más dependa una sociedad de la tecnología, se vuelva más vulnerable. En el marco de reflexión para la comprensión de los cambios que expone Joyanes Aguilar (1997), las transformaciones sociales se muestran en una "magnitud comparable a las producidas por la aparición de la máquina de vapor".

El fenómeno está basado en la implementación de estas *autopistas* de la información, integrando servicios multimedia, realidad virtual, hipertexto, comunicaciones avanzadas (tales como satélites, fibra óptica, red RDSI, tecnología ATM, etc.).

Para ejemplificar podemos recurrir a la siguiente figura que muestra el incremento constante de las TIC en América Latina y el Caribe:



Fuente: ONU CEPAL (2016)

Zbigniew Brzezinski (1970) nos ha dicho que nos hallamos ante una "era tecnotrónica". Es un término acuñado de la combinación de tecnología y electrónica, para plasmar la integración entre la informática, la electrónica, las telecomunicaciones y lo audiovisual en aquel contexto.

No existe un único criterio para definir qué es y qué no es el ciberespacio. Kramer, Starr y Wentz (2009) incluyen las catorce definiciones (lo que revela la inmadurez del concepto) que Daniel Kuehl recopilara[2], quien, después de enumerar esas definiciones, ha definido al *Ciberespacio* como:

> Un dominio global dentro del entorno de la información cuyo carácter único y distintivo está enmarcado por el uso de los espectros electrónicos y electromagnéticos para crear, almacenar, modificar, intercambiar y explotar información vía redes interdependientes e interconectadas usando Tecnologías de la Información y la Comunicación.

En el mencionado trabajo Kuehl rechaza que el ciberespacio sea meramente algo "teórico" y destaca como aspecto distintivo y único que el ciberespacio está enmarcado por el uso de la electrónica y el espectro electromagnético. Y es en ese espacio donde transita la información a través de redes interdependientes e interconectadas que residen de forma simultánea tanto en el espacio físico como en el virtual, y dentro y fuera de las fronteras geográficas.

Siguiendo su concepto, el ciberespacio tiene características físicas únicas y determinantes. Sobre qué es lo que hace único al ciberespacio, es precisamente que se trata de algo más que computadoras e información digital interdependientes e interconectadas. Dos dimensiones importantes del ciberespacio son la información y su intercambio, combinadas precisamente al hacer uso de las TIC.

La norma ISO/IEC 27032:2012 define al Ciberespacio como "el ambiente complejo resultante de la interacción de la gente, el software y los servicios de Internet a través de aparatos tecnológicos y las redes interconectadas, que no existe en ninguna forma física". [3] Esta norma trata sobre la seguridad cibernética, presentando directrices para mejorar sobre la seguridad de la información, seguridad de Internet, seguridad de redes y protección de las IC. El grupo de estándares que conforma la serie 27xxx, agrupa las normas que tienen por finalidad fijar las medidas y actividades que se deben tener en cuenta en relación con los Sistemas de Gestión de la Seguridad de la Información.

En el Manual de Tallin[4] (2013) se define al Ciberespacio como: "El entorno formado por componentes físicos y no físicos, caracterizados por el uso de computadoras y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de redes informáticas".

España, en su Estrategia de Seguridad (EES), lo define así:

> Ciberespacio: Es el espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas *web*, foros, servicios de Internet y otras redes. Creado por el ser humano, es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos. Es mucho más

[2] Daniel Kuehl desarrolla el Capítulo 2, bajo el título "*From Cyberspace to Cyberpower: Defining the Problem.*"
[3] ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. En el campo de la tecnología de la información, la ISO y la IEC han establecido un comité técnico conjunto ISO/IEC JTC 1.
[4] Más adelante en este trabajo se analizará con más profundidad respecto al Manual de Tallin.

> que la Red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite. (EES 2011).

No es por completo verdadero el argumento sobre que el ciberespacio es un entorno hecho por el hombre. La dimensión del ciberespacio no representa una ubicación física específica propia; no consiste en un "espacio en sí mismo", sino una dimensión que, con reglas propias, cruza transversalmente a los dominios físicos tradicionales: tierra, mar, aire y espacio.

Cualquier definición no puede omitir una condición fundamental, la cual es la combinación de energía electrónica y electromagnética reconocida como "*el*" rasgo central distintivo del ciberespacio, es decir, sus características físicas únicas que lo distinguen de los otros dominios. Es decir que si una actividad depende de la utilización de la electrónica y la energía electromagnética, entonces está teniendo lugar en el ciberespacio. Por la manera en que el ciberespacio permite crear, almacenar, modificar, intercambiar y explotar la información, se ha transformado el modo de operar en los otros dominios y de usar los instrumentos del poder nacional.

El ya mencionado Kuehl sintetiza que *Poder Cibernético* es "la capacidad de usar el ciberespacio para crear ventajas e influenciar eventos en todos los otros entornos operacionales y a través de los instrumentos de poder". Para reafirmar sus dichos nos deja una definición que marca de forma tajante la diferencia: "Mientras que el ciberespacio es un entorno, el poder cibernético es siempre un indicador de la capacidad de utilizar ese entorno."

En sus definiciones de ciberespacio y de poder cibernético remarca las relaciones de estos conceptos entre sí y el impacto que tienen sobre los otros dominios y sobre los instrumentos de poder:

> Lo que diferencia al ciberespacio del dominio aeroespacial y del espacio exterior es el uso del espectro electromagnético como medio de 'movimiento' dentro del mismo, y esta distinción clara con respecto a los otros entornos físicos puede ser crucial para su desarrollo futuro dentro de la estructura de seguridad nacional.

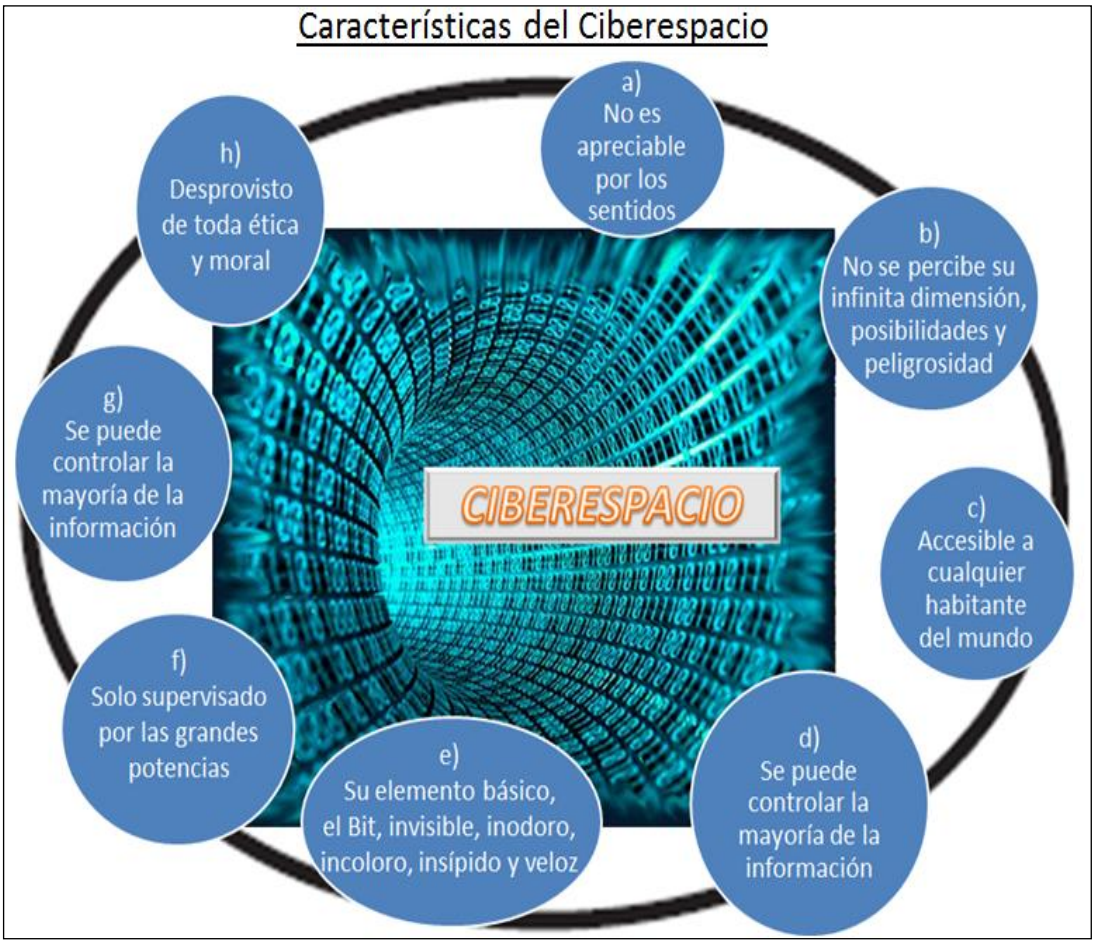
Por su parte Nye (2011) define en un solo renglón el impacto del ciberpoder: "El poder basado en los recursos de la información no es nuevo. El ciberpoder si lo es."

Por la rápida y permanente dinámica de la innovación tecnológica, una cada vez más amplia gama de factores sociales, políticos, económicos y actividades militares dependen del ciberespacio. Por ello son vulnerables tanto a la interrupción de su uso como a la usurpación de sus capacidades, lo que conlleva y exige, una constante adaptación de los sistemas de defensa.

A pesar de que sea sumamente útil en tiempo de paz, la interconectividad también significa que todo lo que tenga una conexión con Internet puede convertirse en un blanco desde cualquier parte del planeta. La interconectividad implica, además, que un ataque puede ocasionar efectos en diversos otros sistemas dado que las redes son, en muchos casos, componentes de la infraestructura comercial.

La amplia disponibilidad de acceso que ofrecen esas tecnologías, (celulares, tablets, Internet, blogs, aplicaciones de comunicación instantánea y gratuita, telefonía IP, etc.), junto al abaratamiento de los costos asociado a cada producto a causa de su uso masivo, da la ilusión de la desaparición de diferencias de clase y de ingresos. Paradójicamente, lo que representa una fortaleza de las sociedades occidentales es al mismo tiempo una debilidad. El desarrollo altamente tecnificado depende en grado extremo de una serie de servicios esenciales y si no se cuenta con ellos la capacidad de subsistencia se resiente de forma muy sensible.

El Coronel "VGM" Enrique Stel (2014) inicia su definición del ciberespacio con las siguientes palabras: "Es el espacio real y existente, invisible a los ojos, por el que transita el 90% de la información que emplea el mundo, transformada en simples objetos de conocimiento u órdenes de ejecución de actividades, haciendo uso de la inteligencia artificial*"*. Desarrolla un grupo de características que considera como las principales y que podemos ver resumidas en la siguiente figura:



Fuente: Elaboración propia con datos de Stel (2014) - *Seguridad y Defensa del Ciberespacio.*

En relación con el objeto de este trabajo final, creemos preciso destacar que el autor mencionado, respecto a la característica señalada en d) *Se puede controlar la mayoría de la información*, remarca que no se trata de "espiar al otro" sino que "se trata de obtener información" que "estratégicamente es crucial para la Seguridad y Defensa de un Estado soberano". Stel (2014).

Frente a los temores de un uso con fines de espionaje interno, el Dr. Roberto Uzal, académico especializado en ciberseguridad de la Universidad Nacional de San Luis, ha

señalado que su puede tener un control mediante el estudio de estadísticas sobre el tráfico realizado por los routers, y que "de ninguna manera puede considerarse violaciones de la privacidad de persona alguna." (Uzal, 2013b).

El ciberespacio ha creado el potencial para un nuevo ámbito de guerra, un teatro de operaciones bélicas que se añade a los campos de batalla tradicionales –tierra, mar, aire y espacio– y que está interrelacionado con todos los demás. El espacio virtual ofrece interconectividad sin pensar en fronteras, es instantánea y aún para aquellos con pocos conocimientos, puede llegar a ser casi anónima. Sin embargo, esto no es completamente cierto.

Lo que se denomina el "Problema de la Atribución" acera de la autoría de los ciberataques y del ciberespionaje, se ha convertido en un desafío mayúsculo para los Estados. Ya que éstos necesitan recopilar elementos probatorios para presentar ante los organismos internacionales, tanto sea para perseguir al atacante o para demostrar que desde su territorio no se han facilitado las actividades delictivas de terceros. No obstante, este problema no es imposible de ser resuelto.

El Dr Uzal (2013b) expresa que pueden desarrollarse herramientas que utilizan el Análisis de Flujos de Redes para monitorear "Patrones de Comportamiento" (y no datos) que pueden ser asociados a actividades sospechosas y obtener estadísticas que permiten determinar la autoría.

Es que existe una manera de representar al ciberespacio en múltiples capas. Como resultado de investigaciones acerca de los esquemas de red como DECNET, SNA y TCP/IP, la Organización Internacional para la Normalización (ISO) (International Standart Organization), durante 1984 estableció la estandarización internacional de los protocolos de comunicación.

El modelo de Referencia OSI (Open Systems Interconnection) fue creado para establecer la comunicación e interoperabilidad entre sistemas heterogéneos que habían sido diseñados con distintos lenguajes y utilizando implementaciones de hardware y software diferentes. Permite visualizar cómo viajan los paquetes de datos a través de la red. Así, el problema de trasladar la información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple.

Cada una de las capas que componen la arquitectura del Modelo OSI desempeña un conjunto de funciones bien definidas que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. Ellas proporcionan servicios por cada nivel que son utilizados por el nivel superior con una comunicación virtual entre capas, pero la comunicación física se lleva a cabo entre las capas de nivel 1.

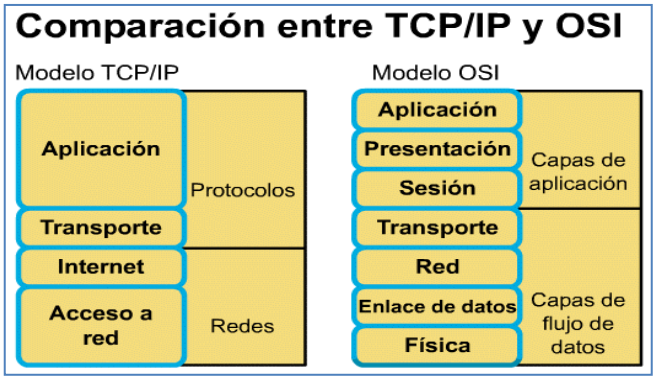
Al dividir en estas siete capas se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Estandariza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite que distintos tipos de hardware y software de red se comuniquen.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desempeñar con más rapidez.

FUENTE http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

Cada una de estas capas de la computadora que envía se comunica, mediante un protocolo de intercambio de información que se conoce como unidades de datos de protocolo (PDU), entre capas iguales en la máquina de destino, para que los paquetes de datos puedan viajar de un punto al otro. Esto se conoce como comunicaciones de par-a-par.

El modelo OSI es universalmente reconocido, pero el estándar de Internet es el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP), que cuenta con cuatro capas y aunque se las nombre de igual manera, tienen diferentes funciones respecto del modelo OSI.



FUENTE: http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

En el modelo OSI la capa "visible" para los usuarios es la capa número siete o capa de la aplicación (la más "externa"). Por lo tanto, la vigilancia es sobre los flujos en las capas tres y cuatro (capa de red y capa de transporte), obteniendo series numéricas que tomarán la forma de histogramas y que son representativas del comportamiento.

