Ministerio de Defensa

Estado Mayor Conjunto de las Fuerzas Armadas

Escuela Superior de Guerra Conjunta

Maestría en Estrategia y Conducción Superior

TESIS

TEMA

LA GUERRA CIBERNÉTICA

TÍTULO

LA DEFENSA NACIONAL Y LA ESTRATEGIA MILITAR DE SEGURIDAD CIBERNÉTICA

AUTOR: CORONEL JUAN FERNANDO BARETTO

Director de Tesis: Grl Div (R) EVERGISTO de VERGARA

Año 2017

A LOS TRIPULANTES DEL A.R.A. SAN JUAN

ÍNDICE

INTRODUCCION

El proceso de digitalización que ha tenido lugar a nivel mundial durante las cuatro últimas décadas, implicó para la humanidad múltiples beneficios en áreas tales como comunicación, información y conocimiento, desarrollo e innovación productiva, comercio, administración, navegación, seguridad e incluso defensa. Este proceso es considerado por algunos, de trascendencia equivalente a la revolución industrial y por otros a la aparición de la aviación. No obstante y producto de las imperfecciones propias de los sistemas tecnológicos o más comúnmente del accionar malicioso de individuos, se generaron simultáneamente, importantes vulnerabilidades que afectan su funcionamiento, llegando incluso a poner en riesgo la vida humana. Surgen así las ciberamenazas.

Desde comienzos de los años 90, varios analistas advirtieron sobre los riesgos de las ciberamenazas para la seguridad del Estado. Numerosos casos expusieron la vulnerabilidad de los sistemas y redes informáticas de Estados poderosos ante actores de escasa significancia, convalidándose esta nueva y en apariencia excelente opción estratégica, convenida en llamar ciberguerra, y cuyo ámbito de ejecución es el ciberespacio.

La trascendencia de la temática es tan grande, que fue incluida como prioritaria en las estrategias de seguridad de las naciones más avanzadas del mundo. Por su parte los países menos desarrollados en este aspecto, paradojalmente resultaron ser los expuestos a menores riesgos. No obstante, los avances en el desarrollo hicieron necesario que aún éstos últimos, debieran involucrarse en su seguridad informática. En este ámbito cibernético, resulta claro que la seguridad es abarcadora, y los Estados deben estar en condiciones de defender su seguridad cuando esta se vea amenazada.

Aunque por su naturaleza el espacio cibernético no tiene límites geográficos, los Estados son responsables de los medios de telecomunicaciones e informática dentro de sus fronteras. La existencia de organizaciones gubernamentales y no gubernamentales, empresas, sistemas bancarios, sistemas de salud, sistemas de servicios públicos esenciales como agua potable, tránsito, transporte y medios militares que hacen uso de los medios de telecomunicaciones e informática, hace que cada Estado deba tener una organización que regule y garantice su propia seguridad informática, para que los ataques sean detectados en oportunidad y para limitar y

controlar los daños que puedan producirse. Es por eso que una Estrategia Nacional de Seguridad Cibernética es imprescindible, como parte de una Estrategia de Seguridad Nacional. La Estrategia Nacional de Seguridad Cibernética es la que orienta todas las acciones en este campo, y en ella se inscribe la correspondiente a los medios militares, estrategia que debiera denominarse Estrategia Militar de Ciberdefensa.

La necesidad de difundir la problemática y de promover la integración de acciones que faciliten en el futuro la elaboración e implementación de una estrategia militar de ciberdefensa, constituyeron el objetivo principal de este trabajo. Se fijó para ello la siguiente hipótesis: “La elaboración e implementación de una Estrategia Militar de Defensa Cibernética, que articule los medios y recursos disponibles, en función de fines relacionados con la defensa cibernética, reduciría la vulnerabilidad de las Fuerzas Armadas Argentinas frente a las ciberamenazas e incrementaría simultáneamente las capacidades de la Defensa Nacional”.

Esta investigación es de carácter exploratorio - cualitativo utilizándose en ella fuentes primarias y secundarias como base documental. Se presentan sin embargo dos dificultades: en primer lugar, la mayoría de la bibliografía está en otro idioma diferente al castellano; en segundo lugar por las diferencias de nivel de desarrollo entre los países avanzados y los menos avanzados en la materia, a veces resulta complejo comparar con otros modelos, incluso hasta en el nivel regional.

Se realizó una intensa búsqueda bibliográfica, su clasificación y el análisis de la información. También se diseñaron encuestas y relevaron datos a partir de entrevistas a especialistas en el tema, vivencias de militares y civiles de las Fuerzas Armadas (con experiencia en áreas relacionadas) y entrevistas a responsables del área informática en Comandos, Unidades y Organismos militares. Se buscó con ello identificar eventuales vulnerabilidades informáticas en sistemas y redes de la Defensa Nacional y determinar el nivel de conocimientos acerca de los riesgos existentes.

Se analizó comparativamente el marco legal vigente en organizaciones internacionales, en algunos países considerados como referentes y también de Argentina, para identificar la eventual existencia de vacíos legales relacionados con la seguridad informática del ámbito de la Defensa Nacional.

Se analizaron políticas y estrategias de defensa cibernética y las doctrinas

de ellas derivadas, elaboradas por otros países, identificando los aspectos esenciales y comunes que fueran aplicables a la elaboración de una propuesta esquemática de estrategia militar de ciberdefensa.

Se fijaron tres líneas básicas de investigación. La primera, la determinación de los métodos, formas y medios empleados como “sistemas de armas cibernéticos”, sus modos de funcionamiento, finalidades y efectos. Posteriormente se investigaron ciberataques y operaciones concretas ocurridas en los últimos veinte años que lograron efectos de importancia, confirmando el nivel del riesgo al que se está expuesto.

En segundo lugar, se analizaron las soluciones integrales adoptadas por otros estados u organismos internacionales para reducir los riesgos y/o mitigar sus efectos. Se definió el marco legal internacional y el particular de esos países, sus estrategias y las organizaciones de ciberseguridad y/o ciberdefensa creadas como parte de dichas estrategias.

Finalmente, se definieron los aspectos básicos que debiera incluir una estrategia militar de ciberdefensa, adaptada a la realidad argentina, a sabiendas de que su implementación, podría significar la solución ante un problema creciente.

La abundante información disponible y las múltiples variables a investigar, abren, nuevas e innumerables oportunidades de investigación, que merecen un trabajo específico para cada una de ellas, justificando detener la investigación en el punto alcanzado. Es de esperar que este trabajo sirva de punto de partida para ellas.

Es evidente que la seguridad cibernética es una necesidad de todos los Estados por igual, dando bases para una requerida seguridad cooperativa, donde la seguridad de uno incremente la del otro recíprocamente. No obstante, el deseo de cooperación se contrapone con el hecho de la realidad que, hasta hoy, las agresiones cibernéticas ocurridas en conflictos como en Irán, Estonia, Georgia, y Ucrania, tuvieron su origen presumiblemente en terceros estados interesados (una agresión cibernética es difícil de comprobar y siempre es negada).

La Estrategia Militar de Ciberdefensa es parte de la Estrategia Nacional de Seguridad Cibernética, a su vez parte de la Estrategia Nacional de Seguridad y Defensa. Analizando y sintetizando conceptos, este trabajo sobre la Estrategia Militar de Ciberdefensa aspira a hacer camino al andar.

LA DEFENSA NACIONAL Y LA ESTRATEGIA MILITAR DE DEFENSA CIBERNÉTICA

A. RESUMEN

La digitalización de las estructuras públicas y privadas de un estado y su integración en red, potencian y facilitan su operación y desarrollo eficiente. Este proceso y sus características generan un nuevo ámbito con naturaleza, propósito y conducta únicos

Sin embargo, existen vulnerabilidades de seguridad que pueden afectar su operación. Las estrategias de seguridad nacional de los EEUU, del Reino Unido, de Francia, España, Brasil y otros estados, han abordado los desafíos planteados, destacando la importancia del problema. Producto de ellas, muchos estados han creado agencias de ciberseguridad y ciberdefensa para proteger sus redes y datos. Otros han ido más allá y desarrollaron capacidades cibernéticas para atacar sistemas de computación en otros países.

Existe un consenso general respecto a que la ciberguerra y todo lo asociado a ella, revolucionará el mundo del mismo modo en que lo hizo el advenimiento de la aviación, a comienzos del siglo XX. Si bien el Estado Argentino conoce los riesgos existentes, ha abordado lentamente sus implicaciones legales y técnicas. La falta de políticas y estrategias específicas y de una integración plena entre las agencias especializadas en el tema, limitan un avance real.

Este trabajo se centrará en estudios de casos específicos de los países que se encuentran a la vanguardia del tema, el análisis de los marcos jurídicos nacionales e internacionales existentes, la opinión de los expertos en la materia y la explotación de encuestas entre usuarios y administradores de redes militares nacionales. El objetivo principal de este trabajo es sensibilizar al lector sobre este problema, al mismo tiempo que contribuye a identificar las vulnerabilidades de los sistemas informáticos militares argentinos y propone los conceptos básicos para desarrollar una estrategia militar de ciberdefensa, que puede servir como base para llevar a cabo acciones a corto y mediano plazo

B. PALABRAS CLAVE

Ciberseguridad - Ciberdefensa - Infraestructura Crítica de la Información y Comunicación – Estrategia de Ciberdefensa.

C. ABSTRACT

The digitalization of a country's public and private structures and its network integration empowers and facilitates its operation and efficient development. Nevertheless, there are security vulnerabilities that can affect its operation. Many states have created specialized security and cyber-defense agencies to protect its network infrastructure and data. Other countries went further by developing offensive cyber capabilities to attack foreign computer systems. The national security strategies of the United States, United Kingdom, France, Spain, Brazil, and other states have addressed their cyber challenges highlighting the relevance of the problem.

There is a general consensus that cyber-warfare and everything associated to it, will revolutionize the world in the same way that the advent of aviation did at the beginning of the 20th century. Although the Argentine state is aware of the cyber domain risks, it has addressed slowly its legal and technical implications. Argentina's lack of specific policies and strategies, and an efficient integration between agencies constrain a real advance in the issue.

This paper will focus on specific case studies of countries at the forefront of the subject, the analysis of their existing national and international legal frameworks, the opinion of subject-matter experts and the exploitation of surveys to be conducted among military network users and administrators. The main intent of this work is to make the reader aware of this problem, while simultaneously contributing to identify Argentine military computer systems vulnerabilities and proposing the basic concepts to develop a military cyber-defense strategy, which can serve as the basis for carrying out concrete actions in the short and medium term.

D. KEY WORDS

Cyber-security - Cyber-defense - Critical Information and Communication Infrastructure - Cyber Defense Strategy.

CAPÍTULO I

EL CIBERESPACIO COMO NUEVO AMBIENTE PARA EL DESARROLLO DE OPERACIONES MILITARES.

"…debemos entender cómo distribuir y proteger nuestros intereses nacionales en el dominio cibernético y aunque se trata claramente de una cuestión de gobierno, la defensa tiene un interés legítimo en el desarrollo de capacidades defensivas y ofensivas cibernéticas".[1]

El proceso de digitalización de cualquier Estado, entendido como la incorporación de sistemas informáticos y capacidad de operarlos en redes integradas, constituye un factor que incrementa sus capacidades de gestión, administración y control, en el marco de la optimización de recursos humanos y financieros que emplea. Aplicado al caso particular de las Fuerzas Armadas, este proceso actúa como multiplicador de su poder militar, al mejorar la gestión de la información y el conocimiento situacional, acelerar la toma de decisiones y dar mayor precisión a los distintos sistemas de armas que ellas emplean.