En la presentación de Uzal y otros (2015) se remarca que en el Análisis de Flujo de Red en Gran Escala, se trabaja fundamentalmente en el nivel 3, lejos del "nivel de aplicación" (nivel 7) que es el más sensible respecto del derecho a la confidencialidad del contenido de los datos de los usuarios.

En el Análisis de Flujo de Datos lo importante es identificar y vigilar "patrones de comportamiento" de los tráficos en las Redes Teleinformáticas. En la siguiente figura se mencionan los atributos que lo caracterizan:

Fuente: Uzal (2013a)

Con esta herramienta se pueden detectar determinados tipos de agresiones compatibles con ciberataques, y esa detección arroja altas tasas de efectividad con margen de error bastante bajo. Cuanto más crítico sea un recurso mayor será la necesidad de garantizar medidas para reducir el riesgo asociado.

Al analizar el riesgo es necesario tener en cuenta la combinación de tres factores importantes:

1) que debe protegerse,
2) detección de vulnerabilidades y
3) amenazas que pueden afectar lo que se intenta proteger.

Sección 2

Ciberseguridad

Aquí también nos encontramos con el problema de ausencia de definición común. Una situación que se reitera a menudo es confundir la Seguridad Cibernética (SC) con la Seguridad de la Información (SI) que circula por las redes. La segunda busca proteger la integridad y privacidad de la información y en este punto resultan muy apropiadas las palabras en Stel (2014) cuando nos grafica que "la SI es como la reja que protege la casa, evita que alguien entre pero el delincuente sigue afuera, esperando la oportunidad, la que lamentablemente en algún momento se produce".

No se debe confundir al término Ciberseguridad como sinónimo de Seguridad de la Información, ya que ocuparse de la seguridad de la información implica un alcance más abarcador que la ciberseguridad. Mientras la información puede ser verbal o escrita (en un papel o una simple madera), por otro lado, la ciberseguridad solo representa la protección de la información que se encuentra en formato digital y los sistemas interconectados que la procesan, transmiten o almacenan, por lo que está más emparentada con la seguridad informática. Tanto la definición de ciberseguridad como la de seguridad de la información tienen mucho en común; ambas deben estar libres de daños o cualquier limitación de su disponibilidad y confiabilidad.

Resulta útil para comprender la diferencia, la idea desarrollada por Luis Feliu (2013) cuando traza un paralelismo con las telecomunicaciones, en las cuales no es lo mismo *transec*, es decir, la seguridad de la transmisión (asegurarse que lo que se transmite se recibe), que la *infosec*, o sea, la seguridad del contenido de la información transmitida. La ciberseguridad comprende no sólo la confidencialidad de la información que circula sino también la seguridad de los sistemas. La ciberseguridad es un proceso de análisis de los riesgos y amenazas, con acciones que permitan reducir los riesgos a niveles y costos aceptables. En consecuencia, debe ser desarrollado por los Gobiernos, dado las responsabilidades del Estado en la protección de personas y patrimonios.

La norma ISO/IEC 27032 antes mencionada, define a la ciberseguridad como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio". Por confidencialidad se entiende que la información no se divulgue a quien no esté autorizado a conocerla o manejarla. Por integridad se entiende a la propiedad de mantener la exactitud y por disponibilidad a que sea accesible ante la demanda de una entidad autorizada. Por esas tres características es común encontrar que se refiera como CIA, por el uso de esos términos en inglés (confidentiality, integrity, availability).

En palabras de Gómez Bule (2014), es probable que tanto Internet como las otras TICs hayan "promovido un tercer salto evolutivo en las capacidades de interrelación y comprensión del ser humano", ubicándolo a este salto de la cibernética por detrás de la escritura y de la invención de la imprenta. Los cambios sociales han sido de una gran importancia, de gran rapidez y nuevas oportunidades, así como también simultáneamente, se han multiplicado los peligros y las incertidumbres. Menciona la definición de la primera Estrategia Española de Seguridad Nacional (EES) de 2011, que señala que:

> "La ciberseguridad no es un mero aspecto técnico de la seguridad, sino un eje fundamental de nuestra sociedad y sistema económico. Dada la cada vez

> mayor importancia de los sistemas informáticos en la economía, la estabilidad y prosperidad económica del país dependerá en buena medida de la seguridad de nuestro ciberespacio." (Gomez Bule, 2014).

La Unión Internacional de Telecomunicaciones (UIT)[5], en la búsqueda de consenso en la definición, desarrollando el programa de acciones de Túnez[6] en el seno de Naciones Unidas, la define como la respuesta de una nación coordinada; una solución multidisciplinar que conlleva aspectos de orden educativo, jurídico, administrativo y técnico, donde la información debe ser tratada como un activo crítico que permite la gobernabilidad. Dado que no existe el riesgo nulo y es difícil prever todas las amenazas que se pueden presentar, hay que reducir la vulnerabilidad del entorno y de los recursos a proteger. (UIT, 2007). Más adelante, la misma UIT definió a la 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. (…) La ciberseguridad incluye para la información, una o más de las siguientes propiedades: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad". (UIT, 2008).

En la misma Recomendación, la UIT define como objetivo de la ciberseguridad a la protección del ciberentorno, definiendo a éste como "un sistema que puede incluir múltiples entidades públicas y privadas", por lo cual propone que deberían ser utilizados distintos métodos para la protección de los sistemas, las redes, las aplicaciones y los recursos .Dentro de este entorno debe incluirse el software, la información almacenada (y transmitida) y además a las instalaciones y los edificios. La ciberseguridad debe proteger todo el ciberentorno, utilizando diversos componentes y distintos métodos.

La ciberseguridad debe ser considerada desde la perspectiva de:

> – El conjunto de políticas y acciones que se utilizan para proteger las redes conectadas (incluidos los ordenadores, los dispositivos, el hardware, la información almacenada y la información en tránsito) del acceso y la modificación no autorizados, el robo, la interrupción u otras amenazas.
> – Una evaluación y supervisión constantes de dichas políticas y acciones a fin de garantizar la continua calidad de la seguridad frente a la naturaleza voluble de las amenazas.

Al hablar de ciberseguridad se debe tener en cuenta la convergencia de la interconexión de sistemas internos, la interdependencia con sistemas externos y la necesidad de estándares abiertos a todo el mundo. Por lo tanto la gestión de la ciberseguridad es lo que Sánchez Gómez-Merelo (2011) define como:

> Un proceso deliberado de análisis de los riesgos y amenazas, y de decisión y ejecución de acciones, con objeto de reducir el riesgo a un nivel definido y aceptable, a un coste razonable, teniendo en cuenta, igualmente, las vulnerabilidades del sistema y actividad.

5 Agencia especializada de las Naciones Unidas para las tecnologías de la información y la comunicación.
6 La Cumbre Mundial sobre la Sociedad de la Información en sus fases de Ginebra y Túnez congregó a organizaciones, gobiernos, empresas y a la sociedad civil para acordar una visión común de la sociedad de la información.

Otra definición que podemos encontrar es la que ha adoptado Colombia. El Consejo Nacional de Política Económica y Social (CONPES) es un organismo asesor del Gobierno de Colombia en materia de desarrollo económico y social, y es el encargado de estudiar y recomendar políticas generales en esas áreas. A través del Departamento Nacional de Planeación ha definido a la Ciberseguridad como la "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética". (CONPES, 2011).

Partiendo del hecho que los dispositivos tecnológicos han sido diseñados para que funcionen con rapidez sin prestar tanta atención a que sean seguros, el abanico de amenazas es amplio. Ante estas amenazas, la ciberseguridad no sólo debe contemplar la prevención frente a ellas, sino también el control y mitigación de daños en caso de producirse un incidente.

En el caso de España, existe la Guía CCN-STIC 8177, cuyo propósito es ayudar a las entidades públicas a tipificar claramente los ciberincidentes y determinar su peligrosidad. Esta Guía tiene una clasificación de nueve tipos de ciberincidentes y 36 subcategorías, que se incluyen en una tabla que permite clasificarlos por la peligrosidad potencial que tengan. Esta tipificación facilita el intercambio de información. En función del tipo y origen de la amenaza, el perfil de usuario afectado, el tipo y la cantidad de los sistemas afectados junto con el impacto que puede tener, los clasifica como Crítico, Muy Alto, Alto, Medio y Bajo, como se puede ver en la siguiente tabla:

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES

NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	Ciberespionaje	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
MUY ALTO	Interrupción de los Servicios IT / Exfiltración de datos / Compromiso de los servicios	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL. - Spear phising / pharming	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	Logro o incremento significativo de capacidades ofensivas / Desfiguración de páginas web / Manipulación de información	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social. -	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de de algún sistema.
BAJO	Ataques a la imagen / menosprecio / Errores y fallos	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

Figura (Fuente: adaptación de la Guía CCN-STIC 817)

[7] La Guía CCN-STIC 817 puede descargarse desde la parte pública del portal del CCN-CERT https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

APT se refiere a un tipo de amenazas a la ciberseguridad que presenta un mayor grado de daño que los habituales. Por sus características a más largo plazo hacen que sus efectos sean más dañinos. Las *amenazas persistentes avanzadas* (en inglés APT por Advanced Persistent Threats) son capaces de aprovechar vulnerabilidades desconocidas oficialmente y por ello pasar inadvertidas, perdurando más tiempo al infectar una máquina. Suelen ser programas especialmente diseñados por actores de elevados recursos, no comparables al malware o amenazas, con capacidad de fragmentación, que le permite descargar módulos encargados de diferentes tareas.

Con base en estos criterios comunes, la clasificación sintética se representa en la siguiente pirámide:

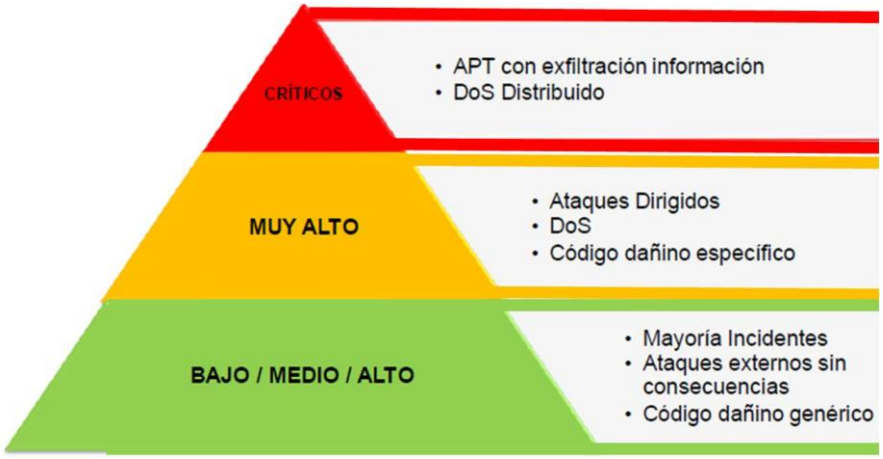


Figura (Fuente: adaptación de la Guía CCN-STIC 817)

Sección 3

Ciberguerra

Tampoco existe una definición acerca de qué es la Ciberguerra. Se confunde Guerra Cibernética (GC) con Guerra Electrónica (GE) porque ambas comparten el contexto de trabajo, lo cual induce a dicha confusión. Como nos aclara Feliu (2013), al utilizar la radiación electromagnética en sus diversas formas y frecuencias, estamos en presencia de GE, en tanto que como acciones de GC debe considerarse a "aquellas que utilizan ordenadores en los sistemas informáticos."

Algunos autores, Ventre (2016), Tyagi (2013), Jolley (2013), Schreier (2015) e incluso el CEDEF[8] (2015) - sugieren que la Resolución 1113[9], "*adoptada"* por el Consejo de Seguridad de las Naciones Unidas el 5 de marzo de 2011, ha definido a la guerra cibernética. Esto no es así, ya que se trata de una resolución que se circunscribe al Modelo "ON CYBER WARFARE" de la University for Peace.

Los Modelos de Naciones Unidas (MNU o MUN por sus siglas en inglés, Model United Nations) son un simulacro o representación de la Asamblea General y de otros órganos multilaterales de la ONU, donde participan alumnos de escuelas secundarias o universidades, actuando como delegados de diferentes países que intervienen en debates y negociaciones, según temas que se corresponden con los programas de trabajo de los diferentes órganos y comisiones. Son eventos educativos y culturales donde los jóvenes, además de capacitarse sobre el funcionamiento de la ONU, adquieren una visión global de la política internacional.

Mencionaremos, no obstante, la mencionada resolución de 2011, según la cual, la guerra cibernética sería:

> 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:
> - 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".

Schreier (2015) agrega otra definición: Ciberguerra es la actividad digital en red, simétrica o asimétrica, ofensiva o defensiva, por parte de Estados o actores que actúan como tales, que incluyan daño a la infraestructura nacional crítica y sistemas militares. (N. del A.: La traducción es propia).

8 CEDEF - Centro de Estudios para la Defensa Nacional, de la Universidad de Belgrano. Su Director es el Doctor Horacio Jaunarena. (Subsecretario de Defensa: Dic 83/Dic 84; Secretario de Defensa: Dic84/Jun86; Ministro de Defensa: Jun 86/Jul 89 y Ministro de Defensa: May 2001/May 2003).

9 La verdadera Resolución S/RES/1113, es del 12 de junio de 1997 y trata sobre la prórroga del mandato de la MONUT en Tayikistán. Las resoluciones del CS se publican como documentos individuales y son enumeradas de manera consecutiva desde 1946. Antes de 1964 no contaban con una determinada signatura. Eran emitidas como documentos generales con la signatura S/-. A partir de 1964, según la estructura: código de signatura: S/RES/-- (año).

Chapple y Seidl (2014), puntualizando que no existe una definición aceptada por todos los planificadores militares, ofrecen una definición concisa, por la cual se entiende que la ciberguerra incluye un amplio abanico de actividades que utilizan los sistemas de información como armas, en contra de una fuerza opositora. Las dos principales actividades comprenden a los ciberataques y al ciberespionaje. Y es la combinación de ambas en forma ofensiva y defensiva lo que constituye la ciberguerra, cualquiera sea el lado del que proviene el ataque, porque ambos bandos buscarán ganar ventaja cuando le sea posible.

Por su parte Gómez Bule (2014) señala que la ciberguerra comprende todas aquellas operaciones originadas por un Estado o por un actor no estatal, (organización terrorista, milicia insurgente o fuerza paramilitar), que están orientadas a penetrar sin autorización en las computadoras y sistemas o redes de información de otro Estado, con el propósito de cometer daño.

Clarke y Knake (2011) expresan que son "Aquellas acciones realizadas por un Estado-nación con el fin de penetrar los ordenadores o las redes de otra nación y el propósito de causar daños o perturbar su adecuado funcionamiento".

En su artículo Nye (2012) menciona una breve definición de ciberguerra, simplemente como "una acción hostil en el ciberespacio cuyos efectos amplían o son equivalentes a una violencia física importante". Al mismo tiempo, por dejar de lado las consecuencias reales en el mundo físico, critica a los expertos que la definen como "una guerra sin derramamiento de sangre entre estados que consiste exclusivamente en un conflicto electrónico en el ciberespacio".

Pastor Acosta (2012) llama la atención sobre que "los ciberataques son ataques a la infraestructura TIC originados desde el propio ciberespacio, excluyendo por tanto los ataques físicos a las TIC". Ciertamente, lo que se denomina "ciberataque" comprende un amplio abanico. Puede ser una simple exploración, infiltrar un sistema informático, activar o manipular un determinado software, la saturación o la interrupción del servicio, el espionaje y la destrucción o desconfiguración de una página web. Lo que al principio era una demostración de vulnerabilidades o una forma pacífica de mostrar el quebrantamiento de las medidas de seguridad, se ha ido convirtiendo paulatinamente en armas de la guerra informática.