Sin embargo, presenta importantes vulnerabilidades en su operación, causadas por fallas de los sistemas o por la acción deliberada de terceros, lo cual se denomina amenaza cibernética, afectando también a otras áreas estatales y privadas. Para reducirlas, muchos Estados crearon organizaciones gubernamentales dedicadas a incrementar su seguridad en materia cibernética y dentro de sus FFAA, organismos especializados en defensa cibernética y en el desarrollo de capacidades ofensivas para afectar los sistemas informáticos de los probables enemigos.

En este contexto, la acción del Estado tanto como de sus Fuerzas Armadas, tiene su desarrollo en un espacio novedoso y único, cuyo empleo consciente o inconsciente, aumenta día a día y que es conocido como ciberespacio o espacio cibernético. Su influencia en la vida cotidiana, difícil de apreciar, ya que hoy cualquier actividad humana, está en él comprendida.

---

[1]Fuerza Aérea Británica Sir Stephen Dalton. Artículo publicado por el periódico *TheIndependent* – 16 Feb 2010 - http://www.independent.co.uk/news/media/online/twitter-is-a-weapon-in-cyber-warfare-1900535.html. Tomado de Guerra Cibernética – Stel, Enrique, Círculo Militar 2005

Se reconoce convencionalmente, que el desenvolvimiento de la vida humana y todas las actividades que con ella se relacionan, guerras incluidas, acontece en cuatro ambientes diferenciados. Estos ambientes reconocidos, son el ambiente terrestre, el marítimo, el aéreo y el espacial. Cada uno de ellos, tiene algunas características distintivas que lo identifican, como ser el medio material sobre el que se sustentan, las actividades que pueden desarrollarse, los bienes, productos y otros elementos que de ellos se obtienen, etc. Sin embargo, comparten otras características comunes, tales como la existencia de límites definidos, un nivel de capacidad física para controlarlos y una base cognitiva desarrollada por el ser humano que permite la comprensión y predicción de su comportamiento cuando interactúa con el hombre.

El ciberespacio, es un nuevo ambiente que se solapa sobre los otros cuatro, integrándolos como nunca antes estuvieron. A diferencia de los cuatro anteriores, no comparte características comunes y por lo tanto es único. En él, el ser humano realiza infinidad de actividades, entre las que se pueden citar el correo electrónico, la banca y el comercio electrónico, lectura, entretenimiento, administración, investigación, desarrollo y diseño en innumerables disciplinas, redes sociales, navegación aérea, marítima y terrestre, comunicaciones terrestres y espaciales, defensa y seguridad, etc.

El término ciberespacio, aparece por primera vez en textos de ciencia ficción. La palabra proviene del griego *Kybernetes* la cual significa “quien dirige o gobierna”. Su acepción moderna apareció en 1948 en un libro del matemático Norbert Wiener, para describir el estudio del comando, control y comunicaciones en el mundo animal o en el mundo de la mecánica (Tabansky, 2011, pág. 77).

Sin embargo en la actualidad, define un fenómeno que aparece inicialmente hacia 1844 con la invención del telégrafo, el cual permitió por primera vez aprovechar las increíbles posibilidades que el empleo de ondas electromagnéticas y los campos asociados, otorgaban a las necesidades humanas. Implícito en ello, iba el uso de tecnologías avanzadas para la época.

Un punto de inflexión esencial en el desarrollo del ciberespacio fue la invención de la primera computadora numérica en 1949, conocida como Eniac.

Posteriormente y limitando más el alcance de su definición, se pueden mencionar otros hitos, entre ellos la vinculación de redes de comunicaciones entre ordenadores y otras máquinas (inicio de los años 70), la aparición de Internet y de las computadoras

personales hacia mediados de los 90, la integración plena de sistemas informáticos con otros sistemas y máquinas y finalmente, el uso masivo de computadoras, procesadores, teléfonos celulares del tipo Smartphone hasta llegar hoy en día al concepto de "*internet of the things*" o IoT, término que hace referencia al empleo masivo de ordenadores y sistema de procesamiento, no sólo en computadoras, sino en innumerables dispositivos y artículos (Smart TV, heladeras, sistemas de control remoto domiciliarios, automóviles con computadora, telefonía de voz sobre datos o VoIP, etc) (Shmuel Even, David Siman-Tov, 2012, pág. 95).

Al referirse al espacio cibernético, Dan Kuehl, en su exposición "*Cyberspace & Cyberpower: Defining the Problem*", presentada en la conferencia *Cyberpower & National Security, 2009*"[2], lo define como:

> *"El Ciberespacio es el conjunto de un dominio global dentro del entorno de la información, cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicaciones"*

Para la Unión Internacional de las Comunicaciones, el ciberespacio es el ***"****terreno físico y no físico creado por y/o compuesto de algunos o todos de los siguientes elementos: Ordenadores, Sistemas informáticos, Redes y programas informáticos, datos (Información, contenido y tráfico) y usuarios"*.

La importancia del ciberespacio es tal, que ha sido definido como uno de los cuatro "*global commons*"[3], en el Informe de la Estrategia de Seguridad Nacional de los Estados Unidos del año 2010 (USGovernment, 2011).

Los tres restantes, aguas internacionales, espacio aéreo y espacio exterior, tienen, a diferencia del ciberespacio, un basamento físico y material claramente limitados. No ocurre lo mismo con el ciberespacio, el que particularmente, integra y está superpuesto en los tres anteriores.

La composición del ciberespacio reconoce tres niveles interdependientes o

[2] (Gómez de Agreda, 2012)
[3]Espacios que, sin ser de soberanía de una nación en particular, pueden ser aprovechados en beneficio propio por cualquier actor, conforme a reglas concretas aceptadas internacionalmente.

capas (Libicki, 2009, pág. 12). En este gráfico, se muestran un resumen de las actividades y propósitos de cada capa, sus contenidos y las tendencias de evolución en el futuro cercano:

CAPA	ACTIVIDAD/ PROPÓSITO	CONTENIDOS	TENDENCIAS
HUMANA	Uso	Lectura, Investigación, redes sociales, comercio, enlace, delito, ciberguerra	Incremento de comunidades (web 2) + interconectividad
LÓGICA	Tareas del software (traducción, proceso, guarda y devolución de información)	Texto, video, imágenes, audio, lenguaje de programación, algoritmos, diagramas de flujo, etc	+ aplicaciones + complejidad + interfases (MMI)
FÍSICA	Hacer funcionar a la lógica a requerimiento usuario	Hardware, señales RF, luces, ondas EM, Datalinks, Comunicación	+ cantidad y variedad de sistemas y subsistemas (blue tooth, IR, FO , Satélite, tablets, smartphones, etc)

Figura 1: Capas componentes del ciberespacio y características (Shmuel Even, 2012, pág. 12) (adaptación del autor).

Estas capas representan diferentes componentes:

- La capa humana: representada esencialmente por los usuarios.
- La capa lógica: constituida por el software y los bits. Representa la información, las instrucciones y los activos del ciberespacio (es decir el software de utilidad y el

malware).

- La capa física: incluye a los componentes físicos, es decir al hardware, las infraestructuras fijas y móviles en tierra, mar, aire y espacio.

De las capas mencionadas, la más vulnerable es la capa humana, tal como lo expresa una tradicional frase conocida entre los informáticos "*no hay parches para la estupidez humana*[4]".

El ciberespacio, adquiere una dimensión especial como ambiente operacional desde el punto de vista militar. Las Tecnologías de la Información y la formación del ciberespacio, están cambiando rápidamente la naturaleza del campo de combate moderno. El ciberespacio constituye hoy un Teatro de Operaciones en el que el público juega un papel central (Shmuel Even, 2012, pág. 9).

¿Pero qué hace del ciberespacio un ambiente operacional distinto a los conocidos tradicionalmente?.

En primer lugar, presenta una estructura organizacional diferente. En contraposición a los otros ambientes, eminentemente materiales, el ciberespacio tiene un ámbito real (las capas físicas y humanas) y uno virtual (la capa lógica), de difícil mensura.

Y aunque los estados tienen responsabilidad sobre los servidores y repositorios de datos en su propio territorio, el ciberespacio, no reconoce fronteras ni límites siendo imposible definir un ciberespacio interno y otro externo.

También y a diferencia de los otros cuatro ambientes, sobre los cuales puede ejercerse un amplio grado de control, el control del ciberespacio es limitado.

Es en la práctica imposible, ejercer el control de ordenadores, redes, interfaces, emisiones electromagnéticas y fundamentalmente a los millones de usuarios que en él actúan. Para organizaciones con escasos recursos, ese control solo es factible de realizar sobre las propias redes y sistemas y en forma limitada. Pretender hacerlo en un nivel mayor, requeriría de computadoras con una capacidad muy superior a las actuales como también, disponer de personal especializado dedicado exclusivamente a ello, hecho que no sería rentable desde el punto de vista de la relación costo eficacia.

[4] Del autor. Parche es en jerga informática, cambios o modificaciones introducidas a un programa para resolver problemas de funcionamiento, actualizarlo o darle mayor capacidad.

Y en relación con los que emplean el ciberespacio para ejecutar acciones que afecten a la integridad de otros sistemas, es redundante decir que el anonimato es una de las características destacables de los atacantes, siendo muy complejo y difícil su identificación sin medios y equipos adecuados y costosos.

Distinguir entre actores estatales o particulares, individuos o grupos, civiles o militares, queda fuera del alcance de la mayoría de las organizaciones.

Del mismo modo, sus fines y propósitos, serán normalmente desconocidos, y podrán variar desde la simple práctica y ejercitación en vulnerar sistemas y redes propias de hackers aficionados, pasando por acciones delictivas varias, terrorismo, *hacktivismo*[5], espionaje industrial y militar, hasta llegar a las nuevas formas de guerra. Y si se considera la facilidad de acceso, tanto desde el punto de vista económico como del conocimiento en informática necesario, los factores de riesgo están al alcance de muchos.

La consideración más breve y dramática del reconocimiento de esta nueva realidad, se puede señalar en las palabras del Dr. Dan Kuehl, de la Universidad Nacional de la Defensa (NDU) de los Estados Unidos.

En su conferencia "*Information and National Security",* afirmó que "*la gran diferencia entre la guerra convencional y la cibernética es que no existe la profundidad estratégica que pueda permitir a una potencia recuperarse tras un primer golpe. En el ciberespacio, el primer golpe puede ser decisivo".*

[5] Acrónimo entre las palabras hacker y activismo.

CAPÍTULO II

LA DIMENSIÓN DEL RIESGO

A. GENERALIDADES

No existe una definición ni categorización consensuada respecto al formato de lo que actualmente engloba el concepto de amenaza cibernética, debido en parte a lo novedoso del tema y al secreto que la envuelve. Asimismo, las diferentes formas de agresión o amenazas, normalmente actúan integradas y logrando efectos variados, lo cual dificulta aún más su clasificación.

Una primera distinción, puede establecerse entre la Netwar (guerra de redes) y la Cyberwar (guerra cibernética). La Netwar puede ser definida como "la serie de conflictos sociales de contenido ideológico, librados principalmente a través de Internet. Se incluyen dentro de ella a las distintas variantes de conflictos sociales, dentro de los cuales, el crimen organizado puede ocupar un lugar central.

La Cyberwar, por su parte, es el conjunto de acciones ejecutadas en el espacio cibernético, librado a nivel esencialmente militar y normalmente, como parte complementaria y de apoyo a otro tipo de operaciones, aunque como se verá más adelante, su papel es cada día mayor.