Por último, tomamos la visión del Doctor Uzal (2012) acerca de lo que él se encarga de remarcar como "una cuestión fundamental":

> La experiencia acumulada a la fecha muestra claramente que, en el nuevo contexto de confrontación entre países utilizando Armas Cibernéticas sumamente sofisticadas, resulta estrictamente necesario que se conformen bloques o alianzas político / tecnológicas. Este sistema de alianzas, en el ámbito de la denominada Guerra Cibernética, ha sido necesario, inclusive, para los Estados Unidos de América.

Sección 4

Ciberdefensa

En el ciberespacio, con independencia de su grado de protección, todos los usuarios son susceptibles de recibir ataques. No se trata de visiones apocalípticas. No se puede decir que los ataques contra infraestructuras críticas sean una ilusión. Ya se han visto y esto indica que se debe poner esfuerzo en buscar soluciones de manera anticipada. Los ciberataques constituyen una amenaza en crecimiento y si provienen de otro Estado-nación, se deberá dar intervención a la Ciberdefensa, en tanto que para otros casos, será responsabilidad de la Ciberseguridad.

El uso más generalizado del término Ciberdefensa está asociado al conjunto de acciones y mecanismos que el Estado emplea en contra de toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional. A tal efecto se empeñan los recursos humanos y materiales de sus propias fuerzas armadas. Es que no se trata de defender el ciberespacio militarmente, sino defender aquellos activos que sean de interés militar, o colocados bajo su responsabilidad.

Para el Comandante del Mando Conjunto de Ciberdefensa (MCCD) español, General Gomez Lopez de Medina, "la ciberdefensa es el componente específico y distintivo de la ciberseguridad" y la define como "el conjunto de acciones, medios y procedimientos para asegurar el uso propio del ciberespacio y negarlo al enemigo". Delimitada generalmente al ámbito de las redes y sistemas militares, se reconoce que en algunos casos se amplía a sistemas con infraestructuras críticas. Para poder cumplir su cometido, la cooperación es vista como factor clave, porque permite explorar las técnicas o procedimientos que están utilizando otros, compartir experiencias y aprender de las operaciones recientes a nivel nacional e internacional. (CIBER Elcano, 2016).

En el caso de Feliu (2013), al igual que Acosta y otros (2009), ambos reproducen la definición de la OTAN de febrero de 2008, que en su MC0571 (NATO Cyber Defence) la define como "la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques". La Reunión de Ministros de Defensa de la OTAN del 10 de marzo de 2011, revisó la Política de Ciberdefensa, recalcando que se trata de un ámbito de la seguridad nacional, donde las acciones tomadas para responder a la agresión deben ser coordinadas. En cuanto a la cooperación internacional, la política establece que tanto la OTAN como los aliados trabajarán con las organizaciones internacionales, el mundo académico y el sector privado de forma que se promueva la complementariedad y se evite la duplicación de esfuerzos.

El Consejo Nacional de Política Económica y Social (CONPES) de Colombia, tampoco la "sectoriza" al considerarla que protege a todo, ya que ha definido a la Ciberdefensa como la "Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional". (CONPES, 2011).

López de Turiso, J. (2012) resalta que la ciberdefensa no es sólo ciberdefensa militar, sino que debe ser ciberdefensa nacional con la particularidad que lo militar sólo deberá ser una parte más de ella.

Pastor Acosta (2012) ubica a la ciberdefensa como un subconjunto operativo más, dentro de las capacidades de ciberseguridad, resaltando esto como algo lógico y coherente, al analizar análogamente a la Defensa como la parte operativa para garantizar la Seguridad Nacional.

Feliu Ortega, L. (2012) argumenta que deberá existir una ciberdefensa que garantice la ciberseguridad, donde trabajen de forma integrada las distintas agencias de seguridad e inteligencia del Estado y los centros de investigación tanto públicos como privados, así como también debe haber coordinación con el sector privado y los propios ciudadanos. Agrega que en el plano internacional, la ciberdefensa debe ser parte de la estrategia de defensa colectiva.

Todos los países, en mayor o menor medida, la relacionan con la protección de las infraestructuras críticas. En ellos, la ciberdefensa comprende todas las acciones y medidas necesarias para garantizar la ciberseguridad, que deben formularse proactivamente como un continuo proceso de análisis y gestión de las amenazas. Debe ser multidisciplinar o multidimensional, por lo que debe contemplar también los aspectos judiciales.

Como se resume en CEDEF (2015), debe entenderse a la ciberseguridad como un objetivo y la ciberdefensa como un medio para alcanzarla, mediante la libertad de acción de las operaciones militares en el ciberespacio ante un ciberataque que pueda afectar a la defensa nacional.

En la seguridad de las infraestructuras críticas (IC), el trabajo debe consistir en la prevención de posibles ataques, la disminución de vulnerabilidades y en caso de crisis, minimizar los daños y potenciar la resiliencia, o sea, acelerar el proceso que disminuya el periodo de recuperación. La resiliencia es el proceso de "rebote" de una experiencia difícil, que resulta de la capacidad de adaptarse ante la adversidad. Es afrontar con flexibilidad y fortaleza las situaciones de crisis y sobreponerse, minimizando y absorbiendo las consecuencias negativas. No significa que no se experimenten dificultades, sino que la recuperación y la salida permitan por lo menos volver al estado anterior de tenerlas.

La protección de IC comprende una serie de instituciones gubernamentales, organismos y hasta empresas del sector privado, que tienen su cuota de responsabilidad en el funcionamiento de los servicios esenciales. Por ello se hace hincapié en que la seguridad debe ser encarada desde una perspectiva integral. Se categorizan en Infraestructuras estratégicas (instalaciones, redes, sistemas y equipos físicos y de TIC necesarios para el funcionamiento de servicios esenciales) y las Infraestructuras críticas (aquellas infraestructuras estratégicas indispensables que no tienen soluciones alternativas).

Para Colombia (CONPES, 2016), la infraestructura crítica cibernética nacional es aquella cuya "afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública". Por su parte, para los Estados Unidos y según la USA Patriot Act de 2001, son los "Sistemas y activos, ya sea físicos o virtuales, tan vital para los Estados Unidos que su incapacidad o destrucción provocaría un impacto sobre la seguridad, la economía nacional, la salud pública o la seguridad nacional, o cualquier combinación de las anteriores.".

Cuando nos referimos a cuál es la Infraestructura Crítica que debiera estar bajo la protección de la Ciberdefensa, encontramos en STEL (2005) una lista acotada que enumera a modo de ejemplo y entre otros, la Bolsa y Mercado de Valores; los sistemas satelitales de comunicación; la canalización de la distribución de gas; las estaciones de control aéreo y hasta la distribución de la energía eléctrica.

Otra lista podemos encontrar en el trabajo del consultor internacional Sanchez Gomez-Merelo (2011) que incluye:

- Administración (servicios básicos, instalaciones, redes de información, y principales activos y monumentos del patrimonio nacional);
- Instalaciones del Espacio;
- Industria Química y Nuclear (producción, almacenamiento y transportes de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.);
- Agua (embalses, almacenamiento, tratamiento y redes);
- Centrales y Redes de energía (producción y distribución);
- Tecnologías de la Información y las Comunicaciones (TIC);
- Salud (sector e infraestructura sanitaria);
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.);
- Alimentación (producción, almacenamiento y distribución); y
- Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones).

Fuente: Adaptación de Sanchez Gomez-Merelo (2011)

La protección de las infraestructuras críticas no puede ser sino un proceso continuo y sistemático, a través del análisis permanente. Cabe destacar que al momento de elegir el procedimiento de protección de las infraestructuras críticas, se contemplan medidas físicas para neutralizar amenazas externas, tales como vigilancia con cámaras y controles de accesos. Tampoco deberían ser obviados los controles para prevenir una mala actuación interna, por error u omisión, proveniente del eslabón más vulnerable, es decir, las personas.

CAPÍTULO II
El enfoque de otros Actores Internacionales

Sección 1
CERTs

Cuando apareció el primer software malicioso a gran escala con capacidad de autoreplicarse (el gusano Morris programado por Robert Tappan Morris), la Universidad de Carnegie Mellon creó el primer Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team). Como la universidad registró ese acrónimo, ahora es utilizado el término CSIRT, que significa *Computer Security Incident Response Team* (equipo de respuesta a incidentes de seguridad informática). (Gomez Hidalgo, 2014).

Ante la presencia de amenazas e incidentes de inseguridad informática, la opción para enfrentarlos fue crear estos equipos de expertos en seguridad de las TIC, cuya principal tarea es contar con una permanente capacidad de respuesta rápida y además ayudar a evitar incidentes futuros. Al principio eran una mera fuerza de reacción, pero en la actualidad han ampliado sus capacidades e incluyen servicios preventivos como alertas, avisos de seguridad, formación y servicios de gestión de la seguridad. Ambos términos (CERT y CSIRT) se usan como sinónimos. El significado original de la letra R fue *Response;* sin embargo, coincidiendo con Pastor Acosta (2012), para ajustar el significado al servicio real que prestan estos equipos, debiera ser modificado por *Readiness* (disponibilidad; estar disponible).

Como explica el Dr Uzal (2013a), el procedimiento de trabajo del CSIRT para dar respuesta a incidentes, se realiza de forma remota, por teléfono, correo electrónico, fax, etc, de forma que el personal en el propio lugar afectado pueda ir recuperando los sistemas afectados.

Los CSIRT nacionales abarcan todos los sectores vitales de las TIC del país y protegen a los ciudadanos, centrándose principalmente en la protección de la información vital y las infraestructuras vitales. Además otros CSIRT especializados (como de la industria o el sistema bancario) colaboran estrechamente con los ministerios públicos relacionados. Los CSIRT del sector militar prestan servicios a organizaciones militares con responsabilidades en infraestructuras de TIC necesarias con fines de defensa, teniendo estrechas relaciones con los Ministerios de Defensa.

Por ejemplo, Acosta y otros (2009) señalan que el US Computer Emergency Readiness Team (US-CERT) de la órbita gubernamental, coordina la defensa y la respuesta ante los ciberataques a lo largo de toda la nación y opera como aglutinador de la información que se comparte entre las organizaciones federales, estatales y locales. El Comando Estratégico (USSTRATCOM) delega lo relativo al ciberespacio en el Comando Cibernético (USCYBERCOM), responsable de gestionar los incidentes en la Red. Al mismo tiempo debe asegurar la integridad y disponibilidad e integrar su trabajo con otras agencias en conjunto. El titular del USCYBERCOM también es el Director de la Agencia Nacional para la Seguridad (ANS), una agencia militar subordinada al Departamento de Defensa que desde 1952 tiene como misión recolectar señales de inteligencia extranjeras, aun cuando no se trate de enemigos.

Como puede verse, el enfoque de ciberdefensa norteamericano difiere del que impera en la Unión Europea. La importancia que tiene la ciberseguridad para la administración norteamericana queda reflejada al ubicar al Comandante del USCYBERCOM al mismo tiempo como director de la ANS.

Desplegados por el mundo, los CSIRT usan los resultados del análisis de vulnerabilidades y los incidentes para entender y desentrañar lo que ha sucedido en casos concretos y analizar de la forma más completa y actualizada posible los incidentes para determinar interrelaciones, tendencias, modelos y firmas intrusas. La recopilación de pruebas forenses procedentes de un sistema informático comprometido, para determinar cambios en el sistema y ayudar a reconstruir los eventos que han comprometido la seguridad, se debe hacer de tal forma que se documente toda la actividad.

Categorización de los incidentes. Todos los incidentes que maneje un CSIRT deberían entrar en una de las categorías de la siguiente lista:

Incident Category	Sensitivity*	Description
Denial of service	S3	▪ DOS or DDOS attack.
Forensics	S1	▪ Any forensic work to be done by CSIRT.
Compromised Information	S1	▪ Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	▪ Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	▪ Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	▪ Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	▪ Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	▪ A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	▪ Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	▪ Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	▪ Sharing offensive material, sharing/possession of copyright material. ▪ Deliberate violation of Infosec policy. ▪ Inappropriate use of corporate asset such as computer, network, or application. ▪ Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Fuente: FIRST.org - Obtenido de https://www.first.org/resources/guides/csirt_case_classification.html

Tanto el análisis de las pruebas por un lado, que pueden ir desde la realización de una copia bit a bit del disco duro de los sistemas afectados; la búsqueda de cambios en el sistema, tales como nuevos programas, archivos, servicios y usuarios; el examen de los procesos en ejecución y los puertos que fueron abiertos, así como por otra parte su conservación, deben desarrollarse de tal forma que sean demostrables y admisibles para ser presentados como medio de prueba ante los foros correspondientes.

El seguimiento, o rastreo de un intruso o identificar sistemas a los que éste haya tenido acceso, es también una actividad esencial de un CSIRT. Averiguar cómo accedió el intruso a los sistemas afectados y las redes relacionadas qué utilizó y desde dónde se originó el ataque, podrían llevar a la identificación del intruso.

Cada CSIRT nacional es el punto de contacto para una coordinación permanente con otros similares, para compartir los resultados de los análisis y las respuestas. Esto ha llevado al surgimiento de lo que podría ser el CSIRT global que relaciona los CERTs reconocidos de los diferentes países. Se trata del FIRST (*Forum of Incident Response and Security Teams*), fundado en 1990, que se considera la organización de CSIRT líder mundial. Fomenta la cooperación y la coordinación en la prevención así como el intercambio de información entre sus miembros.

En el ámbito de la UE, los principales CERTs gubernamentales de Europa se nuclean bajo el Grupo EGC (*European Government CERTs Group*); un grupo eminentemente operacional con un enfoque técnico. No determina políticas. Se trata de una asociación informal donde los miembros efectivamente cooperan en asuntos de respuestas a incidentes, trabajando especialmente sobre la base de confianza mutua y entendimiento.

Bajo la autoridad de la Comisión Europea, el 10 de marzo de 2004 fue creada la Agencia Europea para la Seguridad de la Información y de las Redes, ENISA (*European Network and Information Security Agency*). Tiene como objetivo garantizar un nivel elevado y efectivo de seguridad de las redes y de la información en la Unión Europea y al mismo tiempo ayudar al desarrollo de una cultura de seguridad.

En el caso de la Organización del Tratado del Atlántico Norte (OTAN), se estableció en Tallin (capital de Estonia), el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE: *Cooperative Cyber Defence Centre of Excellence*) para fomentar la investigación y la formación del personal de la Alianza en temas de seguridad cibernética y contribuir a la cultura de la colaboración en dicho campo. Este centro no forma parte de la estructura del Comando de la OTAN ni tampoco fue fundado por ella. Sin embargo, forma parte de un marco más amplio que respalda los Acuerdos de la OTAN.

Por invitación del Centro de Excelencia y luego de tres años de trabajo, un "Grupo Internacional de Expertos Independientes", hizo conocidas sus conclusiones a través del *Manual De Tallin Sobre El Derecho Internacional Aplicable A La Guerra Cibernética*. En este Manual se hace un análisis legal de los incidentes más comunes, así como de otras formas más severas de ciberoperaciones que pueden equipararse con el uso de la fuerza. Reafirma que estas operaciones no ocurren en un vacío legal, sino que por el contrario, los Estados tienen tanto derechos como obligaciones en el ciberespacio, donde las normas legales previas a la era cibernética se pueden y deben aplicar.