No obstante, por las características del ambiente en el que ambas se desarrollan, no pueden ser definidas ni diferenciadas claramente. Es así que en el modelo de conflictos de 4ta Generación o guerras híbridas planteado por Frank Hoffman, cuyo concepto implica "fusionar la letalidad del conflicto estatal con el fervor salvaje y fanático de la guerra irregular, ya resulta sumamente complejo distinguir el límite esencialmente militar de un conflicto.

Ambas están ligadas por los conceptos de "seguridad cibernética" y "defensa cibernética". Aunque ambos conceptos pueden parecer similares, no lo son.

La Seguridad Cibernética se define como "*conjunto de acciones que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros*". Por su parte la defensa cibernética se refiere al *"conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo*

al enemigo o a otras inteligencias en oposición" (Pablo Edgardo Camps Laserre, 2016).

Ciertamente, lo expresado sugeriría que la seguridad cibernética o ciberseguridad, es la actividad primaria e imprescindible para operar en el ciberespacio y que la defensa cibernética, es una actividad que la incluye, como tarea básica.

Sin embargo, estas definiciones establecidas por el Consejo Argentino de las Relaciones Internacionales (CARI) en 2013, en particular la de Seguridad, resultarían algo limitadas en función de las nuevas amenazas y exigencias, y contradictorias con las definidas por países vecinos.

Así por ejemplo, la Doutrina Militar De Defesa Cibernética do Brasil, define a la seguridad cibernética como el "*arte de asegurar la existencia y la continuidad de la sociedad de la información de una nación, garantizando y protegiendo en el espacio cibernético, sus activos de información y sus infraestructuras críticas*[6].

En el mismo documento doctrinario, se define a la Defensa Cibernética, al *"conjunto de acciones ofensivas, defensivas y exploratorias realizadas en el espacio cibernético, en el contexto de un planeamiento nacional de nivel estratégico, coordinado e integrado por el Ministerio de Defensa, con las finalidades de proteger los sistemas de información de interés de la Defensa Nacional, obtener datos para la producción de conocimiento e inteligencia y comprometer los sistemas de información del oponente"*[7].

Estas nuevas definiciones sugieren lo contrario a lo expresado por Camps, ya que coloca a la Seguridad Cibernética como incluyente y por encima de cualquier otra actividad.

La seguridad cibernética, entendida ésta como la protección de los sistemas de un Estado contra cualquier clase de ataque cibernético, reconoce cuatro tipos de amenazas genéricas diferentes. Estas son el delito cibernético, el terrorismo cibernético,

---

[6] Segurança Cibernética - Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. MD31-M-07 - DOUTRINA MILITAR DE DEFESA CIBERNÉTICA – Ministerio da Defesa – 2014. Traducción del autor.

[7] Defesa Cibernética - Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. MD31-M-07 - DOUTRINA MILITAR DE DEFESA CIBERNÉTICA – Ministerio da Defesa – 2014. Traducción del autor.

el espionaje cibernético y la guerra cibernética.[8] De ellas, una sola es atribuible exclusivamente a un origen estatal (guerra cibernética), en tanto que las otras acciones, pueden ser indistintamente originadas en actores estatales como privados.

El delito cibernético[9], es una de las áreas delictivas de mayor crecimiento. Cada día más delincuentes, explotan la velocidad y anonimato que ofrecen las modernas tecnologías para cometer sus ilícitos, los que incluyen ataques contra computadoras, robos de bases de datos, robos de identidad, pedofilia, fraudes en internet, penetración de entidades financieras, etc.

Con las mismas herramientas y acciones que el delito cibernético, para obtener recursos o para infiltrar a sus combatientes, el ciberterrorismo persigue objetivos y finalidades diferentes, siendo sus blancos prioritarios, los sistemas de infraestructuras críticas de la información y comunicación.

El espionaje cibernético es ejecutado por Estados o empresas, para obtener información relacionada con adelantos tecnológicos, procesos productivos, estados financieros y otros secretos. Es curioso que aunque el espionaje es condenado en las leyes nacionales, es tolerado en el derecho internacional.

La ciberguerra, por su parte, puede definirse como, "…el empleo de los medios cibernéticos por las fuerzas armadas en un contexto de enfrentamiento bélico contra otro actor relevante en términos de seguridad"(Stel, 2005, P 11), para atacar sistemas, redes e instalaciones informáticas y de comunicaciones. Puede traer implícito el uso de la fuerza convencional para complementarla o repelerla. Por su parte, Joseph Nye[10] la definió como"… una acción hostil en el ciberespacio cuyos efectos amplían o son equivalentes a una violencia física importante..."[11]. Sus características son: gran complejidad, asimetría, objetivos limitados, corta duración, reducción de daños físicos, mayor espacio de combate, menor densidad de tropas, lucha por la superioridad de la información, mayor integración y exigencias a los comandantes, cambios en el concepto de concentración de fuerzas y necesidad de reacción rápida, características compartidas

[8] El uso internacional hace que se lo refiera indistintamente como ciberdelito, ciberterrorismo, ciberespionaje y ciberguerra. Así se los denominará en este trabajo a partir de este momento.
[9] En inglés cybercrime. En el tema, es de uso normal los neologismos ciberdelito, ciberespionaje, ciberterrorismo y ciberguerra.
[10] Antiguo asesor del Secretario de Estado de los EEUU.
[11] Tomado el 21 de abril de 2013 de la web http://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish#4Dm6oKEdyx0wEikX.99

con otros niveles de conflicto, fundamentalmente el de baja intensidad. Sin embargo, hay tres exclusivas y distintivas de otras formas de guerra: su naturaleza dual (la ejecutan con igual eficiencia, civiles y militares, contra otros civiles y militares), luego el anonimato y finalmente, su accesibilidad, al emplear medios cada día más baratos y al alcance de todos.

La amenaza cibernética se manifiesta en dos tipos básicos de ataque. El primero o *Broadband attack* (ataque de banda ancha) se caracteriza por ser indiscriminado, no buscar efectos definidos o concretos y sin existencia de control sobre los riesgos que su ejecución implica.

El segundo denominado *Targeted Attack* (en referencia a un ataque específico hacia un blanco), se caracteriza por ser dirigido, sus efectos son deseados y existe cierto control de riesgos en cuanto a efectos no deseados se refiere (Amir Averbuch, Gabi Siboni, 2013, pág. 45).

La constante evolución de las amenazas, ha llevado al hecho de que en sólo cinco años, se haya revertido el mayor índice de incidencia de los ataques tipo Broadband, por los de ataques dirigidos.

Las amenazas genéricas mencionadas, se distinguen entre sí por su propósito o finalidad y por los modos y armas que se emplean en ellas.

Como una forma de clarificar las distintas ponencias y definiciones, en la intención de establecer una lógica para su descripción, se establece en la tabla siguiente, una propuesta de clasificación, distinguiendo las herramientas empleadas de los propósitos.

ACCIONES	PROPÓSITO O FINALIDAD	MODOS/ARMAS
CIBERDELITO	Fraudes, robos de información, comisión de delitos, robos de identidad, robo de datos, violación de datos personales, etc.	Ransomware, Denegación De Servicio (DoS Y DDos), tráfico HTTPs malicioso, Malware diverso
CIBER TERRORISMO	Penetración ideológica, expansión de acción terrorista, instauración del terror, transmisión de información en forma encubierta mediante el empleo de redes abiertas.	Campañas abiertas (uso de redes y aplicaciones como Youtube, Facebook, etc) o encubiertas. Eventualmente, ciberdelitos para generación de recursos. Emplea los mismos medios que el ciberdelito, además del Chipping.
CIBER ESPIONAJE	Robo de información técnica, personal o financiera a empresas, organizaciones de gobierno o particulares.	Phishing, Spearphishing, Chipping, Ransomware y esencialmente Spyware, además de otros tipos de Malware.
CIBERGUERRA	Lograr la victoria en el ciberespacio sobre fuerzas enemigas, en el marco de un conflicto bélico, sea en apoyo a otras operaciones convencionales o por sí misma.	Su ejecución puede enmarcarse además, dentro del concepto de guerra preventiva. Al igual que el ciberterrorismo, emplea los mismos medios que el ciberdelito, además del Chipping. Tiene modalidades ofensivas y defensivas, las que contemplan el uso de programas de seguridad, tales como Firewall complejos.

Figura 2: Amenazas clásicas en el ciberespacio (del autor).

En los últimos años, algunos autores señalan la aparición de otros dos tipos de amenazas genéricas, que se diferencias de las anteriores también en base a los

parámetros mencionados, la finalidad y los modos.

La primera de ellas es conocida como hacktivismo. El término surge de la unión de las palabras hacker más activismo. El hacktivismo implica el uso no violento de herramientas[12] o armas cibernéticas, persiguiendo fines políticos u otros ajenos al interés estatal.

Los primeros actos de *hacktivismo* eran frecuentemente simples modificaciones de los sitios web (se cita como ejemplo, la peletería Kriegsman Fur, hackeada en 1996). Posteriormente se inició la práctica de *doxing*. El *doxing* consiste en la investigación, recopilación y difusión de información personal que puede ser asociada a un individuo.

El *hacktivismo* se hizo más agresivo desde hace unos 10 años. Las protestas del Project Chanology en 2008, ejecutadas por el grupo de hackers Anonymous, utilizaron ataques de denegación de servicio distribuido (DDoS) y divulgaron comunicaciones internas de dicha organización[13].

La siguiente forma de amenaza es la denominada *Haxposción* (hacking + exposición de datos). Esta consiste en el robo y divulgación pública de datos confidenciales de sitios web, con la finalidad de que cesen con su actividad. Se dio a la luz en gran escala en 2015, cuando dos objetivos de alto perfil fueron atacados. Ellos fueron Hacking Team, una empresa italiana dedicada a la seguridad informática y Ashley Madison, un sitio web destinado a acordar relaciones sexuales entre sus miembros. La diferencia fundamental con el robo de datos conocido hasta entonces, fue que la información fue dada a conocer públicamente a través de un sitio de internet propio.

Según los especialistas, la *haxposición* pertenece a una categoría diferente de

---

[12] Entre ellas se pueden citar alteración de páginas webs, redirecciones a sitios de interés, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software aplicado. Los movimientos hacktivistas, se relacionan normalmente con campañas ambientalistas, de desarme, opositoras a organizaciones o instituciones estatales o privadas, apoyo a corrientes de opinión, etc.

[13] Project Chanology fue una serie de protestas iniciadas en la web, y promovida por el grupo de hackers Anonymous, contra la Iglesia de la Cienciología. La intención inicial fue protestar por el retiro del sitio de videos de Youtube, un video promocional del actor estadounidense Tom Cruise, en el que el actor expresaba que la iglesia era la salvación y la esperanza de muchos. Anonymous consideró que el hecho era un acto de censura y subió un video contra la mencionada secta (Message to Scientology - Mensahe a la cienciología), en el que pide expulsarla de Internet.Posteriormente se realizaron ataques de denegación de servicio (ver más adelante en Página) y otras medidas que incluyyeron protestas públicas, coordinadas a través de internet. En forma paralela, se pretendió (sin éxito a la fecha), que se investigue la exención de impuestos de la cual goza la Iglesia Cienciologica.
https://www.theguardian.com/technology/2008/feb/04/news

amenaza y que, con el paso del tiempo, será más frecuente.

En el mes de julio de 2015, hackers robaron y subieron a un sitio web, unos 400 gigabytes de información de la empresa de seguridad italiana *Hacking Team*. Según los datos revelados, la empresa proporcionaba soluciones de seguridad informática (algunas de ellas veladas) a gobiernos o regímenes represivos y autoritarios. Este hecho contribuyó a la búsqueda de los atacantes, ofreciéndose una recompensa elevada para ello.