Muchos países miembros de la OEA (Organización de Estados Americanos) iniciaron sus esfuerzos en materia de Ciberseguridad con el establecimiento de equipos de respuesta CERT. Estos países habían adoptado por unanimidad la Estrategia Interamericana Integral de Ciberseguridad en 2004, nueve años antes que la UE adoptaba una Estrategia de Ciberseguridad en febrero de 2013.

Acompañando la evolución de las amenazas, los gobiernos aprobaron una declaración sobre el "Fortalecimiento de la Ciberseguridad en las Américas" en marzo de 2012. Otras acciones incluyen la Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes de 2015, adoptada por el Comité Interamericano contra el Terrorismo (CICTE) de la OEA. También durante abril de 2015 fue dado a conocer el primer *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas* (OEA, 2015) que contiene la información de los ataques sufridos por las infraestructuras críticas en la región, así como las políticas y la colaboración de los gobiernos locales. En el *Resumen Ejecutivo* del citado informe se llega a la siguiente conclusión: "los gobiernos de la región necesitan tender la mano a los encargados de la infraestructura crítica que buscan ayuda y guiarlos para ofrecer mejor protección contra los crecientes ataques a este sector crucial".

Otro ejemplo es Colombia, primer país latinoamericano en adoptar estrategia de ciberseguridad y ciberdefensa. En el marco político que aprobara el CONPES en 2011, para proteger a la ciudadanía de los riesgos informáticos, el Gobierno creó tres dependencias:

- el colCERT, *Grupo de Respuesta a Emergencias Cibernéticas de Colombia*, integrado por funcionarios civiles y personal militar. Es el órgano público responsable a escala nacional de la coordinación de la Ciberseguridad y Ciberdefensa Nacional, con especial interés en la vulnerabilidad de la infraestructura crítica.

- el Comando Conjunto Cibernético de las Fuerzas Militares, responsable de salvaguardar los intereses nacionales en el ciberespacio; y

- el Centro Cibernético Policial, a cargo de la prevención e investigación y del apoyo a la judicialización de los delitos informáticos.

Para fijar la visión estratégica y darle el direccionamiento al colCERT se ha establecido una Comisión Intersectorial encabezada por el Presidente de la República e integrada por el Ministro de Tecnologías de la Información, Ministro de Defensa, el Alto Consejero para la Seguridad, el Director del Departamento Administrativo de Seguridad, el Director de Planeación Nacional y el Coordinador del colCERT. (CONPES, 2011).

Pasando a la República Federativa de Brasil, vemos que la ciberseguridad se encuentra directamente a cargo de la Presidencia de la República y a cargo del Ministerio de Defensa, a través de las fuerzas armadas, está la defensa cibernética (CEDEF, 2015). En este país la defensa nacional y la seguridad interior no se autoexcluyen, es más, resultan complementarias una de la otra, lo que explica que según las políticas de ciberseguridad y de ciberdefensa, los organismos responsables deben también ser complementarios, trabajando en conjunto.

La adopción de estos pasos muestra que existe una tendencia generalizada de los Estados en buscar la mejor forma de lograr una gestión integral de la Ciberseguridad y que hay consenso político sólido tendiente a lograr la cooperación y el intercambio de información. Tal como se resalta en CEDEF (2015), "tanto ciberseguridad y ciberdefensa forman parte de un mismo abanico de herramientas y procedimientos del que las naciones tienen que disponer para garantizar su libertad".

Sección 2

Estrategia y Seguridad Cooperativa

La Carta de las Naciones Unidas expresamente prohíbe la guerra y el Derecho Internacional obliga a encontrarle solución pacífica a los conflictos. Pero esto no es determinante para que no haya ninguna guerra. Para anticiparse y estar preparado un Estado debe tener una Estrategia. Esto no se trata de un simple plan. Es un método para ordenar el razonamiento, tal que permita identificar el problema, plantear los posibles caminos a seguir y escoger la mejor solución estimada.

Pero como resalta el Coronel Cornut "si bien puede y debe ser plasmada en un plan – que traduzca el pensamiento en acción – no es posible limitar el concepto a una secuencia ordenada de pasos". Se destaca además que la estrategia estará siempre inmersa en un ambiente de incertidumbre y que deberá contar con capacidad anticipatoria, ya que en caso de carecer de esta aptitud, sería una mera "lista de actividades cotidianas programadas". (Cornut 2009).

Se puede decir que se trata de una abstracción teórica para hallar soluciones que, según el concepto extendido de la corriente Beaufre, deben ser aplicables a la conducción de todos los medios del poder nacional en la paz o en la guerra. Es bajo esta premisa que los Estados han empezado a elaborar su Estrategia Nacional de Ciberseguridad dentro del marco de la Seguridad Nacional, dado que la Ciberseguridad es una función, que enfrenta un problema real y actual, que afecta a la Seguridad Nacional. Necesariamente hay que coincidir con Joyanes Aguilar (2010), cuando expresa que "La seguridad del ciberespacio es un objetivo estratégico de la seguridad nacional. El impacto de una amenaza sobre el ciberespacio tiene implicaciones sociales y económicas en el país".

Podemos ver también a Kuehl (2009) yendo en el mismo sentido, cuando define a la *Estrategia Cibernética* como:

> El desarrollo y el empleo de capacidades estratégicas para operar en el ciberespacio, integrada y coordinada con los otros dominios operacionales, para lograr o apoyar el logro de los objetivos a través de los elementos del poder nacional en apoyo de la estrategia de seguridad nacional.

El ex Ministro de Seguridad Interior de EEUU, Michael Chertoof (al escribir el prólogo de Carr 2012), no solamente alienta para que se determinen cuáles medidas podrían ser tomadas de manera ofensiva para eliminar o desalentar las amenazas críticas, sino que advierte acerca de la necesaria formulación de una estrategia que las englobe. De lo contrario serían acciones incompletas.

Las posibilidades de ser el blanco de un ciberataque están proporcionalmente ligadas a la importancia estratégica que tenga el actor. A mayor importancia, mayores posibilidades. La complejidad para la estrategia está dada por el imperativo de trabajar con escenarios a mediano y largo plazo.

Según Keohane y Nye (1988a), la interdependencia implica que existen múltiples grupos no estatales, trasnacionales, organizaciones no gubernamentales, movimientos sociales y otros grupos de presión materializando canales que interconectan a las sociedades. Esto pone en tela de juicio el papel del Estado como supremo actor de la

arena internacional, que se encuentra matizada por el accionar de esos actores en una red de relaciones globales que, sumadas al dinámico desarrollo de las tecnologías de las comunicaciones, erosionan el concepto de soberanía del Estado.

La unidad de análisis ya no es el Estado, el cual parcialmente pierde su carácter de actor principal. El poder no solo se define en términos militares. Más que la fuerza militar, son los recursos económicos los que determinan el grado de poder del Estado. Los problemas ahora abarcarán, no sólo las cuestiones militares sino que se deben considerar competencias económicas, energéticas, de desarrollo de capacidades de alta tecnología y de comunicaciones y la habilidad de desarrollar influencia política y cultural más allá de sus fronteras.

Todos los usuarios, desde individuos a corporaciones o instituciones y organismos públicos deben mantener la seguridad en el ciberespacio. Dado que no es posible evitar todos los ataques, el Estado debe contar con una planificación, una estrategia para detectar y actuar ante ataques en lo posible mientras se encuentren en progreso, y además tener la capacidad de recuperarse e incluso hasta responder.

La condición multidimensional de la seguridad incluye a las problemáticas que afectan el ciberespacio. No son amenazas que afectan exclusivamente al Estado y a sus propios ciudadanos. El escenario internacional podría ver afectada la seguridad ya que hasta un ámbito de cooperación internacional "tiene a su vez una dimensión político-militar en la organización del tablero de ajedrez internacional" (Nye, 2005).

La tendencia y el convencimiento a nivel mundial es que para hacer frente a una posible situación de ciberguerra los esfuerzos deben ser centralizados y coordinados al mayor nivel posible.

No obstante, estas medidas no son de entera aplicación para enfrentar amenazas que traspasan y desbordan los espacios territoriales. La naturaleza de los conflictos y las amenazas son diferentes. Como puede observarse, el concepto de seguridad hemisférica plasmado en la Declaración sobre Seguridad en las Américas, en ocasión de realizarse la Conferencia Especial sobre Seguridad de la OEA, en México en octubre de 2003, hace más amplio el concepto tradicional de seguridad. Responde a la Declaración de Bridgetown de junio de 2002 que le reconoció naturaleza diversa y alcance multidimensional a las amenazas y otros desafíos a la seguridad en el hemisferio, resaltando además que el enfoque debe ampliarse para abarcar aquellas que no provienen sólo de conflictos armados.

Así, tuvimos una Seguridad Colectiva, propiciada y utilizada desde época de la Sociedad de las Naciones, que básicamente se apoya en la noción de todos contra uno, por la que los estados estarían dispuestos a formarse en coalición para enfrentar aquel que se convierta en agresor. Tras la caída del régimen comunista, se ha pasado a la Seguridad Cooperativa, cuyo objetivo es conformar comunidades de seguridad de carácter voluntario de los Estados, donde prevalezca una expectativa de confianza. El rasgo más exponente lo constituye el fomento de medidas de confianza mutua, con transparencia y fijando metas por consenso. Los conflictos fronterizos son probablemente los mejores ejemplos de litigios desactivados bajo este marco.

La cooperación regional en materia de ciberseguridad busca facilitar el intercambio de información para poder abordarlos de manera más eficaz y para mantener canales directos con otros equipos de respuesta ante incidentes en el país y la región. En este sentido, ya en su Informe General de 2007, la agencia europea ENISA había alertado que era necesario unir los esfuerzos para evitar un *"eventual 11S digital".*

El problema puede presentarse en el Hemisferio Occidental, donde no hay una estrategia consolidada, ya que a pesar de privilegiar la cooperación y el consenso en materia de defensa, no se han implementado mediadas de naturaleza común porque las distintas iniciativas no han podido consolidarse completamente. Como dice el profesor Pablo Celi (2014):

> El escenario en Sudamérica muestra una evidente debilidad de integración e identidad, presentando un campo de asimetrías significativas y estructuras heterogéneas en cuanto a la administración de sus sociedades. Las diferentes perspectivas y puntos de vista de algunos gobiernos limitan excesivamente, la posibilidad de integrar todos los estados en un esquema de seguridad colectiva común, lo que permitiría optimizar costes en este campo.

La retórica de la seguridad colectiva plasmada en la OEA, ha quedado en nada más que gestos, deteriorando este concepto, al mismo tiempo que se profundiza la deslegitimación de la OEA. Esto ha llevado a la conclusión de que el sistema ha fracasado como esquema de seguridad hemisférica. Los países latinoamericanos buscando otras formas de protección, desembocan en organizaciones subregionales como la Unasur, su CDS con las medidas de confianza mutua o en la declaración de "Zona de Paz", concepto éste que surgiera del propio seno de la ONU en junio de 1978.

La Unasur representa un instrumento de integración importante, que responde a una visión del multilateralismo en concordancia con la ONU, y plantea la cooperación entre los Estados en diferentes dimensiones, como infraestructura, finanzas, políticas sociales, energía y defensa.

La defensa es uno de los pilares de UNASUR, porque la región cuenta con valiosos recursos naturales (Amazonas, petróleo, gas, carbón, cuencas hídricas de agua dulce, grandes extensiones de pesca, entre otros), considerando que sus respectivas seguridades no podían ser tomadas separadas y aisladas unas de otras.

Considerado como un avance tras el estancamiento dentro del ámbito de la OEA y tratando de no producir duplicidad de funciones con esta institución hemisférica, el objetivo consiste en fortalecer y modernizar las instituciones existentes antes que crear nuevas instancias o estructuras para la defensa colectiva. Como consecuencia, el Consejo de Defensa Suramericano (CDS) fue concebido en diciembre de 2008 bajo el principio de preservar a Suramérica como una zona de paz, como un mecanismo de diálogo político y cooperación en materia de defensa en el que participan todos los Ministerios de Defensa. Es un foro político de diálogo definido desde sus inicios como un órgano de consulta, cooperación y coordinación en materia de la defensa regional.

Por ser un consejo de defensa no trata asuntos de seguridad. En todo caso aboga por un sistema de seguridad cooperativa dejando de lado los mecanismos de seguridad colectiva. Se creó para asegurar las condiciones de estabilidad que permitan funcionar los mecanismos diplomáticos. Sus decisiones, por la vía del consenso positivo de los estados

miembros, no son vinculantes sino que solamente tienen carácter declarativo. No es una alianza sino la intención de establecer políticas de defensa comunes, un entrenamiento común y una base industrial de defensa común; no contempla compromisos que obliguen a sus miembros a modificar normas, estrategias o políticas, sino que su base es la cooperación.

Sin embargo, ha tomado iniciativas para la adopción de estrategias defensivas para evitar ataques contra objetivos vitales en el ciberespacio. El CDS, en pos de alcanzar políticas y estrategias en común, tiene el foro regional para el intercambio de información, experiencias y procedimientos de solución y una red de contactos de autoridades competentes, para la toma de decisiones en lo que atañe a la ciberdefensa.

CAPÍTULO III
El enfoque argentino

Sección 1
Principales diferencias

La tendencia mundial de otros actores es considerar el tratamiento de la Ciberseguridad a través de esfuerzos centralizados y coordinados al mayor nivel posible, centralizándolo lo más cerca posible del jefe de estado. En la República Argentina se ha optado por una dispersión de organismos mayoritariamente al nivel de subsecretaría, dirección nacional o coordinaciones, dentro de varios ministerios. Se han creado diversos estamentos con alguna porción de responsabilidad, que representa una amplia disgregación.

El primer aspecto a resaltar es que a través de distintas normas se ha delimitado una clara diferenciación entre los conceptos de "Seguridad" y "Defensa", (llegando al punto de dejar de lado definiciones de organismos a los que se ha adherido, tales como las ONU o la OEA), aunque se reconoce que en su sentido literal deben ser comprensivos uno del otro y que la Seguridad implica e incluye la Defensa. Con base en los postulados del Preámbulo de la Constitución Nacional que señalan las políticas de defensa y seguridad, contra los enemigos externos e internos respectivamente, ambos conceptos se encuentran explicitados en las frases "*consolidar la paz interior*" y "*proveer a la defensa común*".

Por un lado el concepto "Seguridad" tiene exclusiva relación con la seguridad interna, en tanto que "Defensa" con la seguridad del Estado, en el sentido que se encara desde varios organismos internacionales. Se tiene así a la Seguridad Interior separada de la Defensa Nacional, cuando *Seguridad* es un concepto amplio y abarcador, que implica mantener la paz interior al mismo tiempo que disuadir o defenderse de agresiones externas.

La defensa nacional es parte de la seguridad nacional en el sistema de protección de los intereses nacionales. La defensa nacional es un medio, no el único, que contribuye al logro de la seguridad nacional. (Echeverría Jesús, 2015). En palabras de José Manuel Ugarte (2001):

> En Latinoamérica, al amparo del concepto de *seguridad nacional,* la defensa nacional y la seguridad interior tendieron y tienden a confundirse y a expandirse hasta incluir virtualmente la totalidad de la política de los respectivos países.
>
> Por otra parte, la *defensa nacional* es definida sobre la base del concepto de *seguridad nacional,* como el conjunto de medidas tendientes a su logro. De ese modo, la *defensa nacional* participa de la amplitud de este último concepto.