Ese mismo mes, se produjo otro incidente aparentemente no relacionado. Un grupo autodenominado *Impact Team*, subió a internet datos privados de las cuentas de usuarios del sitio web Ashley Madison (un sitio de citas para encuentros sexuales en esencia), exigiendo su cierre. Adicionalmente, exigieron el pago de un rescate por los datos secuestrados. Al no cumplir las exigencias, se subieron más datos al mes siguiente.

La ruptura del convenio de confidencialidad entre quienes pagaban el sitio y la empresa propietaria, dio inicio a una serie de demandas judiciales y a la pérdida de credibilidad y posibilidad de subsistencia del sitio. Parte de los datos que habían sido divulgados, probaban que la empresa incumplía su parte contractual y además inventaba perfiles falsos femeninos para atraer a mayor cantidad de hombres.

Hechos similares ocurrieron cuando se divulgaron adulteraciones a los registros de las pruebas de emisiones de la empresa Volkswagen y en las vulnerabilidades de seguridad de los sistemas informáticos de vehículos Chrysler, Jeep y Fiat, los que aparentaban un riesgo para conductores y acompañantes.

Y aunque *"…Los cibercriminales que creen tener la razón y el derecho de actuar como árbitros de la justicia pueden sentirse inclinados a buscar nuevos secretos y exponerlos públicamente, dañando a víctimas inocentes en el proceso…"* (Ramos, Cobb, Gutiérrez Amaya, 2016, pág. 72).

En la *haxposición*, la violación de la seguridad, el robo de datos y su publicación, se complementa con la exigencia del pago de un rescate, se agrava el robo con la extorsión y se excede el límite ético planteado por la mayoría de los hactivistas. Y se adiciona la publicación de información personal identificable de empleados o clientes de una empresa u organización, se pasa a un nuevo y riesgoso nivel de irresponsabilidad.

La evolución de las amenazas es constante y creciente en variedad, sofisticación

y efectos. La NATO, las clasifica y agrupa en tres niveles, usando como parámetros de comparación, el nivel de conocimiento, los recursos financieros disponibles, el conocimiento del blanco, la facilidad de detección y las herramientas que emplean para el logro de sus propósitos, entre otros (NATO, New threats: the cyber-dimension).

En el gráfico siguiente, se muestran los diferentes niveles y los riesgos que llevan implícitos.

AMENAZA NIVEL 1 (Variedad de Jardín)	AMENAZA NIVEL 2 (Mercenario)	AMENAZA NIVEL 3 (Estado Nación)
• Poca experiencia • Recursos monetarios limitados • Oportunistas • Conocen debilidades del blanco • Usan virus, gusanos, troyanos básicos y bots • Fácilmente detectables • Se emocionan mientras realizan el ataque y se jactan de lo hecho	• Grandes habilidades. • Buen apoyo financiero • Ataques dirigidos • Conocen debilidades del blanco • Usan virus, gusanos, troyanos, bots y medios para introducir herramientas sofisticadas • Buscan y explotan datos de valor • Son detectables per es difícil atribuirle la responsabilidad	• Medios muy sofisticados/variados • Norma: son agencias de Inteligencia • Muchos recursos financieros • Conocimiento acabado del blanco y de la información • Presencia encubierta redes claves • Difícil detección • Pueden emplear técnicas de chipping

Figura 3: Niveles de amenazas y riesgos (adaptación del autor).

Definidos los conceptos básicos sobre los ámbitos de aplicación de las ciberamenazas y sus propósitos, se describirá en el punto siguiente, las principales medios empleados en estos ámbitos.

B. LAS ARMAS CIBERNÉTICAS

Las modalidades, medios y “armas especiales”, están definidas esencialmente por su

finalidad, lógica de programación y formas de accionar. Entre las más conocidas, se pueden destacar:

- Corrupción del hardware (modchip, bootkit o chipping)[14]:

Es la modificación del funcionamiento normal de un sistema informático mediante la instalación ilegal de un chip u otros dispositivos, que alteran el funcionamiento de los circuitos electrónicos. En la imagen siguiente, se muestra un ejemplo de chipping realizado sobre una cónsola de juegos.

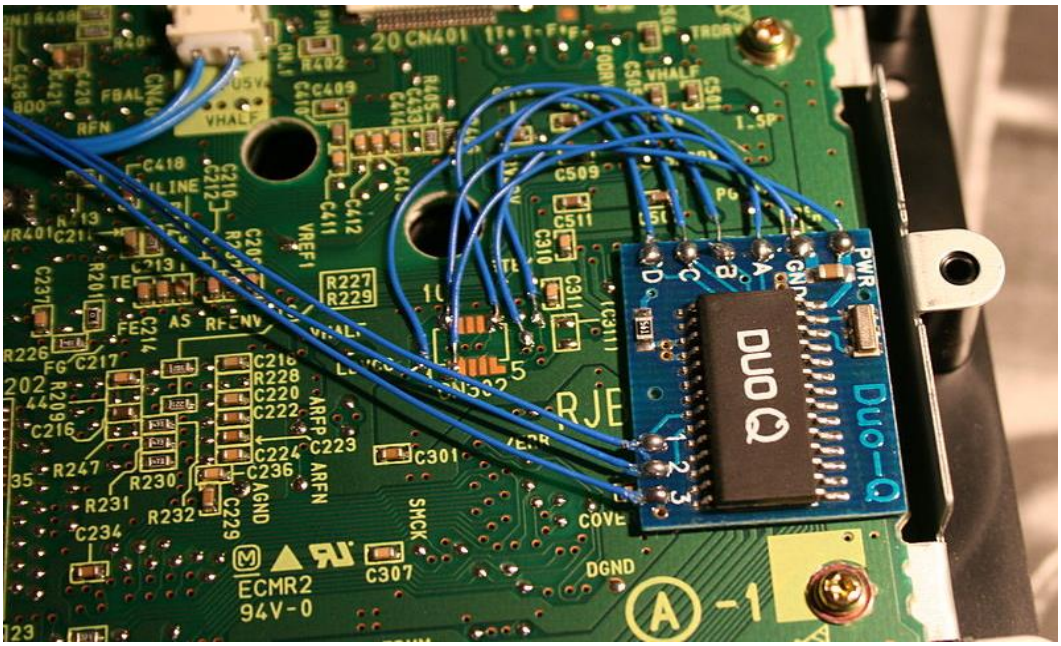


Figura 4: Ejemplo de procesador afectado por chipping (fotografía libre de internet).

- Afectación del software o malware:

Es la alteración del funcionamiento de un programa mediante software especializado. Entre ellos, podemos mencionar (Kaspersky, s.f.):

1) "**Virus clásicos**. Programas que infectan a otros programas por añadir un código que le permite tomar el control después de la ejecución de los archivos infectados. El objetivo principal de un virus es infectar. La velocidad de propagación de los virus es algo menor que la de los gusanos"[15].
2) "**Gusanos de red (worms)"**. Este tipo de malware usa los recursos de red para

[14] Del inglés *chip*, circuito electrónico integrado.

[15] Ver https://support.kaspersky.com/sp/viruses/general/614

distribuirse. Su nombre implica que pueden penetrar de un equipo a otro como un gusano (o parásito). Normalmente se propagan por medio de un correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (Peer Two Peer - P2P, tales como el Ares o Emule), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.

Al penetrar un equipo, el gusano busca obtener las direcciones IP (Internet Protocol) de otros equipos en la red para empezar a enviar sus copias. También suelen usar los datos de la lista de contactos del correo electrónico. La mayoría de los gusanos se propagan en forma de archivos pero existe una pequeña cantidad de gusanos que se propagan en forma de paquetes de red y penetran directamente la memoria RAM del equipo víctima, donde a continuación ejecutan su código.

3) "Troyanos" (Trojans): Su nombre guarda relación directa con el Caballo de Troya de la literatura griega. La característica principal de esta clase de malware, es su capacidad para penetrar la computadora a través de algún software especial que sea descargado intencionalmente o no por el usuario. A partir de ello, puede ejecutar, a través de una gran variedad de programas, acciones diversas sin que el usuario lo perciba o consienta. Entre estas acciones, se puede mencionar la recolección de datos y su remisión otros sistemas, la destrucción o alteración de datos con intenciones delictivas, la provocación de desperfectos en el funcionamiento del sistema, e incluso el uso de los recursos de la computadora (por ejemplo, la captura de listas de contactos), para fines varios, como ser el envío de correos masivos (Spam).

No actúan como un virus clásico ya que no infecta a otros programas o datos. La diferencia principal, es su incapacidad para penetrar a los equipos por sí mismo. No obstante ello, son capaces de ocasionar daños más importantes que un virus convencional.

4) Spyware: Consiste en un software que permite recolectar información sobre un usuario u organización de forma no autorizada. Su presencia puede resultar completamente invisible para el usuario. Normalmente obtienen datos sobre actividades de los usuarios, el contenido de su harwdare de almacenamiento, los programas en él instalados y otros relacionados con las características de la

conexión. Algunos de ellos (los más conocidos el Gator y EZula[16]), permiten ejercer el control remoto del equipo.

5) Rootkits: son un tipo de software maligno diseñados para acceder o controlar remotamente a un equipo, sin que el usuario o los programas de seguridad lo detecten. Una vez instalado, habilita a la ejecución de programas, acceso a datos, robo de información, alteración de los programas de seguridad para evitar su detección e incluso permitir su empleo como botnet, etc.

Son usados normalmente por un hacker para evitar ser detectado mientras busca obtener acceso no autorizado a un ordenador. Esto se logra de dos formas: reemplazando archivos o bibliotecas del sistema o instalando un módulo de kernel. Una vez instalado el rootkit se obtiene un acceso similar al del usuario, por lo general, craqueando una contraseña o explotando una vulnerabilidad, lo que permite usar otras credenciales hasta conseguir el acceso de raíz o administrador.

Constituyen uno de los malwares más peligrosos y de difícil detección, ya que permanentemente actúa oculto.

6) Bots: en esencia constituyen programas que ejecutan automáticamente funciones específicas. Aunque son parte normal de software legal (video juegos, respuestas online, etc), cada vez se emplean para funciones maliciosas, incluido el uso de ellos para activar botnets, spambots que crean avisos en sitios web, afectan servers o distribuyen malware a partir de búsquedas populares de internet.

7) Bugs: son fallas de programación que provocan efectos no deseados en los programas. Si bien normalmente son hechos con intención, algunos programas de software abierto tienen estos bug incluidos en forma intencional, para facilitar el acceso posterior al sistema. En los casos de los programas de seguridad informática,

---

[16] Ezula (que a veces se escribe "eZula") es una forma de adware que se instala como parte de un objeto de ayuda al navegador (BHO). Sin el permiso del usuario, el ezula se comunica con un servidor remoto y le muestra a la persona anuncios basados en contexto. El Ezula no contiene virus peligrosos, pero puede hacer más lento el navegador del usuario y tiene que instalarse manualmente. Como forma parte de un BHO o Browser Helper Object (en español: objeto ayudante del navegador), puede aparecer como un complemento de terceros opcional durante el proceso de instalación. El programa agrega enlaces de publicidad a palabras clave en una página web, y cuando se hace clic en él, dirige al usuario a un sitio web de un tercero, por lo general relacionado con lo que originalmente estaba buscando. El programa se inicia automáticamente con el arranque de Windows y se puede actualizar de forma remota a través de Internet sin consentimiento del usuario. Se ha informado de que vienen como parte de un programa llamado TopText o Surf+. https://latam.kaspersky.com/co/internet-security-center/definitions/ezula-virus consultado el 15 de octubre de 2016.

la existencia de bugs es la más riesgosa, ya que permitiría a los atacantes, penetrarlos, cambiar los privilegios de usuario y eventualmente, sustraer datos del sistema.