Una profundización de las diferencias en el uso de ambos conceptos puede hallarse en el trabajo publicado por el General de División (R) Evergisto de Vergara, profesor de la Escuela Superior de Guerra Conjunta, quien resalta que "estos dos

términos son aplicados, invocados, manipulados, acomodados a las ideologías, retorcidos o a veces hasta ignorados según las conveniencias e intereses abiertos o encubiertos."

Resume en casi una sola línea la principal diferencia que debe tenerse en cuenta: "Mientras la seguridad es una condición, la defensa es una acción propia del componente armado del poder nacional." Desde la óptica del estadista nos advierte que "colocar la seguridad y defensa de un Estado como si fuera compartimentos estancos, genera sistemas caros, ineficientes y obsoletos cuando se los trata de implementar – operacionalizar en la jerga - también como si fueran compartimentos estancos." (De Vergara, 2009).

En 2005, en un documento[10] del Observatorio de Políticas Públicas de la Coordinación General del Cuerpo de Administradores Gubernamentales de la Jefatura de Gabinete de Ministros, se reconoció que se ha llegado a esta separación de los conceptos como consecuencia de la mala reputación de la frase "*Doctrina de la Seguridad Nacional*". Esta doctrina implicaba incorporar como problema de la defensa nacional y por ende de intervención militar, todo problema de seguridad.

> Basado en la experiencia de la aplicación de la llamada "Doctrina de la Seguridad Nacional" se ha preferido delimitar el concepto "seguridad" a la seguridad de la población, o interna y "defensa" a la seguridad del estado con respecto al orden internacional. (OPP CAG, 2005).

No obstante, el propio Observatorio aclara que en la participación en los diversos foros mundiales, como las Cumbres de las Américas, Cumbre Extraordinaria y Conferencias sobre Seguridad, se utiliza el término en su sentido técnicamente aplicado por los especialistas.

El Poder Legislativo ha elaborado sendas leyes, la Ley 23.554 de Defensa Nacional y la Ley 24.059 de Seguridad Interior, ambas a través de arduos procesos para lograr un resultado consensuado, teniendo en cuenta el contexto que se vivía al momento de su creación. La distinción entre defensa y seguridad queda plasmada en el Artículo 2º de la Ley 23.554 de Defensa Nacional de 1988, al definir a la defensa 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.

El Artículo 4° recalca que "se deberá tener permanentemente en cuenta la diferencia fundamental que separa a la defensa nacional de la seguridad interior". Según el Observatorio de Políticas Públicas esta ley estableció:

[10] Este documento fue producido por los responsables del Área Temática "Defensa y Seguridad Internacional" del Observatorio de Políticas Públicas.

> Los lineamientos generales que apuntaban a garantizar el ejercicio de la autoridad civil, la no intervención de las Fuerzas Armadas en asuntos políticos internos, la regulación desde una perspectiva restrictiva de la participación militar en seguridad interior; y el apuntalamiento de una organización militar de base conjunta. (OPP CAG, 2010).

Los legisladores crearon la Ley 23.554 en abril de 1988, que establece que la defensa nacional debe "enfrentar las agresiones de origen externo", sin poner característica limitante al agresor, sino que las engloba a todas. Pero la Reglamentación de esa ley, que llegó 18 años después a través del Decreto N° 727/06, va más allá, modifica la letra de la ley auto-limitándose, al circunscribir el empleo del instrumento militar de la defensa nacional (es decir, las Fuerzas Armadas) a las "agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro/s Estado/s". Excluye así la posibilidad de accionar contra otras agresiones externas, al identificar una única y exclusiva categoría de origen. En la decisión política se plasma una ideología negativa hacia cualquier intento que pretenda extender la utilización de las Fuerzas Armadas contra las llamadas "nuevas amenazas".

En enero de 1992 fue publicada la Ley 24.059 de Seguridad Interior que regula el empleo de los elementos humanos y materiales de todas las fuerzas policiales y de seguridad, excluyendo taxativamente el empleo de las Fuerzas Armadas. Al mismo tiempo fija los casos puntuales donde éstas podrán participar como apoyo logístico y aquellos casos en que podrán emplearse elementos de combate para el restablecimiento de la seguridad interior, cuando las fuerzas policiales se vieran sobrepasadas y con previa declaración del "estado de sitio".

Si bien reitera la prohibición impuesta por la Ley 23.554 de Defensa Nacional en cuanto al uso de lo militar para seguridad interior, especifica las condiciones para permitir la participación de las FF.AA. en funciones de seguridad interna. Define en su artículo 2, a la seguridad interior como:

> La situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional.

Sección 2
ICIC-CERT

Así, en consonancia con el criterio descripto en la sección anterior, se ha diferenciado la Ciberdefensa de la Ciberseguridad con el simple aditamento del prefijo *ciber* a los términos defensa y seguridad. No se toma a la Ciberseguridad como un todo al que la Ciberdefensa pertenece como una parte. Se adaptan conceptos para acotar los términos a la ideología.

Aun reconociendo que los países más avanzados del mundo han creado grupos de especialistas al máximo nivel, conocidos mundialmente como CERT (en español: "Equipo de Respuesta ante Emergencias en Computadoras"), se creó en 1999 un Equipo de Respuesta para incidentes en las redes, como una *Coordinación* en el ámbito de la SUBSECRETARIA DE TECNOLOGÍAS INFORMÁTICAS de la por entonces SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS (JGM). Se hizo mediante la Resolución Nº 81/99 que creó la ArCERT (acrónimo de "*Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Argentina*"), a través de la Oficina Nacional de Tecnologías de Información (ONTI), que se ocupa del uso eficiente de los recursos digitales. Como puede verse se utiliza casi el mismo acrónimo pero adaptado.

Con este servicio para dar respuesta frente a eventos de seguridad, Argentina fue considerada uno de los primeros países de América Latina en operar un CERT nacional. Por ser un CERT nacional trataba los incidentes de seguridad sufridos por los organismos de la Administración Pública Nacional, pero sin tener responsabilidad directa sobre la administración de las redes. Esto es así porque cada organismo administra sus propias redes y es responsable de la seguridad. Corresponde a las autoridades responsables de cada organismo efectuar las denuncias y eventualmente iniciar los procesos de investigación.

La respuesta era eminentemente técnica y no contemplaba la investigación del origen de los ataques ni sus responsables. Básicamente sus principales funciones era centralizar los reportes sobre incidentes y facilitar el intercambio de información para afrontarlos, aunque lo hacía con un horario limitado de 09:00 a 17:00 horas.

La Decisión Administrativa del JGM Nº 669 de 2004 estableció que debía dictarse una "Política de Seguridad de la información Modelo", como base para la elaboración de las respectivas políticas a dictarse por cada organismo y precisó, entre otras cuestiones, las funciones del Comité de Seguridad de la Información y del Coordinador del Comité de Seguridad de la Información. Este "modelo" fue implementado por la ONTI, y ha sido actualizado en varias oportunidades, siendo la última mediante la Disposición ONTI N° 1 del 19 de febrero de 2015.

En cuanto a la ONTI, posee distintas responsabilidades primarias en relación con la elaboración de estándares de tecnologías, prestar asistencia técnica a los organismos de toda la administración pública y debe intervenir dando opinión técnica previa en los proyectos de innovación tecnológica. Debe "*promover la estandarización tecnológica en materia informática, teleinformática o telemática, telecomunicaciones, ofimática o burótica*" y tampoco actúa en el trabajo de protección propiamente dicho.

Se aboca a la seguridad de la información, que se entiende como la preservación de las siguientes características:

- Confidencialidad: que garantiza el acceso a la información sólo por parte de aquellas personas autorizadas a tener acceso a la misma.

- Integridad: debe salvaguardar la exactitud y la totalidad de la información y los métodos de procesamiento.

- Disponibilidad: en todo momento los usuarios autorizados deben poder acceder a la información y a los recursos relacionados.

Como esta dedicación a la protección de la información dejaba de lado a las estructuras, en julio de 2011 se creó el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC), mediante la Resolución 580 en el ámbito de la ONTI y que derogó a la Resolución 81/99. Tiene como objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas para la adopción de un programa regulatorio.

Con posterioridad a que el día 7 de Marzo del año 2012 la Argentina suscribiera la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" del Comité Interamericano contra el Terrorismo (CICTE) de la OEA, la cual exhortaba a los Estados Miembros a que continúen con sus esfuerzos para crear o fortalecer a sus equipos nacionales contra incidentes cibernéticos, conocidos como Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), dentro del marco del Programa Nacional ICIC, a través de la Disposición 2 de agosto 2013, la ONTI creó cuatro Grupos de Trabajo:

1) Grupo de trabajo ICIC-CERT: (nombrado taxativamente como "Computer Emergency Response Team"). Administra la información sobre reportes de incidentes de seguridad y colabora a encausar posibles soluciones y brinda asesoramiento técnico. Promueve la coordinación entre las unidades de administración de redes informáticas del sector público nacional que hubieren adherido al Programa, para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad.
2) Grupo de trabajo ICIC-GAP: (Grupo de Acción Preventiva). Es responsable de monitorear los sistemas y servicios informáticos expuestos en las redes y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad.
3) Grupo de trabajo ICIC-GICI: (Grupo de Infraestructuras Críticas de Información). Sus objetivos son elaborar y proponer normas y políticas de resguardo de la seguridad digital con actualización constante, y coordinar la implementación de ejercicios de respuesta. Define a estas infraestructuras como instalaciones, redes, servicios y equipos físicos y de TI, cuyo funcionamiento es indispensable para brindar servicios a los ciudadanos y a las instituciones.
4) Grupo de trabajo ICIC-INTERNET SANO: Promueve a formar conciencia de los riesgos respecto al uso de medios digitales.

Como puede verse, desde su creación, el Programa Nacional ICIC solamente impulsa la adopción del marco regulatorio, pero no participa en la trabajo de protección

de las infraestructuras estratégicas y críticas, las cuales debieran ubicarse dentro del ámbito de la Ciberdefensa.

El Decreto 1067 del 10 de junio de 2015, creó la SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD en el ámbito de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS.

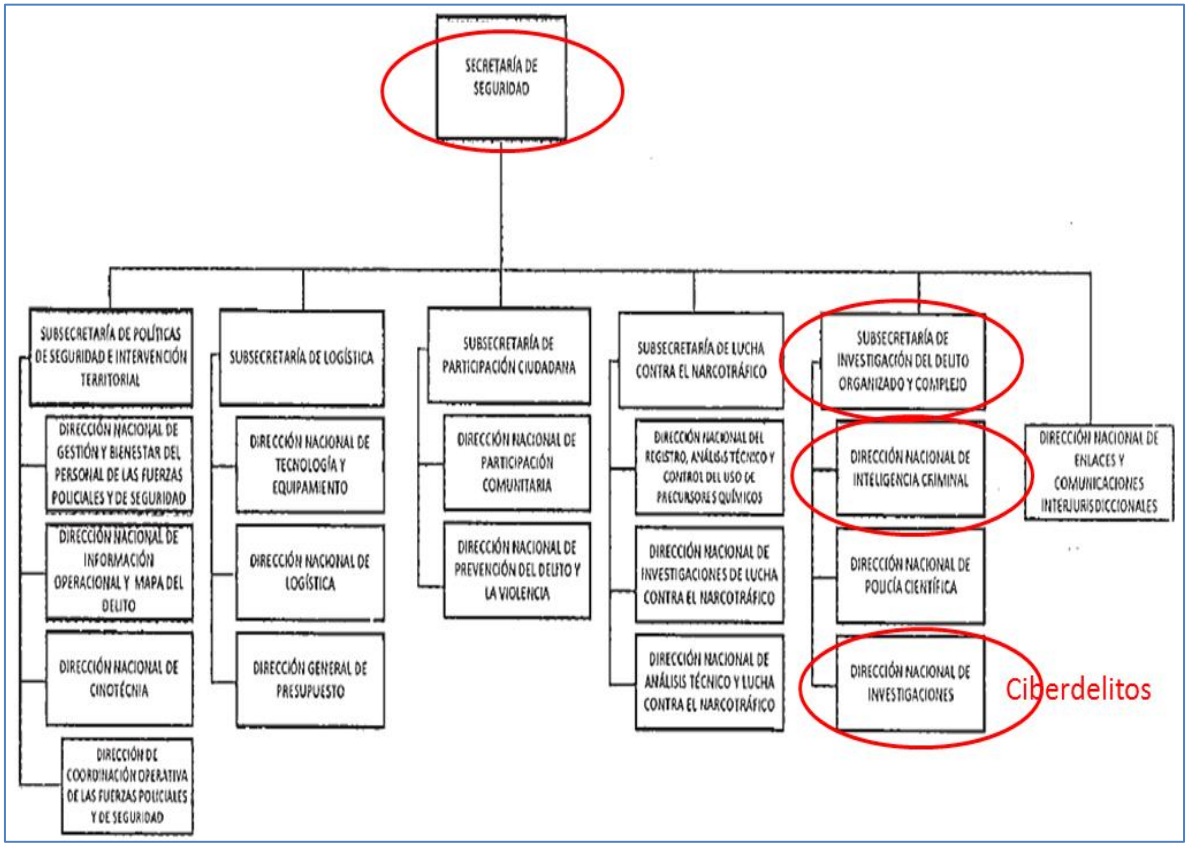
Esta subsecretaría debía entender en la elaboración la estrategia nacional de protección de infraestructuras críticas de información y ciberseguridad y entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT Nacional). Para ello se transfirió el "Programa Nacional ICIC", a la órbita de la DIRECCION NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD dependiente de la subsecretaría recién creada.

Sección 3
Ministerio de Seguridad

La seguridad interior era responsabilidad de la Secretaría de Seguridad Interior que formaba parte del Ministerio del Interior hasta febrero de 2002, cuando mediante el Decreto 357, la mencionada Secretaría fue transferida al ámbito de la Presidencia de la Nación. Más tarde, a través del Decreto 1210 de 10 de julio de 2002, por modificación de la Ley de Ministerios se transfirió, una vez más la Secretaría de Seguridad Interior de la Presidencia de la Nación a la órbita del Ministerio de Justicia, Seguridad y Derechos Humanos, según la nueva denominación que recibió.

Por Decreto 1993 del 14 de diciembre de 2010, como escisión del Ministerio de Justicia y Derechos Humanos se creó el Ministerio de Seguridad. El día 15, el inmediato siguiente, con el Decreto 2009, se transfirieron las competencias, funciones y unidades organizativas provenientes de la ex Secretaria de Seguridad Interior. Es en el ámbito del Ministerio de Seguridad, donde debiera entonces encontrarse el organismo encargado de ejecutar las actividades de Ciberseguridad.