***- Spam**:*

Son mensajes no solicitados de un remitente desconocido, enviados masivamente. Normalmente tienen carácter publicitario, político, de propaganda, de solicitud de ayuda, etc. Algunos spam suelen proponer realizar operaciones ilegales con dinero o la participación en algún negocio de gran rentabilidad. El Spam genera una carga adicional a los servidores de correo y pueden causar pérdidas de información.

En el siguiente ejemplo de correo electrónico recibido por el suscripto, se muestra simultáneamente, el envío de un correo tipo Spam, que puede incluir suplantación de identidad y seguramente un gusano como adjunto. Se ordenan cronológicamente recepción y respuesta.

Las imágenes corresponden a capturas de pantalla del celular del autor. En la imagen superior izquierda, se muestra el correo original recibido de un remitente conocido, con el cual no obstante, no existe un intercambio fluido de correo electrónico. En ella, el remitente solicita se acceda a un enlace, sin mayores precisiones.

En la imagen superior derecha, se observa la respuesta del autor, en la cual se advierte al contacto real, sobre la recepción de un correo no esperado o en su defecto, sospechoso.

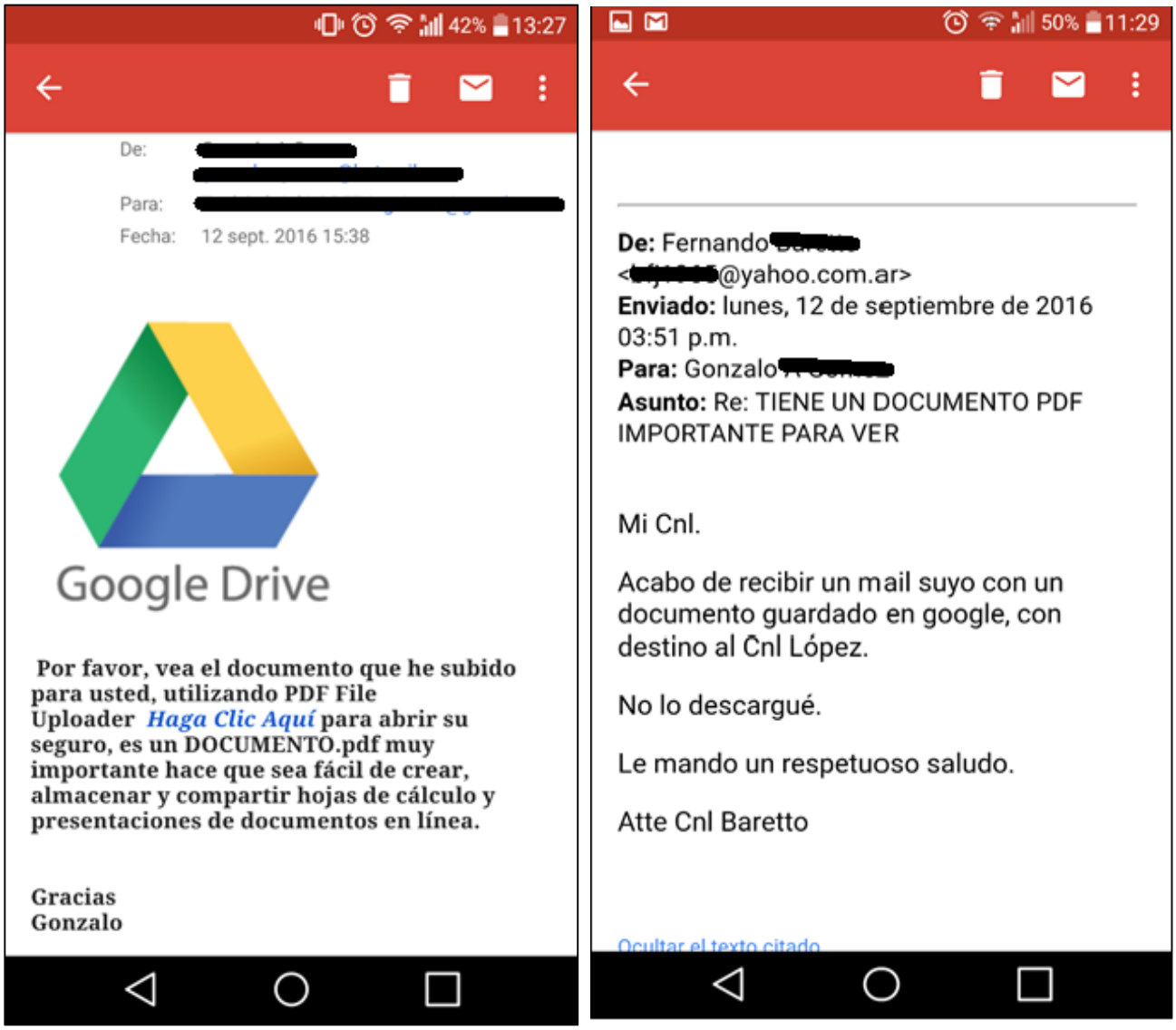
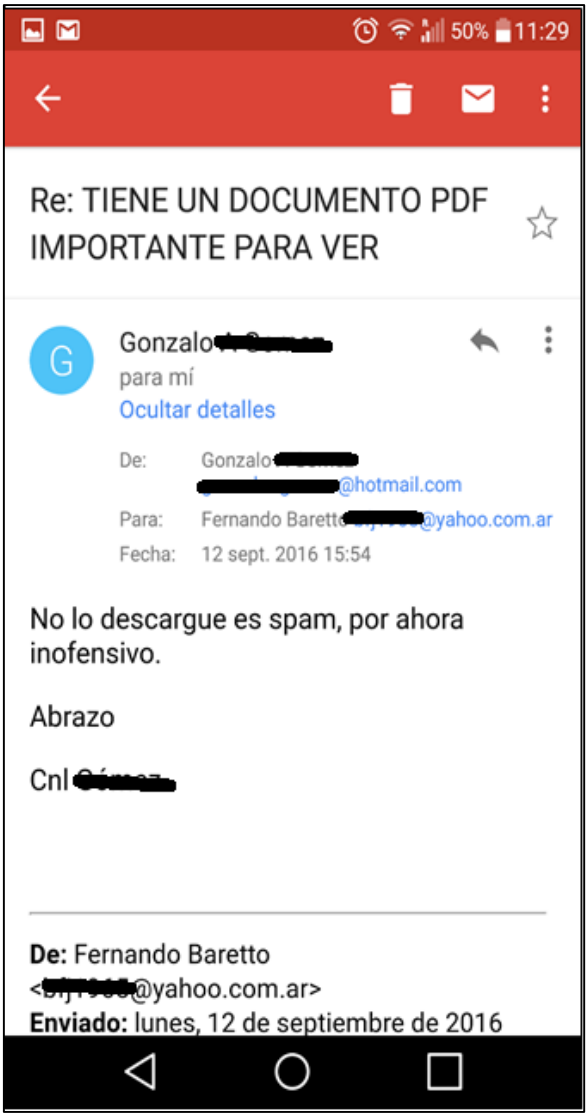


Figura 5 a 8: Ejemplo de Spam (del autor).

En forma casi simultánea y con menos de dos minutos de diferencia, se reciben correos, el primero, reiterando la autoría del correo y solicitando se acceda al enlace y el segundo, del remitente real, negando el envío del original.

En el primer caso, se asume que alguien ha intervenido la cuenta de correo del contacto conocido y no es un simple Spam, ya que la respuesta el correo propio, no es automática, sino que da indicios de una lectura previa.



NOTA: Los horarios y nivel de carga de la batería del teléfono celular, corresponden a los del momento de captura de pantalla y no a los de recepción o envío del correo.

-Denegación de servicio (en inglés DoS o Denial of Service):

Consiste en la saturación de un sitio o red multiplicando los requerimientos de acceso automáticamente desde un servidor, si el requerimiento se replica en varias computadoras simultáneamente, mediante botnet (red de robots en inglés)[17], se está ante un ataque tipo DDoS (ataque de denegación de servicio distribuido). En este tipo de ataques, cualquier ordenador o incluso servidor instalado en un país distinto al del origen del ataque, puede convertirse (y ser rastreado por ende) en un atacante no intencional.

[17] Puede encontrarse una explicación más técnica en el iguiente sitio de internet: http://ws.edu.isoc.org/data/2006/570066312448cfa2c134a4/060515.AfNOG-DNS-DDOS.pdf fecha de consulta 20 Abril 2013.

Los riesgos implícitos en ello, son elevados, toda vez que grandes potencias han anunciado públicamente la intención de responder del modo que sea necesario (incluye el uso de ataques cibernéticos y eventualmente empleo de la fuerza militar con carácter preventivo o punitorio), contra quienes originen intencionalmente o se conviertan en atacantes inconscientes.

Las formas o procedimientos de ataque son variados, aunque normalmente implican alguna o más de las siguientes acciones:

- Consumir recursos de los sistemas informáticos incluyendo el ancho de banda, espacio libre en dispositivos de almacenamiento, o tiempos de procesamiento.
- Cambios en la con configuración del sistema, incluyendo rutas de apertura de archivos, loops (reinicio de programas), etc.
- Cambios en la información de estado del sistema y redes asociadas, tales como interrupción de sesiones TCP[18].
- Alteración del funcionamiento de componentes físicos de la red (ejemplo: eliminación de los programas o drivers de hardware asociado al sistema).
- Afectación de medios de comunicación entre usuarios normales del servicio y el sistema atacado, de manera que ya no puedan enlazar adecuadamente (por ejemplo, clientes de un banco con su sistema de banca electrónica).

Entre los tipos de DoS más comunes y empleados se encuentran los ataques tipo NUKE en los que las peticiones de datos al sistema objetivo, se hacen de manera incongruente. Al no poder dar una respuesta lógica, se reitera otra petición incongruente y el propio sistema blanco del ataque, se aboca a buscarlas en forma reiterada, ocasionando con ello que se sature y deje de operar.

Otro común y no menos riesgoso es el DoS amplificado, Un ataque amplificado tiene gran efectividad, ya que agota el ancho de banda de la víctima. Por ejemplo, un ataque de DNS amplificado de solo una petición de 60 bytes del atacante, podría generar una respuesta hacia el blanco de más de 3Mb (más de 50 veces el tráfico generado por un solo atacante). Con una velocidad de conexión de por ejemplo, 6 Mbps, la víctima recibiría un caudal de 300 Mbps.

Si se realiza bajo el esquema DDoS, cabría multiplicar este número por la cantidad de

[18] Transmission Control Protocol (TCP) o Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn. https://es.wikipedia.org/wiki/Transmission_Control_Protocol fecha de consulta 16 de octubre de 2016.

zombies, generándose caudales de varios Terabytes por segundo, imposibles de gestionar por servidores pequeños a medianos (Arismendi, s.f.).

Otro tipo de ataque DoS, es el Smurf (pitufo), en el cuál el atacante, efectúa un requerimiento desde la misma dirección IP del blanco. Esto hace que el propio sistema genere respuestas a todos los usuarios conectados al mismo, ya que no distingue el origen de la primera petición. Los usuarios conectados, responden a su vez a la dirección IP inicial, generándose nuevas respuestas que terminan saturando el sistema objeto del ataque. Si bien es un tipo de ataque conocido y relativamente antiguo, no deja de ser efectivo de no disponerse de herramientas de protección adecuadas.

En los gráficos siguientes, se muestran ejemplos simplificados de un ataque DoS y DDoS. En el primero de ellos los requerimientos al blanco se realizan en forma directa. No obstante y debido al aumento en la capacidad de los servidores, se han tornado poco efectivos y su origen, resulta de fácil localización.

En el caso de un ataque DDoS, el atacante, captura a través de troyanos otras PC conocidas como zombies, las que sin el conocimiento ni el consentimiento del usuario, efectúan requerimientos al blanco hasta lograr su saturación.

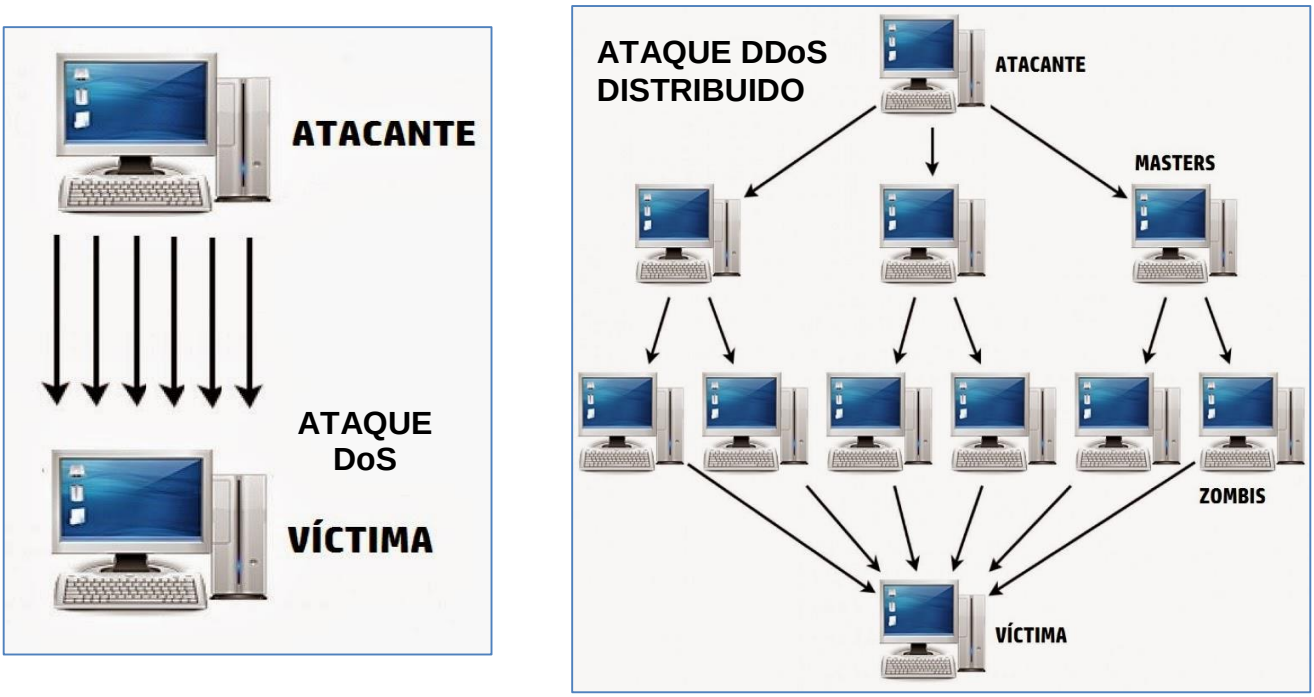


Figura 9: Esquema de ataque DoS y DDos (Tomado de http://luisarizmendi.blogspot.com.uy/2014/03/ataques-dos-y-ddos-prevencion-deteccion.html.

-Pishing[19]:

El Phishing es la obtención de información confidencial para emplearla generalmente en fraudes. Es lograda mediante Keyloggers (capturadores de teclado) y Spyware (software espía). La propagación de este último, se realiza normalmente a través de correo electrónico asociado a spam. Los más empleados, buscan recabar datos confidenciales, preferentemente relacionados con asuntos bancarios (contraseñas, números de cuenta, etc).

Simulan ser coreos electrónicos convencionales y legales de entidades bancarias o comercios y disponen de un link o enlace que redirecciona al usuario a una página web falsa en la que se solicitan datos confidenciales (por ejemplo, números de tarjeta de crédito, renovación de contraseñas, etc).

En la imagen siguiente se muestra uno de los capturadores de teclado (Keyloggers) más comunes, el REFOG. La versión gratuita de este programa, permite el registro de las teclas activadas y los archivos o sitios de internet abiertos.

Obviamente la ventana del programa permanece oculta, lo mismo que su ícono de acceso directo y solo se activa mediante el accionamiento de una secuencia o combinación de teclas de quien lo instaló.

Una vez abierto, permite ver, grabar o imprimir los comandos que alguien tipeó anteriormente, rescatándose con frecuencia contraseñas y nombres de usuario.

[19] Proviene del inglés *fishing*, acción de pescar.

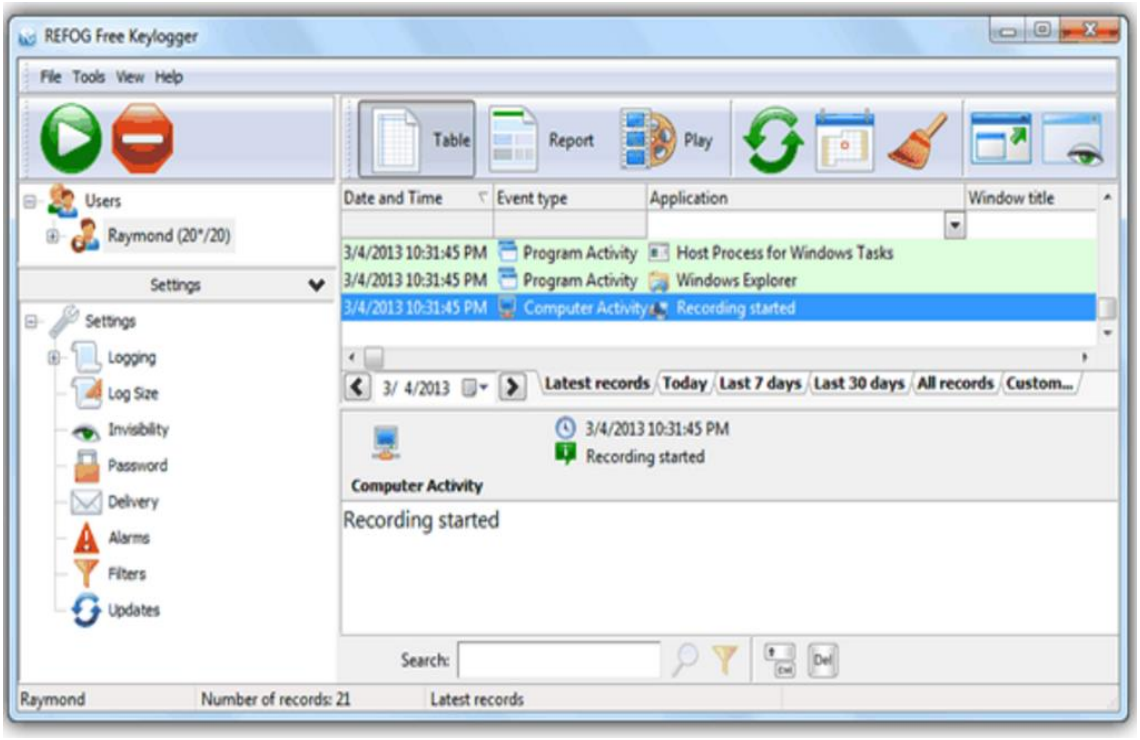


Figura 10: Pantalla de Keylogger Refog. (tomado de http://www.computerbild.de/download/Refog-Free-Keylogger-10139415.html).

La imagen siguiente (Borghello, 2015), muestra un ejemplo de un correo electrónico mediante el cual se intenta realizar phishing a partir de la difusión de un correo electrónico originado falsamente en entidades bancarias. En el extremo derecho de la imagen, se indican indicios que hacen presumir sobre la falsedad del correo y las intenciones perseguidas.

Entre los defectos más comunes, se pueden citar la mención de de un problema de gravedad en el sitio, errores de ortografía y/o gramaticales, el envío general de información e instrucciones sin un nombre definido de usuario, el requerimiento de escritura de datos, claves, etc y finalmente, un link (con la leyenda de la entidad). Este enlace redirecciona a un sitio falso (se verifica al parar el cursor sobre el enlace y verificar sin clickear, en la parte inferior izquierda del navegador, que el nombre del enlace que aparece automáticamente, corresponda con el sitio al que accederemos).

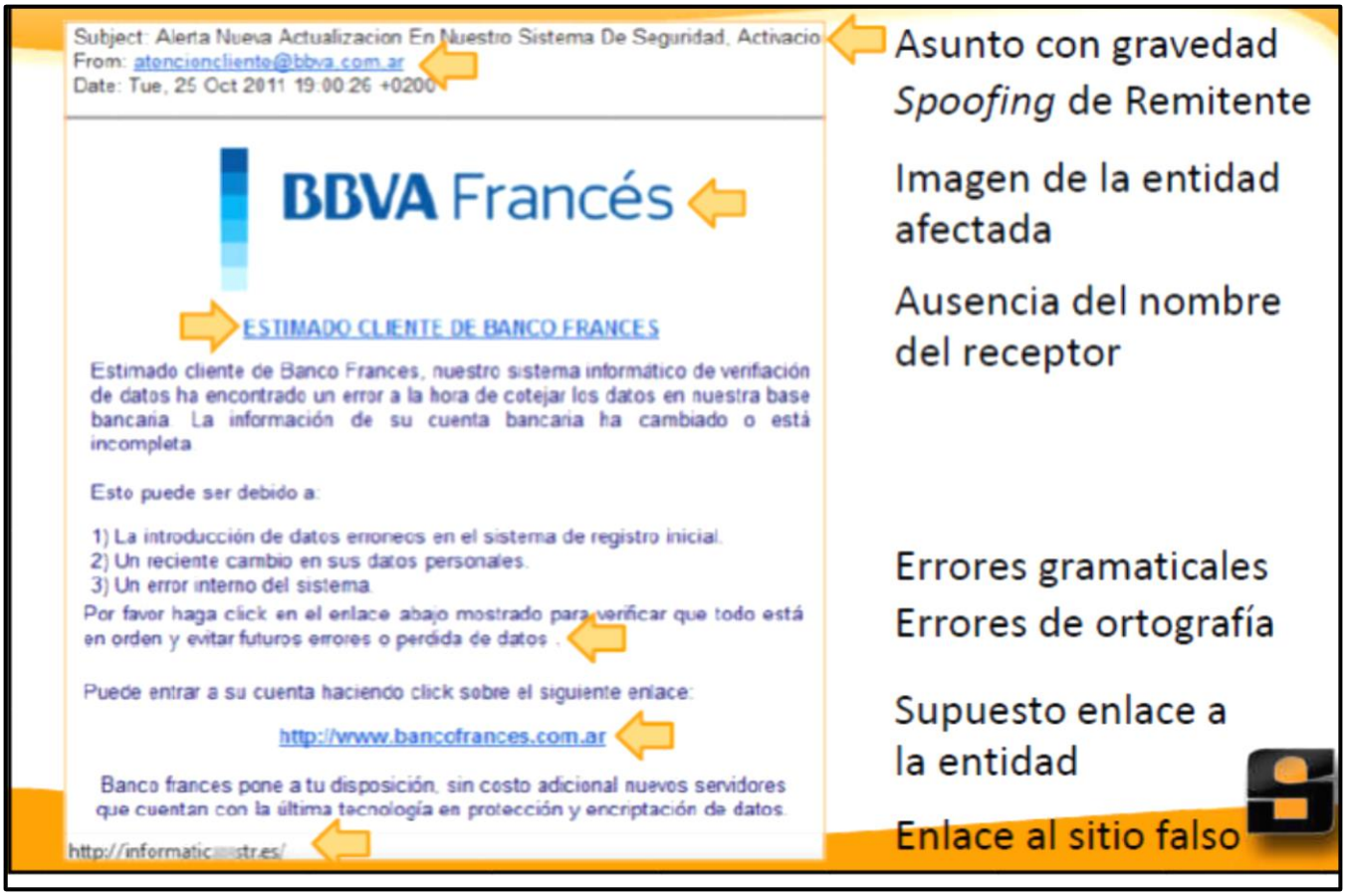


Figura 11: ejemplo de Phishing bancario (Borghello).