La Decisión Administrativa 421 del 05 de mayo de 2016 aprobó la estructura organizativa de primer nivel operativo del MINISTERIO DE SEGURIDAD, el que quedó configurado con (entre otras) una SECRETARÍA DE SEGURIDAD y su dependiente SUBSECRETARÍA DE INVESTIGACION DEL DELITO ORGANIZADO Y COMPLEJO, tal como muestra la siguiente figura:



Fuente: "Anexo Ic" de la Decisión Administrativa 421/2016

Dentro de la subsecretaría mencionada se encuentra la Dirección Nacional de Inteligencia Criminal que debe ocuparse de planificar y ejecutar las actividades de obtención y análisis de la información para la producción de la inteligencia nacional en

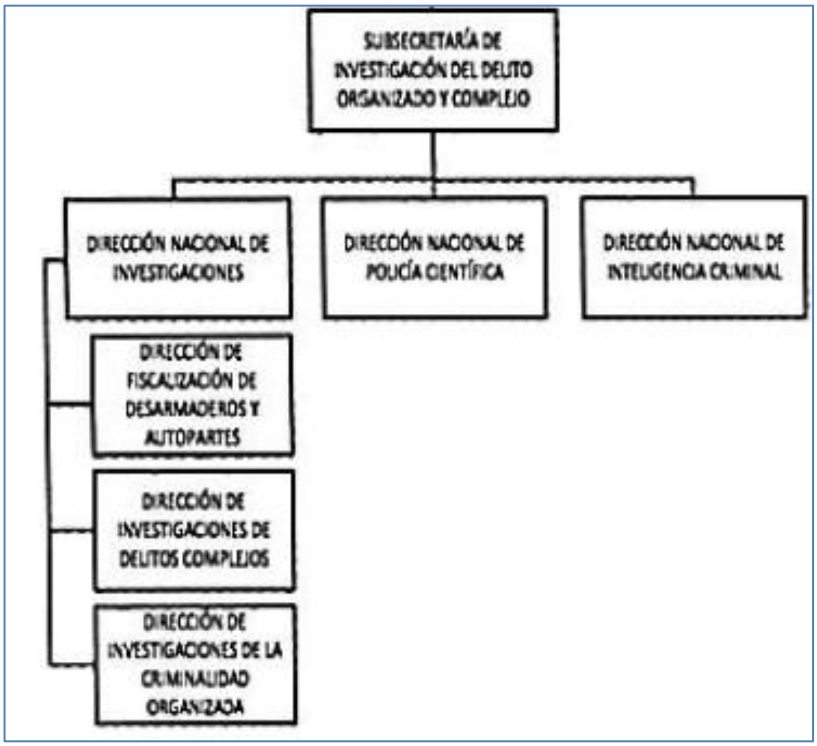
materia criminal, así como también las relaciones con los organismos de inteligencia del Estado Nacional y Elaborar el informe anual de actividades de inteligencia criminal a los efectos de su elevación a la Agencia Federal de Inteligencia (AFI).

Por su parte, dentro de la misma subsecretaría, la Dirección Nacional de Investigaciones tiene la responsabilidad primaria de colaborar en las investigaciones de los ciberdelitos, pero es la Dirección Nacional de Policía Científica la que puede efectuar las pericias informáticas y los estudios técnicos y científicos conducentes a descubrir todas las circunstancias del delito.

La Resolución Ministerial 225 del 01 de junio de 2016 aprobó la estructura inferior al primer nivel operativo de la UNIDAD MINISTRO y de las Secretarías de este ministerio. Aquí aparecen, subordinadas a la DIRECCIÓN NACIONAL DE INVESTIGACIONES dos Direcciones.

1) La DIRECCIÓN DE INVESTIGACIONES DE DELITOS COMPLEJOS, que tiene que ocuparse, entre otros, de entender principalmente en la investigación de delitos informáticos.

2) La DIRECCIÓN DE INVESTIGACIONES DE LA CRIMINALIDAD ORGANIZADA, que debe asistir al Director Nacional en las acciones de interacción con otros organismos en materia de ciberdelitos (entre otros).



Fuente: Anexo 1 Ic (Parcial) de la Resolución Ministerial 225/2016

Sección 4
Ministerio de Modernización

Cuando se produjo el traspaso de gobierno a fines de 2015, con el Decreto 151 del 17 de diciembre de 2015, se reordenaron las responsabilidades y las competencias asignadas a la JGM. Este decreto transfirió la entonces SECRETARÍA DE GABINETE (y varias de sus unidades organizativas dependientes) a la órbita de la nueva SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD en el ámbito del MINISTERIO DE MODERNIZACIÓN.

A este ministerio, también creado recientemente, le compete entender en el perfeccionamiento de la organización y funcionamiento de la Administración Pública Nacional Central y Descentralizada, procurando optimizar y coordinar los recursos técnicos con que cuenta, como así también intervenir en la definición de estrategias y estándares sobre tecnología de la información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de la información, y en el desarrollo de sistemas tecnológicos con alcance transversal o comunes a los organismos y entes de la Administración Pública Nacional, Centralizada y Descentralizada.

Tiene como objetivo impulsar las formas de gestión que requiere un Estado moderno, el desarrollo de tecnologías aplicadas a la administración pública central y descentralizada, que acerquen al ciudadano a la gestión del Gobierno Nacional, así como la implementación de proyectos que permitan asistir a los gobiernos provinciales y municipales que lo requieran.

De lo expuesto resulta que esta subsecretaría pasa a ser la sucesora de la ex SECRETARÍA DE LA FUNCIÓN PÚBLICA y dirige y supervisa el accionar de la ONTI. El Decreto 13 del 05 de enero de 2016 ordena las responsabilidades de la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD, entre las que se encuentran:

- Entender en la elaboración de la estrategia nacional de Infraestructura tecnológica, la protección de infraestructuras críticas de información y ciberseguridad, en el ámbito del Sector Público Nacional.
- Entender en la administración, supervisión y operación de los sistemas informáticos del Sector Público Nacional, garantizando la disponibilidad y confiabilidad de los mismos.
- Asistir al Ministro en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del Sector Público Nacional, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los mencionados sectores.
- Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL).
- Dirigir y supervisar el accionar de la ONTI.

En marzo de 2016, mediante la Decisión Administrativa 232/2016 aprobó la estructura organizativa de la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD, a la que se le asigna entre otros, el objetivo de "*Dirigir y supervisar el accionar de la ONTI.*"

Por su parte, ahora a la ONTI se le impone la responsabilidad primaria de "Intervenir en la formulación de políticas e implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado, promoviendo la integración de nuevas tecnologías, su compatibilidad e interoperabilidad de acuerdo con los objetivos y estrategias definidas en el Plan de Modernización del Estado."

Entre las acciones a llevar a cabo, debe "Intervenir y supervisar en los aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica del Sector Público Nacional."

En el caso de la DIRECCIÓN NACIONAL DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD, su responsabilidad primaria es "Asistir en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional".

Para lo cual debe:

- Establecer prioridades y planes estratégicos de abordaje de la ciberseguridad.
- Monitorear los servicios que el Sector Público Nacional brinda a través de la red de internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad.
- Alertar en casos de intentos de vulneración de infraestructuras críticas así como de las vulnerabilidades encontradas.
- Entender en la planificación e implementación de ejercicios de respuesta ante incidentes cibernéticos del Sector Público Nacional.
- Coordinar acciones entre las unidades de administración de redes informáticas del Sector Público Nacional, para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad.
- Coordinar las acciones del equipo de respuesta a emergencias informáticas a nivel nacional, administrando toda la información sobre reportes de incidentes de seguridad en el Sector Público Nacional y encauzar sus posibles soluciones de forma organizada y unificada.
- Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa, estándares y buenas prácticas.

A su vez, el Decreto 898 del 27 de julio de 2016 le establece a la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD los objetivos a cumplir:

1. Entender en la elaboración de la estrategia nacional de Infraestructura tecnológica, la protección de infraestructuras críticas de información y ciberseguridad, en el ámbito del Sector Público Nacional.

2. Supervisar el correcto funcionamiento de los servicios de infraestructura de los centros de datos.

3. Dirigir y operar centros de datos y cómputos, a efectos de brindar servicios centrales de infraestructura a otras jurisdicciones, optimizando el uso de los recursos, mejorando la seguridad y aumentando los niveles de calidad en la prestación del servicio.

4. Entender en la administración, supervisión y operación de los sistemas informáticos del Sector Público Nacional, garantizando la disponibilidad y confiabilidad de los mismos.

5. Dirigir, coordinar y organizar la asistencia a los usuarios de tecnología del Sector Público Nacional, en la solución de problemas relacionados con la utilización de los diversos sistemas en el ámbito de su competencia.

6. Entender en materia de dictado de normas, políticas, estándares y procedimientos de Tecnología y Seguridad Informática en el ámbito de su competencia.

7. Asistir al Ministro en la formulación de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras críticas del Sector Público Nacional, y a las organizaciones civiles, del sector privado y del ámbito académico que así lo requieran, fomentando la cooperación y colaboración de los mencionados sectores.

8. Entender en las acciones de supervisión, monitoreo, análisis y detección de los activos críticos de información, en el ámbito de su competencia.

9. Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL).

10. Difundir las mejores prácticas y elaborar políticas de capacitación para el Sector Público Nacional y contribuir a la capacitación de las organizaciones civiles, del sector privado y del ámbito académico en temas de seguridad de la información y protección de información crítica, que así lo requieran.

11. Desarrollar programas de asistencia a los organismos del Sector Público Nacional y a las provincias y municipios que así lo requieran en el ámbito de su competencia y en coordinación con los organismos competentes.

12. Dirigir y supervisar el accionar de la OFICINA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN (ONTI).

13. Entender en todos los aspectos relativos al desarrollo y mantenimiento de telecomunicaciones y redes en el ámbito del Sector Público Nacional incluyendo el diseño, desarrollo y mantenimiento de los sistemas de telecomunicaciones y redes asociadas.

14. Diseñar y proponer las estrategias, la arquitectura y la planificación para el desarrollo, modernización, optimización y el mantenimiento respectivo de las redes de telecomunicaciones del Sector Público Nacional y sus servicios asociados que procuren el acceso e inclusión a los servicios digitales, logrando una gestión centralizada de los mismos.

15. Participar en grupos de trabajo multisectoriales, comisiones y organismos nacionales e internacionales interviniendo en acuerdos, convenios y tratados internacionales que incluyan aspectos relacionados con redes y telecomunicaciones en el Sector Público Nacional.

16. Intervenir en la elaboración y supervisión de planes y procedimientos de contingencia y de desastre en el ámbito de su competencia, conforme los criterios establecidos.

17. Brindar asistencia y asesoramiento a todas las áreas del Sector Público Nacional en aspectos vinculados con telecomunicaciones y redes públicas.

La Resolución del Ministro de Modernización 490 del 16 de noviembre de 2016 aprobó la estructura organizativa de segundo nivel operativo de la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD. Como resultante, se le ha subordinado la DIRECCIÓN DE OPERACIONES TÉCNICAS DE CIBERSEGURIDAD, que a su vez, tiene subordinadas a dos COORDINACIONES.

Esta Dirección es la encargada de llevar adelante, entre otras, las acciones de:

- Analizar los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como infraestructura crítica para la prevención de posibles fallas de seguridad.

- Proponer y coordinar el accionar del equipo de respuestas a emergencias informáticas nacional (CERT NACIONAL).

- Coordinar y supervisar las acciones de los equipos de respuestas a emergencias informáticas (CERT) y de los equipos de respuestas a incidentes de seguridad informática (CSIRT) a nivel nacional, administrando toda la información sobre reportes de incidentes de seguridad y encausando sus posibles soluciones de forma organizada y unificada.

Como ya se ha dicho, a la DIRECCIÓN DE OPERACIONES TÉCNICAS DE CIBERSEGURIDAD le dependen dos *COORDINACIONES:*

a) COORDINACIÓN DE OPERACIONES DE CIBERSEGURIDAD

Entre otras acciones, debe "Asesorar técnicamente ante incidentes de ciberseguridad en sistemas informáticos de los organismos del Sector Público Nacional para la prevención de posibles fallas".

Además se encarga de "Promover la coordinación entre las unidades de administración de redes informáticas del Sector Público Nacional para la prevención, detección, manejo y recopilación de información sobre incidentes de ciberseguridad".

b) COORDINACIÓN DE PROYECTOS E INVESTIGACIÓN DE CIBERSEGURIDAD

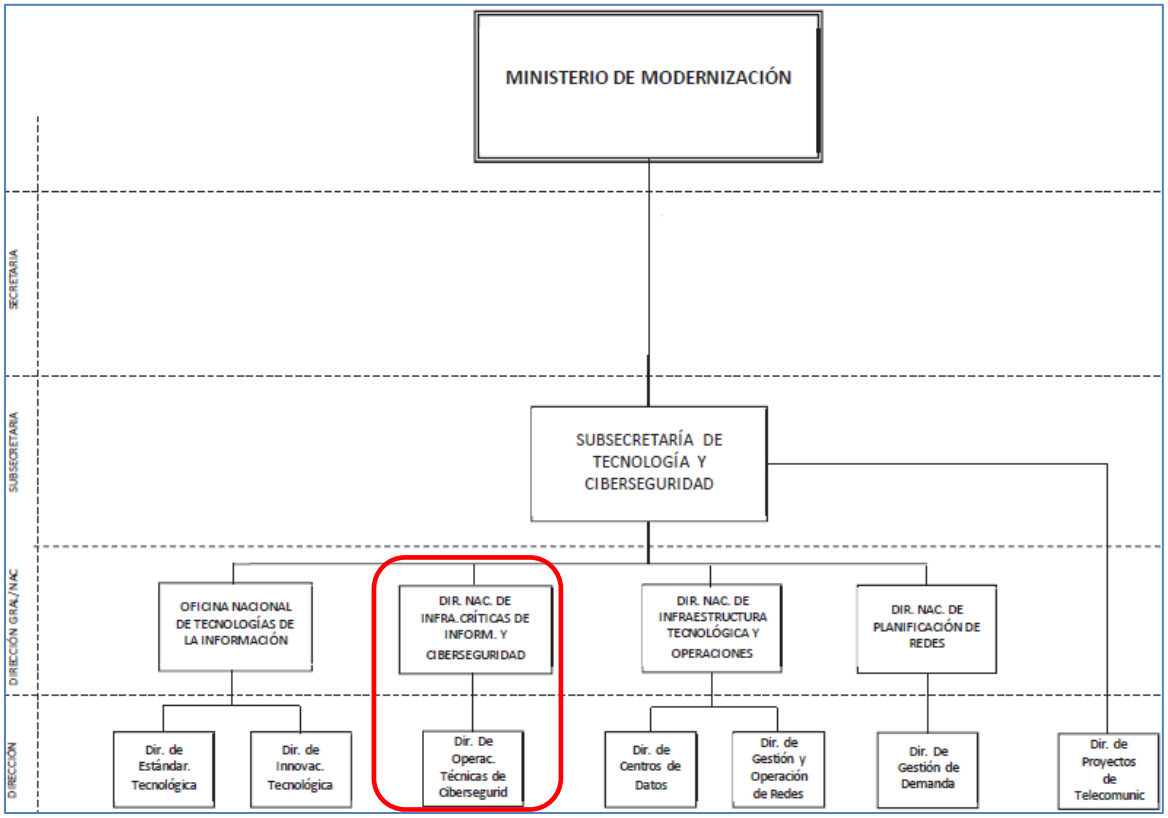
Entre otras acciones, debe "Desarrollar e integrar las plataformas de análisis de vulnerabilidades, de gestión, y de servicios de ciberseguridad y de infraestructuras críticas de información de la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD".

Proponer las acciones de supervisión, monitoreo, análisis y detección de los activos críticos de información de la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD.

Proponer, desarrollar e implementar la red de detección de amenazas cibernéticas.

Investigar sobre nuevas tecnologías y herramientas en materia de seguridad informática, así como de las relativas a nuevas amenazas cibernéticas

Nos encontramos con una nueva estructura que una vez más se encarga de "proponer y coordinar". Al momento la estructura organizativa de la SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD del MINISTERIO DE MODERNIZACIÓN es la que se muestra en la siguiente figura y como puede verse, le dependen la ONTI y tres Direcciones Nacionales.



Fuente: Anexo 1 de la Resolución 490/E/2016 del Ministerio de Modernización.

Por otra parte, en marzo de 2015 la Ley 27.126 modificó la Ley 25.520 de Inteligencia Nacional y creó la Agencia Federal de Inteligencia (AFI) como organismo superior del Sistema de Inteligencia Nacional y director del mismo.

Asimismo, disolvió la Secretaría de Inteligencia (ex SIDE). Por esta ley queda definida la Inteligencia Nacional como "la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación".[11]

La AFI queda instituida como el organismo rector superior del Sistema de Inteligencia Nacional y lo dirige, abarcando los organismos que lo integran. Será conducida por un Director General con rango de Ministro y un Subdirector General con rango de Secretario de Estado. Deberá cumplir las siguientes funciones:

> 1. 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.
>
> 2. 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.

En cuanto a su forma de trabajo y a la celeridad con que se puedan transmitir las informaciones para que lleguen a las autoridades que deben tomar decisiones, cabe destacar que el Artículo 15 bis establece textualmente que:

> Toda relación o actuación entre la Agencia Federal de Inteligencia, y funcionarios o empleados de cualquiera de los poderes públicos federales, provinciales o locales, vinculados a las actividades reguladas por la presente ley sólo podrán ser ejercidas por el Director General o el Subdirector General o por el funcionario a quien se autorice expresamente a realizar dicha actividad.
>
> El incumplimiento de este artículo conllevará la nulidad de lo actuado y hará pasible de responsabilidad disciplinaria, penal y civil a todos quienes incurrieran en dicho incumplimiento.[12]

[11] En el Boletín Oficial número 33.083 del 05 de marzo de 2015 aparecen las palabras "*Defensa Nacional"* con mayúsculas y "*seguridad interior"* con minúsculas.

[12] El Art 43 bis reprime este incumplimiento con prisión de seis (6) meses a tres (3) años e inhabilitación especial por doble tiempo.

El Decreto 1311 de fecha 06 de julio de 2015 estableció lo que taxativamente denomina “NUEVA DOCTRINA DE INTELIGENCIA NACIONAL” (NDIN). Entre sus considerandos indica que el nuevo concepto de inteligencia nacional deriva de una visión integral que la define como:

> La actividad institucional que se inscribe dentro del marco del Estado constitucional social y democrático de derecho y que apunta a dar cuenta de los desafíos, coacciones y conflictos que ponen en riesgo la defensa y la seguridad democráticas de nuestro pueblo.

También crea, en su artículo 8, la COMISIÓN PARA LA CREACIÓN DEL BANCO DE PROTECCIÓN DE DATOS Y ARCHIVOS DE INTELIGENCIA que la Ley N° 25.520 (modificada por la Ley N° 27.126), dispone para centralizar las bases de datos de los organismos del Sistema de Inteligencia Nacional en un único Banco de Datos. Este banco deberá observar la clasificación de seguridad que corresponda en interés de la seguridad interior, la defensa nacional y las relaciones exteriores de la Nación.

Esta Comisión la integran, entre otros, el titular de la Dirección Nacional de Inteligencia Criminal, dependiente del MINISTERIO DE SEGURIDAD y el titular de la Dirección Nacional de Inteligencia Estratégica Militar, dependiente del MINISTERIO DE DEFENSA.

Según esta NDIN, “el sistema de inteligencia nacional se configura como un «observatorio» abocado exclusivamente a la producción y gestión de conocimientos acerca del conjunto de problemáticas relevantes en materia de defensa nacional y de seguridad interior.”

Define esas problemáticas para ambos ámbitos. Para el caso de la defensa nacional reproduce los conceptos de la Reglamentación de la Ley de Defensa. Por su parte, para el ámbito de la seguridad interior enumera específicamente los fenómenos delictivos complejos de relevancia federal que abarca esa problemática, incluyendo:

> (...) las acciones que atenten contra la ciberseguridad, delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos, o parte de ellos, el uso fraudulento y la difusión ilegal de contenidos.

El Artículo 2 de la Ley 25.520 de Inteligencia Nacional, en los Incisos 3 y 4 que se transcriben, establece que:

> 3. [Se entenderá por] Inteligencia Criminal a la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional.
>
> 4. [Se entenderá por] Inteligencia Estratégica Militar a la parte de la Inteligencia referida al conocimiento de las capacidades y debilidades del

> potencial militar de los países que interesen desde el punto de vista de la defensa nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento estratégico militar.

Y por su parte el Decreto 1311, en el Capítulo II de la NDIN describe las *Actividades* que comprende la producción de la inteligencia nacional, dando las siguientes definiciones:

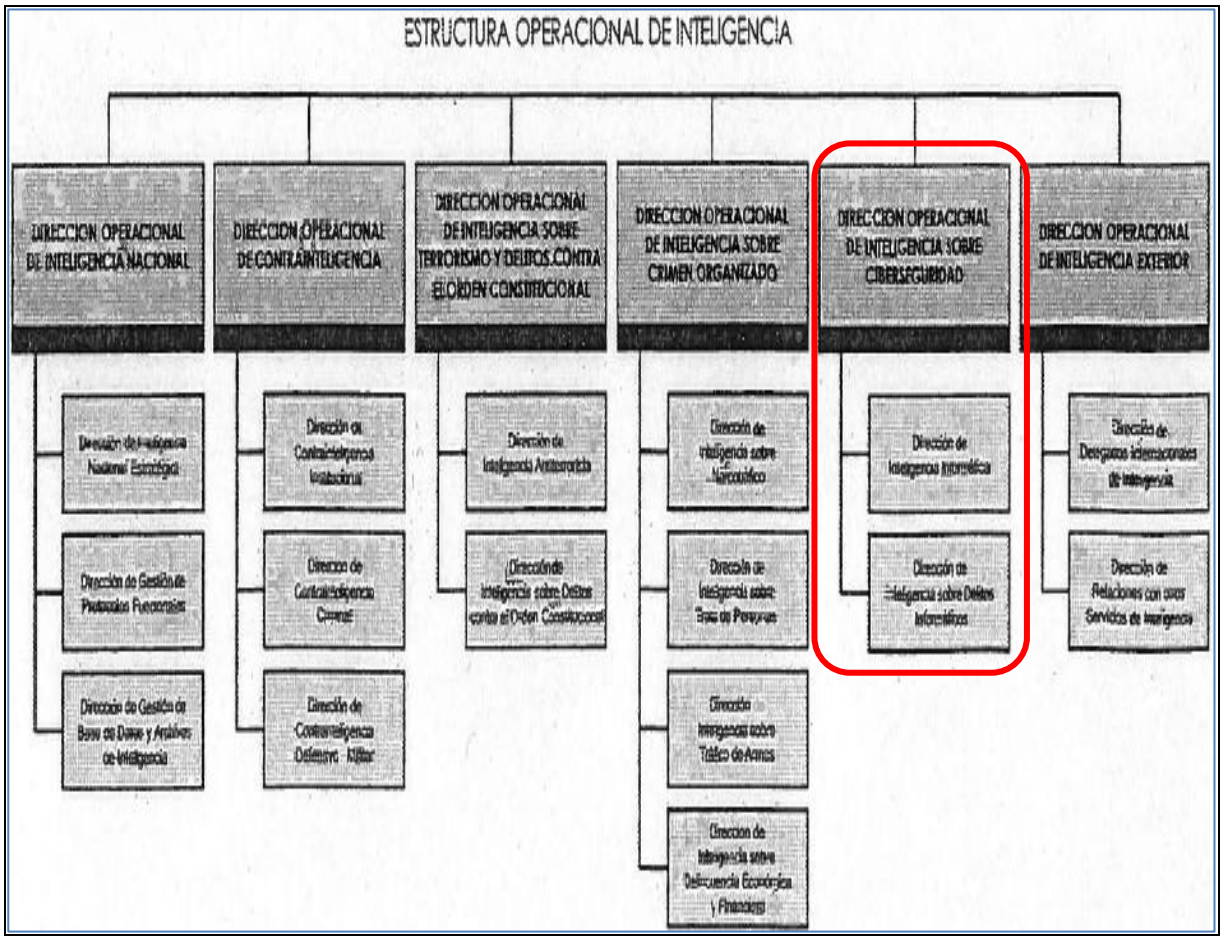
> La inteligencia criminal comprende la producción de inteligencia referida a las problemáticas delictivas y, en particular, a aquellas problemáticas delictivas complejas de relevancia federal relativas al terrorismo, los atentados contra el orden constitucional y la vida democrática, la criminalidad organizada y los atentados contra la ciberseguridad.
>
> La inteligencia estratégica militar comprende la producción de inteligencia referida a eventuales riesgos o conflictos generados por agresiones de origen externo perpetradas por Fuerzas Armadas pertenecientes a otros Estados, contra la soberanía la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas.

Según la NDIN la AFI producirá inteligencia estratégica con base en la información recolectada por la Dirección Nacional de Inteligencia Estratégica Militar (DINIEM) y la Dirección Nacional de Inteligencia Criminal (DINICRI). Ello se hará de acuerdo a "protocolos funcionales" que "son formulados por la AFI, en tanto organismo superior y rector del sistema de inteligencia nacional, para ser cumplidos por la DINIEM y, a través de ella, por los organismos de inteligencia de las Fuerzas Armadas, así como por la DINICRI y, a través de ella, por los organismos o áreas de inteligencia de las policías y fuerzas de seguridad federales".

LA AFI cuenta con una Estructura de Dirección y Administrativa por un lado y por el otro, con una Estructura Operacional que tiene a su cargo la producción de inteligencia nacional y que se compone de una Dirección General y seis Direcciones Operacionales.

Precisamente la ubicada en quinto lugar es la Dirección Operacional de Inteligencia sobre Ciberseguridad. Debe encargarse de "la producción de inteligencia orientada al conocimiento de las acciones que atenten contra la Ciberseguridad en el marco de la defensa nacional o la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevarlas a cabo."

Se le subordinan la Dirección de Inteligencia Informática, con relación al uso de las TIC y la Dirección de Inteligencia sobre Delitos Informáticos, en cualquiera de sus formas y modalidades.



Fuente: Organigrama parcial del Anexo III del Decreto 1311/2015

Sección 6
Ministerio de Defensa

En mayo de 2014, dependiendo orgánica, funcional y operacionalmente del Estado Mayor Conjunto de las Fuerzas Armadas, el Ministro de Defensa creó el Comando Conjunto de Ciberdefensa, con la misión de ser capaz de conjurar y repeler ciberataques contra las infraestructuras críticas de la información y los activos del SISTEMA DE DEFENSA NACIONAL y su INSTRUMENTO MILITAR dependiente.

El Decreto 42 del 07 de enero de 2016 aprobó el organigrama correspondiente al Ministerio de Defensa y también estableció los objetivos de las unidades organizativas. Entre estas se encuentra la SECRETARÍA DE CIENCIA, TECNOLOGÍA Y PRODUCCIÓN PARA LA DEFENSA, que, (en relación con este trabajo final), deberá:

- Entender en la coordinación y conducción 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 extra jurisdiccional.

A esta secretaría le depende la SUBSECRETARÍA DE CIBERDEFENSA, que el mismo decreto le impone el cumplimiento de las siguientes 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.

Posteriormente, la Decisión Administrativa 546 del JGM, de fecha 30 de mayo de 2016 dictó las Responsabilidades Primarias y Acciones a cumplir por parte de:

- DIRECCIÓN NACIONAL DE INTELIGENCIA ESTRATÉGICA MILITAR:

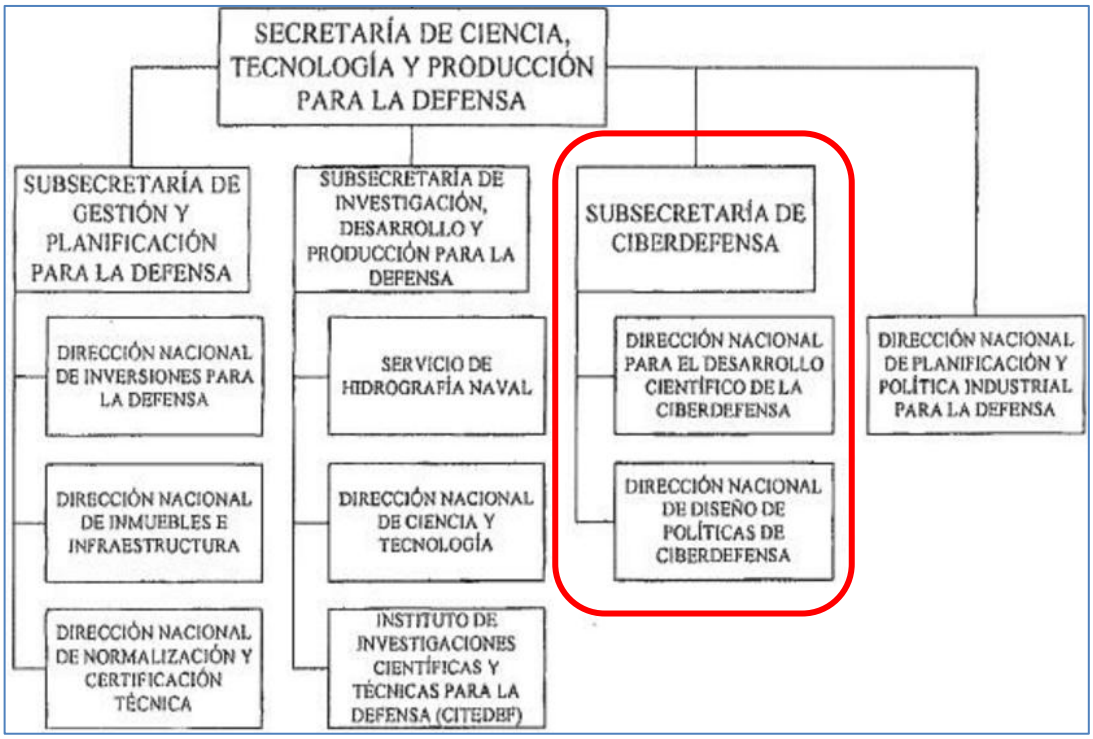
  Como integrante del Sistema Nacional de Inteligencia, requerir a la AFI la información e Inteligencia necesaria para contribuir en la producción de la Inteligencia Estratégica Militar.

- DIRECCIÓN NACIONAL PARA EL DESARROLLO CIENTÍFICO DE LA CIBERDEFENSA

  Coordinar los trabajos y proyectos, el diseño, implementación y control de las políticas, planes e iniciativas de Investigación y Desarrollo en temas de Ciberdefensa.

- DIRECCIÓN NACIONAL DE DISEÑO DE POLÍTICAS DE CIBERDEFENSA

  Asistir en el planeamiento, formulación, dirección, supervisión y evaluación de las políticas y estándares de Ciberdefensa para la jurisdicción del MINISTERIO DE DEFENSA coordinando las operaciones de ciberdefensa en los organismos antedichos.



Fuente: Anexo I D de la DA 546/2016

CONCLUSIONES

Es el Estado el que, sin ser el único, continúa como actor principal de las relaciones internacionales. En este escenario los gobiernos deben actuar con prudencia política, de manera de actuar estratégicamente en este mundo complejo, en sus relaciones con otros estados en el plano regional, al conformar bloques que permitan hacer un uso provechoso de la dispersión de los núcleos clásicos del poder.

El énfasis en distinguir los conceptos Defensa y Seguridad, porque a este último se lo relaciona con la desprestigiada "Doctrina de Seguridad Nacional" asociada a las dictaduras militares en América Latina, se basa en un problema conceptual que actúa como condicionante y que en la práctica ha servido solamente con fines académicos, resultando dilatoria y desgastante por su inaplicabilidad. Ha sido determinante para que la legislación nacional cuente con dos leyes para tener a la Seguridad Interior separada de la Defensa, cuando la seguridad es un concepto amplio y abarcador, que incluye mantener la paz interior al mismo tiempo que disuadir o defenderse de agresiones externas. La defensa es la contribución militar a la seguridad nacional y la seguridad del estado significa mucho más que emplear a las fuerzas militares.