En los primeros días del mes de febrero de 2017, la Armada de la República Argentina, sufrió un intento de ataque de phishing, el cual buscaba a través del correo electrónico institucional, obtener datos de usuarios y contraseñas.
Dicho intento, se concretó mediante correo spam conteniendo una página web falsa. Esta página solicitaba a los usuarios, la actualización de sus datos y contraseñas.

Una vez introducidos los datos, se remitía a otro sitio en el cuál se solicitaba información adicional.

En la imagen siguiente, se muestra una captura de pantalla del correo recibido.

Cabe acotar que el diseño de la página no se corresponde con el diseño de la página oficial del Webmail de la Armada Argentina y usa imágenes, palabra y recursos no empleados por dicha institución, por ejemplo “nombre de pila”.

A la fecha, no había podido determinarse ni el origen ni el propósito de dicha acción, pero si algunos usuarios desprevenidos hubieran introducido los datos requeridos, las

consecuencias podrían haber sido de gravedad.

Figura 12: pantalla de mail oficial de la Armada Argentina hackeada mediante un intento de phishing (Dir Com Informática de la ARA).

La mayoría de los implicados en casos de phishing efectivos, corresponden a usuarios desprevenidos y con poco conocimiento sobre amenazas cibernéticas.

El último ejemplo mostrado, guarda similitud con una página de una red social de acceso por varios tipos de dispositivos (Borghello, 2015).

Figura 13: pantalla de Facebook modificada para capturar datos personales mediante Phishing (tomado de Borghello).

En la parte superior izquierda, se observa la página real y válida (Facebook.com), mientras que superpuesta, se halla una página similar, pero que enlaza a una dirección distinta (Fakebook.com). Cuando el usuario completa los datos, los envía automáticamente a un sitio que los empleará seguramente, para fines delictivos.

-Spoofing[20]:

Es la suplantación de identidad del usuario con fines delictivos o maliciosos y aunque su uso es materia de delito cibernético, su aplicación en el ámbito de la defensa resulta de alta peligrosidad[21] por la posibilidad de que se impartan órdenes, se activen sistemas, se difunda información no deseada, etc. El spoofin, conlleva serios riesgos a las capacidades defensivas de cualquier estado.

[20] Proviene del inglés *spoff*, acción de parodiar.
[21] Basta imaginar la suplantación de las identidades de los responsables del lanzamiento de misiles nucleares por hackers enemigos, para lanzarlos contra el mismo Estado o un tercero.

Una variante es el spoofing contra el servidor DNS (Domain Name System – Sistema de Nombres de Dominio). El DNS asocia nombres de dominio a direcciones IP. El atacante, modifica el servidor DNS para redirigir un nombre de dominio específico a una dirección IP diferente. En muchos casos, la nueva dirección IP corresponderá a un servidor controlado por el atacante, desde el cual, se propagarán otros tipos de malware (Veracode, s.f.).
Más adelante, se expondrá un caso que bien podría asimilarse al *spoofing*, conocido como “Operación Orchard”, el ataque israelí a la central nuclear siria de Al Kibar.

- Ransomware:
Consiste en un malware que infecta equipos variados (particulares, de organizaciones, de empresas, etc), incluyendo computadoras, sistemas de control, sistemas de seguridad, smartphones, etc. Una vez ingresado al dispositivo, codifica los archivos y programas haciendo imposible su empleo al usuario real. Quien ejecuta el ransomware, es el único en capacidad de recuperar esos datos. A partir de ello, se extorsiona a la víctima, solicitando un “rescate” (en inglés ransom) a cambio de su liberación.

Los riesgos asociados pueden ser enormes y normalmente se prefiere el pago del rescate ante la eventual pérdidas temporal o permanente de información, la interrupción de la actividad normal, las pérdidas económicas que genere y los daños a su reputación. Casi la mitad de las organizaciones en España, han sido objeto de ataques de este tipo durante el año 2016[22] y su crecimiento es exponencial dada su rentabilidad, la mayor disponibilidad de equipos y datos factibles de ser secuestrados, los avances en cifrado, la facilidad de ocultamiento de la actividad delictiva y finalmente, el uso de sistemas de pago internacionales anónimos, que dificultan su rastreo.

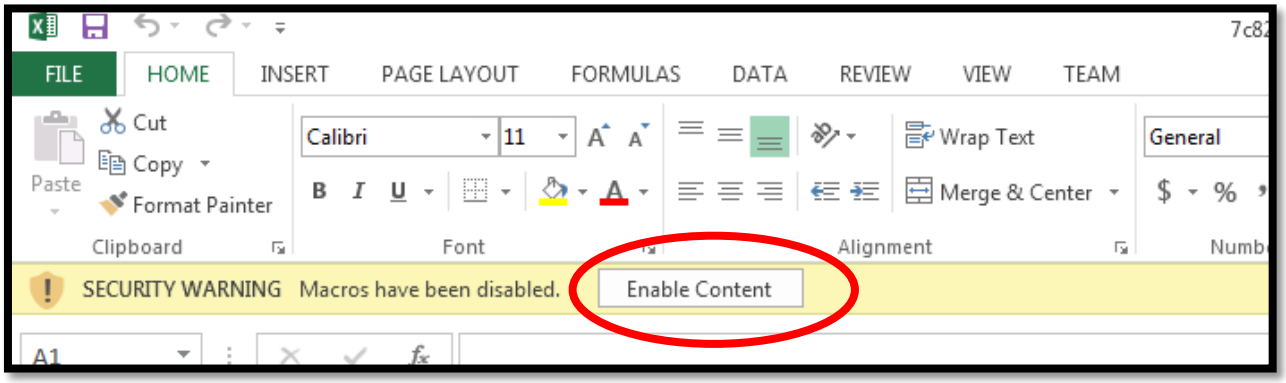
Normalmente se detecta cuando el equipo ya ha sido secuestrado, apareciendo en la pantalla un mensaje de advertencia y el pedido de rescate, el que suele incluir amenazas de destrucción de la información y plazos para realizar el pago.

Un ejemplo de ransomware se muestra en la figura siguiente:

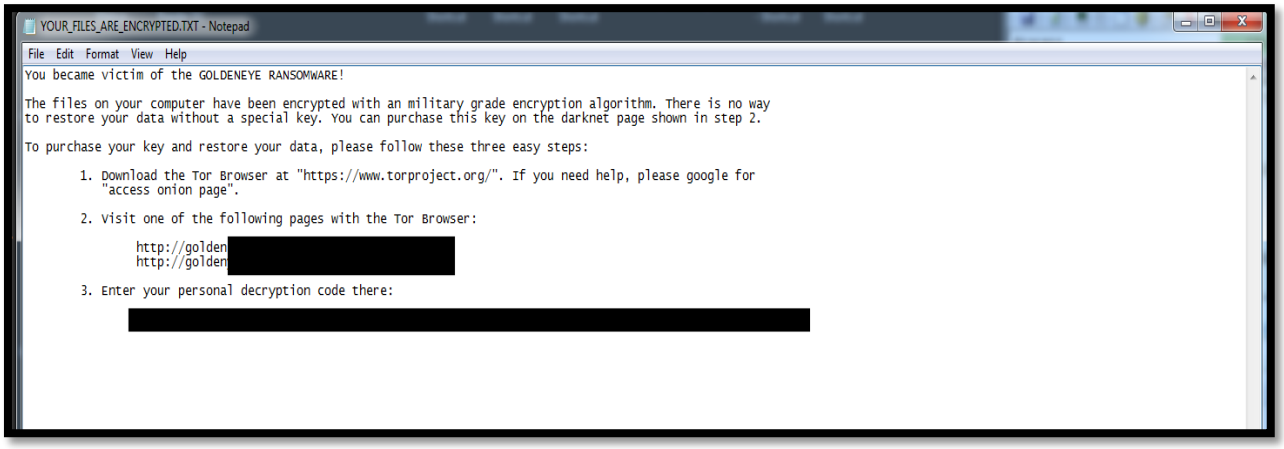
[22] Ver http://www.computing.es/ciberseguridad/informes/1094000045201/casi-la-mitad-de-las-organizaciones-sufrio-un-ataque-de-ransomware-el-ano-pasado.1.html consultado el 12 de febrero de 2017.

Figura 14 a 19: ejemplos y secuencia de ataques de ransomrware (del autor).

Otros programas ransomware son aún más vistosos y complejos, como el GoldenEye. En la secuencia de imágenes, se muestran las diferentes pantallas que se abren desde la activación del malware hasta que se realiza el pedido de rescate:
En la primer imagen, mientras se emplea un programa cualquiera (en este caso el MS Excel), sale una alerta que lleva en forma inconsciente al usuario a activar el botón “Enable Content” (Contenido Activado).



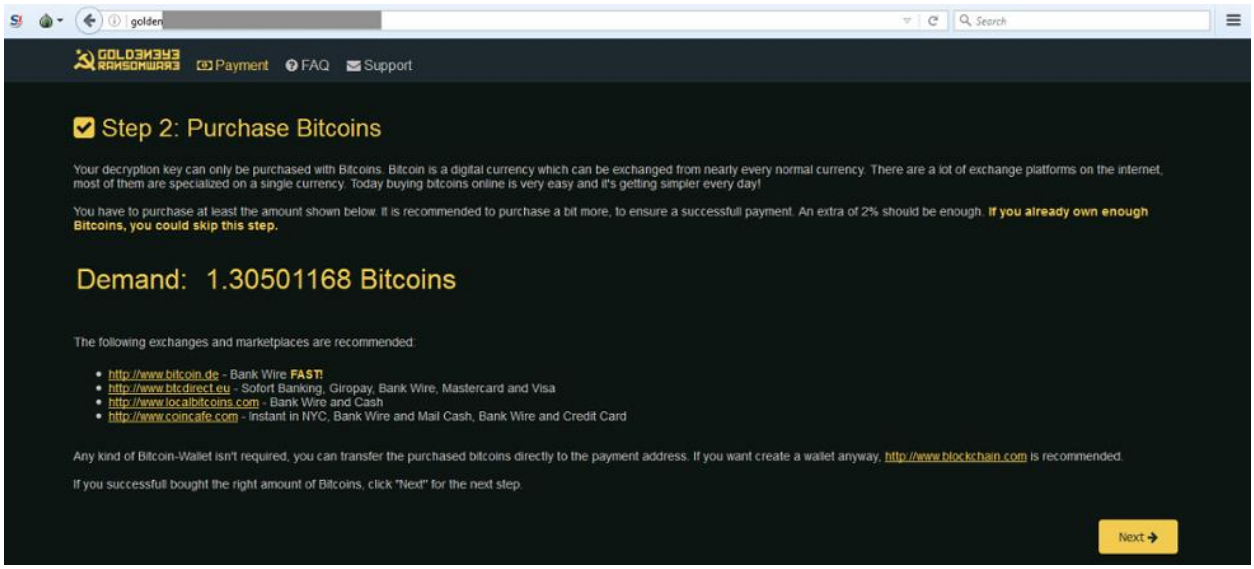
La activación de ese comando, inicia automáticamente GoldenEye, apareciendo una advertencia en formato .txt, indicando que fue víctima del malware, que los archivos han sido encriptados y que puede comprar la “llave” en una dirección web (mostrada en pantalla) de la internet profunda (Darknet) y que se descarga a partir del buscador Tor. En esa dirección figura un código para iniciar el proceso de decodificación.