Para soporte de su posición defensiva, Argentina se apoya en mecanismos de disuasión supranacionales en materia de defensa en el hemisferio. El concepto de "seguridad cooperativa" apunta a resaltar el carácter voluntario de los Estados a someterse a un proceso de cooperación a fin de prevenir conflictos intrarregionales, fijando objetivos por consenso y no la amenaza de la fuerza. Se basa en la confianza mutua y la transparencia.

Uno de los ingredientes esenciales para evaluar y enfrentar los riesgos que presenta el ciberespacio ha sido la cooperación. La integración cooperativa implica el empleo de organizaciones bajo un comando combinado permanente, necesario para la conducción tanto en las fases de detección, como en para la respuesta y la recuperación de los ataques. Tener una ciega dependencia en las estrategias comunes de cooperación implica un obstáculo a la libre determinación, un derecho inmanente de legítima defensa meramente declarativo y un paso más en dirección hacia un estado de indefensión olvidando que la seguridad es una función del estado con responsabilidades indelegables.

Cabe preguntarse, en el plano de la ciberseguridad, si es factible avanzar en un proyecto común a nivel regional, en virtud de las diferencias en cuanto a la legislación nacional, la estructura y nivel de los organismos responsables de la ciberseguridad, que se suman a la falta de un consenso en torno a conceptos más que básicos que dificultan la ejecución de una estrategia regional y una real integración de las Fuerzas Armadas de la Unasur, teniendo en cuenta la cuestión relativa a las diferencias existentes en los conceptos en seguridad y defensa entre los países integrantes del CDS y las dificultades que podrían derivar de tales diferencias.

Pero peor aún es contar con estructuras internas que trabajen en forma dispersa, sin contar con un ente que concentre todos los esfuerzos, demostrando incomprensión del valor estratégico de la Ciberseguridad para la Seguridad Nacional, al carecer de la capacidad de actuar con la celeridad que impone esta dimensión en continua mutación.

BIBLIOGRAFÍA

LIBROS

Acosta, O., Rodriguez, J., Arnáiz de la Torre, D., & Taboso Ballesteros, P. (2009). *Seguridad nacional y Ciberdefensa* (1a. ed.). Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Aron, R. (1985). *Paz y Guerra entre Naciones*. Madrid: Editorial Alianza.

Bartolomé, M. C. (2000). *La Seguridad Internacional (Después de la Guerra Fría)*. Buenos Aires: Editorial Instituto de Publicaciones Navales.

Bartolomé. M. C. (2006). *¨La Seguridad Internacional Post 11–S¨*. Buenos Aires: Editorial Instituto de Publicaciones Navales.

Brzezinski, Z. (1970). *Between Two Ages: America's Role in the Technetronic Era.* Nueva York, Viking Press.

Carr, J. (2012). *Inside Cyber Warfare. 2da Ed.* California, EEUU: O'Reilly Media.

Castells, M. (2000). *La era de la información. Economía, sociedad y cultura.* Madrid*:* Alianza Editorial, S. A. 2da Ed.

Celi, P. (2014). *"Nuevas tendencias en defensa y seguridad en América Latina"*. En Atlas Comparativo de la Defensa en América Latina, RESDAL.

Chapple, M. & Seidl, D. (2014). *Cyberwarfare: Information Operations in a Connected World*. Massachusetts: Jones & Bartlett Publishers.

Clarke, R. y Knake, R. (2011). *Guerra en la red. Los nuevos campos de batalla*. Barcelona: Editorial Ariel - Grupo Planeta.

Cornut, H. (2009). "*El Discurso Estratégico en el Ámbito Militar"* en La Revista de la ESG 573 Sep-Dic 09.

Echeverría Jesús, C. (2015). *Relaciones Internacionales III. Paz, Seguridad y Defensa en la Sociedad Internacional.* Madrid: UNED

Gómez Bule, J. - *Cap 06 Ciberamenazas* en De La Corte Ibáñez L. y Blanco Navarro J. (Coord) (2014). *Seguridad nacional, amenazas y respuestas.* Madrid: LID Editorial.

Gomez Hidalgo, M. (2014) *Ciberseguridad y protección en la red: los CERTs/CSIRTs* en Jordà Capitán, E. y de Priego Fernández V. (directoras) (2014) *La protección y seguridad de la persona en Internet. Aspectos sociales y jurídicos*. Madrid: Edit Reus.

Hoffmann, S. (1978). *Primacy or World Order: American Foreign Policy since the Cold War*. New York: McGraw Hill.

Joyanes Aguilar, L. (1997) «*Cibersociedad. Los retos sociales ante un nuevo mundo digital*». Madrid: McGraw-Hill.

Kaplan, M. (1957). *System and Process in International Politics.* New York: Wiley

Keohane, R. y Nye, J. (1988a). *Poder e interdependencia. La política mundial en transición*. Buenos Aires: GEL - Grupo Editor Latinoamericano.

Keohane, R. y Nye, J. (1988b) *Realismo e Interdependencia Compleja.* Buenos Aires: GEL - Grupo Editor Latinoamericano.

Kuehl, D. en el Capítulo 2 "*From Cyberspace to Cyberpower: Defining the Problem.*" en Kramer Franklin, Starr Stuart y Wentz Larry (Eds) (2009). *Cyberpower and National Security.* Washington, D.C. National Defense University Press.

Morgenthau, H. (1986). *Política entre las Naciones. La lucha por el poder y la paz.* Buenos Aires: GEL - Grupo Editor Latinoamericano. 6ª Ed.

Nye, J. (2005). *Soft Power: The means to success in World Politics.* New York: Public Affairs.

Nye, J. (2011). *The Future of Power*. New York: PublicAffairs.

ONU CEPAL (2016). *Ciencia, tecnología e innovación en la economía digital. La situación de América Latina y el Caribe*. Santiago: CEPAL

Palomares Lerma, G. (2006): *Relaciones internacionales en el siglo XXI*. Madrid: Tecnos.

Pastor Acosta (2012). "*Capacidades para la defensa en el ciberespacio*" en *El Ciberespacio. Nuevo Escenario de Confrontación*. Monografías del CESEDEN 126. Madrid: (Centro Superior de Estudios de la Defensa Nacional). Ministerio de Defensa del Reino de España.

López de Turiso, J. (2012). "*La evolución del conflicto. Hacia un nuevo escenario bélico"* en El Ciberespacio. Nuevo Escenario de Confrontación. Monografías del CESEDEN 126. Madrid: (Centro Superior de Estudios de la Defensa Nacional). Ministerio de Defensa del Reino de España.

Feliu Ortega, L. (2012). "La Ciberseguridad y la Ciberdefensa." en El Ciberespacio. Nuevo Escenario de Confrontación. Monografías del CESEDEN 126. Madrid: (Centro Superior de Estudios de la Defensa Nacional). Ministerio de Defensa del Reino de España.

Puime Maroto, J. (2009). "*El ciberespionaje y la ciberseguridad."* en *La violencia del siglo XXI. Nuevas dimensiones de la guerra.* Monografías del CESEDEN 112. Madrid: (Centro Superior de Estudios de la Defensa Nacional). Ministerio de Defensa del Reino de España.

Stel, E. (2005) - *Guerra Cibernética: ciberespacio*. Buenos Aires: Círculo Militar.

Stel, E. (2014). Seguridad y Defensa del Ciberespacio. Buenos Aires: Edit. Dunken.

Tyagi, R. K, Colonel. (2013). *Understanding Cyber Warfare and Its Implications for Indian Armed Forces.* Delhi: Vij Books.

Uzal, R., Dr. (2012) - Artículo *Guerra Cibernética: ¿Un Desafío para la Defensa Nacional?* - Revista Visión Conjunta – Año 4 Número 7 – de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Ventre, D. (2016). *Information warfare*. New Jersey: Wiley

ARTICULOS

Caro Bejarano, M. J. (2011) "La protección de las infraestructuras críticas", IEEE, Documento de Análisis 021/2011, Julio 2011, disponible en: www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf.

CEDEF (2015). Centro de Estudios para la Defensa Nacional de la UNIVERSIDAD DE BELGRANO. Boletín Año 2 - Nº 13 (Dic 2015). Consultado el 18 de marzo de 2016. Disponible en www.ub.edu.ar/centros_de_estudio/cedef/13_diciembre_2015.pdf

CIBER Elcano (2016). Análisis de la actualidad internacional: Jornadas de Ciberdefensa 2016 "Operaciones Militares en el Ciberespacio", del GD. Carlos Gómez López de Medina. Consultado el 20 de setiembre de 2016. Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-12-marzo-2016

CONPES (2011). Documento 3701 - Lineamientos de Política para Ciberseguridad y Ciberdefensa. Consejo Nacional de Política Económica y Social- Departamento Nacional de Planeación. Bogotá. Consultado el 16 de abril de 2017. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

CONPES (2016). Documento 3854 - Política Nacional de Seguridad Digital. Consejo Nacional de Política Económica y Social- Departamento Nacional de Planeación. Bogotá. Consultado el 24 de setiembre de 2017. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Costa Vaz, A. y Jacome, F. (2009) – Policy paper "*El Consejo de Defensa Suramericano. Retos para la cooperación en seguridad y defensa en Suramérica".* Disponible en http://www.fes-seguridadregional.org/images/stories/docs/4646_g.pdf

Dallanegra Pedraza, L. (2008) – *Realismo sistémico estructural. Hacia una teoría totalizadora de las relaciones internacionales* - Reflexión Política, Vol. 10, Núm. 19, junio, 2008, pp. 6-28 Universidad Autónoma de Bucaramanga, Colombia. Disponible en http://www.redalyc.org/articulo.oa?id=11001900

De Vergara, E. Gral Div (R). (2009). Las diferencias conceptuales entre Seguridad y Defensa. IEEBA Instituto de Estudios Estratégicos de Buenos Aires. Disponible en: http://www.ieeba.com.ar/colaboraciones2/Las%20diferencias.pdf

EES 2011. *Estrategia Española de Seguridad. Una responsabilidad de todos*. Consultado el 16 de abril de 2017. Disponible en http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423

ESCUELA DE ALTOS ESTUDIOS DE LA DEFENSA (2014) – *Documentos de Seguridad y Defensa 60 - Estrategia de la información y seguridad en el ciberespacio*. Madrid - - Ministerio de Defensa del Reino de España. Disponible en PDF en http://dialnet.unirioja.es/servlet/libro?codigo=559597

Feliu, L. (2013). Ponencia. *Aproximación Conceptual: Ciberseguridad y Ciberdefensa*. Conferencia en la UPM- Escuela Superior de Ingenieros de Telecomunicaciones. Consultado 16 de abril de 2017. Disponible en http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf

Hoffmann, S. (2002). Tendencias: *Leer el mundo sin anteojeras*. Le Monde. Traducción de Elisa Carnelli en Diario Clarín. Ediciones anteriores. Disponible en http://edant.clarin.com/diario/2002/02/04/o-02415.htm

Jolley, J. D. (2013) "Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World? " International Law Research; Vol. 2, No. 1; Canadian Center of Science and Education. Consultado el 20 de setiembre de 2016. Disponible en: http://www.ccsenet.org/journal/index.php/ilr/article/view/28683

Joyanes Aguilar, L. (2010) "*Conclusiones*" en Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. CUADERNO DE ESTRATEGIA 149 Publicado por el Instituto Español de Estudios Estratégicos (IEEE). Disponible en: https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

LIBRO BLANCO DE LA DEFENSA 2015. Archivo Digital: descarga y online. Disponible en: http://www.mindef.gov.ar/institucional/pdfs/libro_blanco_2015.pdf

Nye, J. (2012). Artículo. *Ciberguerra y ciberpaz*. Disponible en https://www.project-syndicate.org/commentary/cyber-war-and-peace?version=spanish Consultado el 10 de marzo de 2016.

OEA (2015) - Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. Trend Micro Inc. Consultado el 28 de febrero de 2016. Disponible en https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

OPP CAG. (2005). *Políticas de Defensa y Seguridad Internacional*. Observatorio de Políticas Públicas del Cuerpo de Administradores Gubernamentales. Archivo disponible en http://www.sgp.gov.ar/contenidos/ag/paginas/opp/docs/2005/05_OPP_2005_DEFENSA_Y_SEG_INT.pdf Consultado el 14 de marzo de 2017.

OPP CAG. (2010). *Defensa y Seguridad Internacional. El concepto multidimensional de la seguridad en la agenda política argentina.* Observatorio de Políticas Públicas del Cuerpo de Administradores Gubernamentales. Archivo disponible en http://www.sgp.gov.ar/contenidos/ag/paginas/opp/docs/2010/06_OPP_2010_seguridad.pdf Consultado el 14 de marzo de 2017.

Sánchez Gómez-Merelo, M. (2011) *Infraestructuras Críticas y Ciberseguridad*. Disponible en https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/ Consultado el 15 de abril de 2017.

Schreier, F. (2015). *On Cyberwarfare.* DCAF HORIZON 2015 Working Paper Series. Issue No. 7. Disponible en http://www.dcaf.ch/Publications/On-Cyberwarfare. Consultado el 07 de mayo de 2017.

Tallin (2013). *Manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética*. Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE: *Cooperative Cyber Defence Centre of Excellence*). Disponible en https://issuu.com/nato_ccd_coe/docs/tallinnmanual Consultado el 07 de abril de 2016.

Ugarte, J (2001) Investigación. *Los conceptos de defensa y seguridad en América Latina: sus peculiaridades respecto de los vigentes en otras regiones, y las consecuencias políticas de tales peculiaridades*. Latin American Studies Association Disponible en http://lasa.international.pitt.edu/Lasa2001/UgarteJoseManuel.pdf Consultado el 15 de abril de 2017.

,

UIT (2007). *Guía de ciberseguridad para los países en desarrollo*. Disponible en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-S.pdf Consultado el 01 de mayo de 2017.

UIT (2008). *Recomendación UIT-TX. 1205- Aspectos generales de la ciberseguridad*. Disponible en https://www.itu.int/rec/T-REC-X.1205-200804-I/es Consultado el 15 de abril de 2017.

Uzal, R., Dr. (2013a). Transcripción de la exposición realizada el 08/08/2013 en el CARI. Disponible en http://www.cari.org.ar/pdf/crimenorganizado-uzal-2013.pdf Consultado el 15 de abril de 2017.

Uzal, R., Dr. (2013b). AFCEA. Transcripción de la exposición realizada el 24/10/2013 en la Escuela Superior Técnica. Disponible en http://argentina.afceachapters.org/wp-content/uploads/2013/07/presentacionDrUzal.pdf Consultado el 15 de abril de 2017.

Uzal, R., Dr. (2014). *Hostilidades en el ciberespacio entre Estados naciones.* Fundación CEIC (Centro de Estudios Internacionales contemporáneos). Disponible en http://fundaceic.org/2014/08/11/hostilidades-en-el-ciberespacio-entre-estados-naciones/ Consultado el 15 de abril de 2017

Uzal, R., Dr., Riesco, D., Montejano, G., Agüero, W. y Baieli, C. (2015). Presentación en el SIE 2015, 9º Simposio de Informática en el Estado. Disponible en http://44jaiio.sadio.org.ar/sites/default/files/sie160-179.pdf Consultado el 15 de abril de 2017.