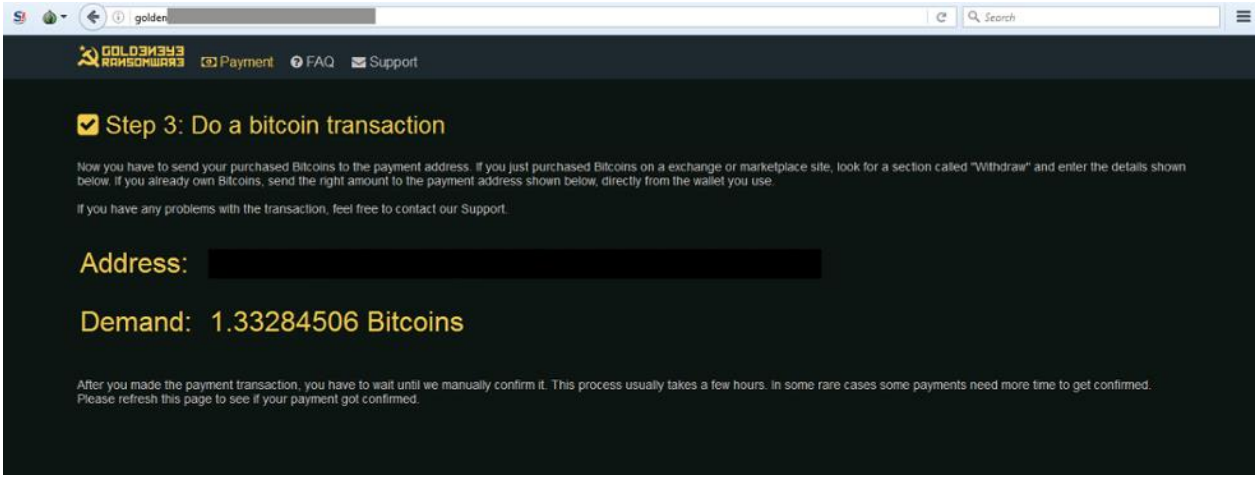


Inserto el código en la pantalla previa (ver 3.), se inicia una ventana en el sistema operativo DOS, seguida posteriormente por la imagen de una calavera y un nuevo aviso para ingresar en la Darknet para comprar la llave.

Finalmente, aparecen ventanas para realizar el pago en bitcoins[23] (monedas electrónicas) y recuperar la llave maestra que permitirá desencriptar los archivos secuestrados.

[23] BITCOIN: Es una moneda electrónica, aunque el término también se aplica al protocolo y a la red Peer Two Peer (P2P) en el que se apoya. Bitcoin opera en forma descentralizada, no siendo respaldado por ningún gobierno, Las operaciones se realizan entre usuarios y dispone de varios dispositivos de seguridad que evitan el pago doble o el fraude en caso de no prestarse el servicio por el cual se efectuó deterinado pago. No existen intermediarios para los pagos y pueden ser convertidas a monedas corrientes como Euros o Dólares en centros de intercambio. En Argentina, WideExchange.com permite el intercambio de Bitcoin y ArgenBits (una nueva moneda electrónica) por pesos argentinos y otras criptomonedas, siendo éste el primer centro de intercambio electrónico que opera bajo la modalidad de un mercado financiero como tal. El precio corriente alcanzó el 28 de enero de de 2016, era de 351,81 Euros. Ver https://www.bbva.com/es/noticias/ciencia-tecnologia/tecnologia/cuanto-vale-bitcoin/





Aunque no implican el encriptado de archivos o programas, algunos ransomware buscan la comisión del fraude y el cobro de dinero a manos de usuarios desprevenidos o culposos. Los más comunes, pretenden la imposición de multas por infracciones de tránsito, pago de derechos de autor o multas por acceso a sitios ilegales, tales como páginas pornográficas.

En el ejemplo siguiente, se muestra una pantalla desde la cual se pretende el cobro de una multa sin especificar concretamente la causa.

Figura 20: pantalla de PC atacada mediante ransomware (Del autor).

Es un intento sumamente burdo, dada la cantidad de errores ortográficos y de redacción, incluyendo la ausencia de acentos ortográficos, la denominación en otro idioma del organismo (Police Federal Argentine) y otros errores (criminal code, pago UKash, etc).

- Otros softwares perjudiciales: se incluyen en ellos a los siguientes

1) **Adware**: Muestran publicidad al usuario. La mayoría de programas adware son instalados a software distribuido gratis. La publicidad aparece en la interfaz. A veces pueden colectar y enviar los datos personales del usuario.
2) **Riskware**: No son programas maliciosos pero contienen una amenaza potencial. En ciertas situaciones ponen sus datos a peligro. Incluyen programas de administración remota, marcadores, etc.

Aunque se intentó describirlas por sus características y propósitos principales, resulta complejo aislar cada una de ellas para su clasificación, toda vez que actúan en forma complementaria y la mayoría de los programas de tipo malicioso, pueden corresponder simultáneamente a varios tipos. Así como se puede verificar, un programa diseñado para phishing, se propaga a través de spam, pudiendo actuar como un botnet a los fines de captar nueva información mediante el control de otras computadoras.

Las posibilidades de acción de los distintos tipos de malware son enormes y los límites y alcances, difíciles de definir.

En el gráfico siguiente, se observa la evolución de las distintas armas cibernéticas desde su aparición a la fecha. Sobre el eje vertical, el grado de sofisticación y sobre el eje horizontal, el tiempo transcurrido (CIO).

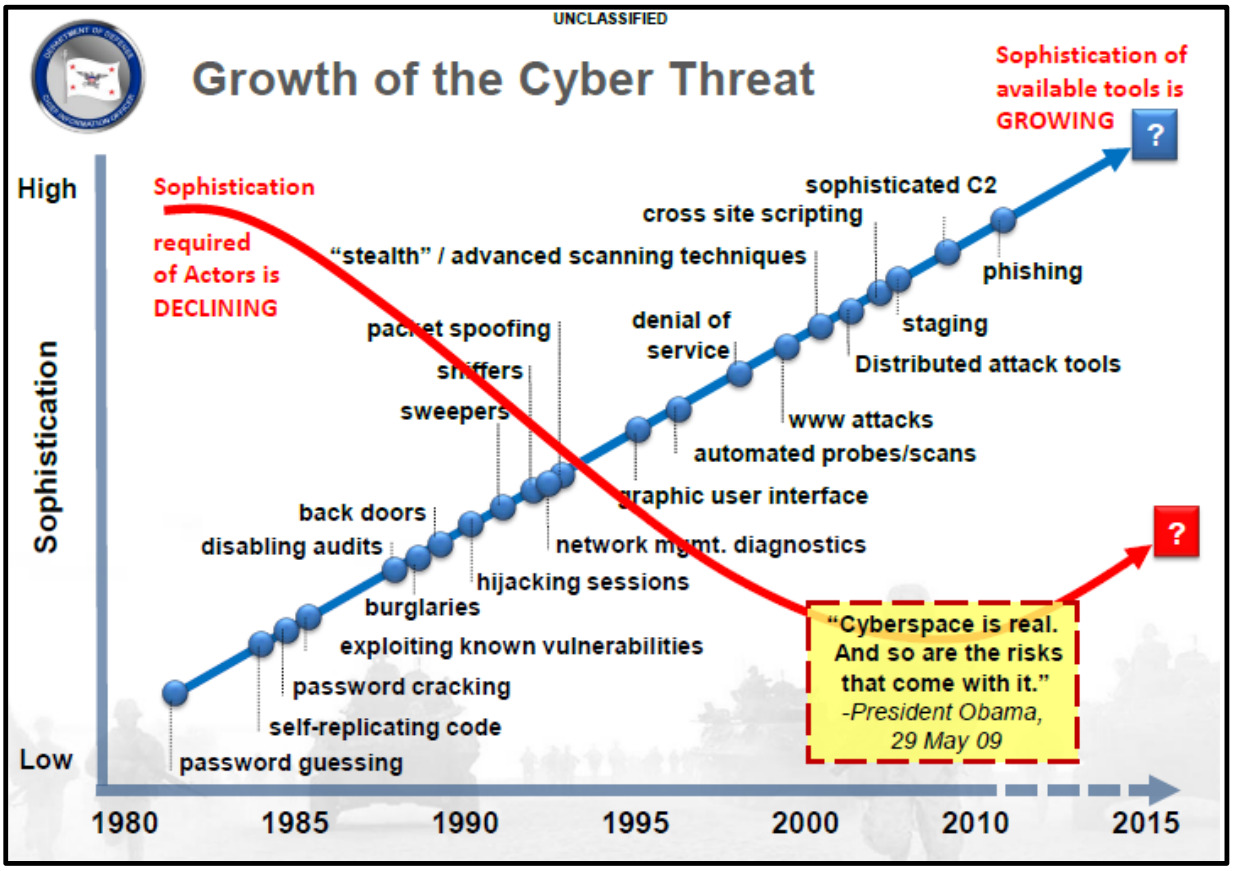


Figura 21: Evolución de las amenazas cibernéticas (Nato).

El gráfico presenta dos conclusiones importantes. Con el paso de los años, aumentó el nivel de sofisticación de las ciberarmas y herramientas disponibles, en tanto que disminuyó el nivel de sofisticación de los autores de los ciberataques (esta tendencia tiende a revertirse).

C. Algunos ejemplos de ataques cibernéticos

En la guerra cibernética, el principal problema es el desconocimiento de la magnitud del riesgo, al no registrarse aún un ataque cibernético en gran escala o de

efectos devastadores (Sánchez Medero, 2010, pág. 64). No obstante, es lógico imaginar que las guerras del siglo XXI se librarán cada día con mayor preponderancia en el espacio cibernético y seguramente serán tan efectivas como una convencional en términos de efectos de destrucción. La guerra cibernética no es ciencia ficción y todos los objetivos son rentables, aunque uno no piense así con respecto a los propios sistemas[24].

Algunos ejemplos recientes de ataques cibernéticos, ayudan a comprender la real dimensión y peligro que entraña la ciberguerra.

Entre ellos se pueden destacar la Operación Orchard mencionada previamente, el ataque cibernético la central nuclear de Natanz, en Irán, los datos reportados por el Informe Mandiant además de otras acciones menos conocidas en cuánto a su ejecución pero si en cuanto a sus efectos.

1. La Operación Orchard:

Orchard (Huerta) es el nombre en clave de la operación realizada por Israel contra el complejo nuclear sirio de Al Kibar, el 05/06 de septiembre de 2007. La central había sido construida con tecnología norcoreana.

En ese entonces, Siria disponía de dos de los sistemas antiaéreos más modernos del arsenal ruso, el sistema de misiles Tor[25] y el sistema autopropulsado mixto Pantsyr[26], asociados a una compleja red de alerta temprana, la que incluía cazas con rápida capacidad de reacción. En la noche del 5 al 6 de septiembre, y mientras 8 hombres del comando Shaldag de la Fuerza Aérea Israelí (IAF) señalaban el objetivo con sus designadores láser, 10 aviones de ataque F15 I Strike Eagle, armados con bombas guiadas por láser y misiles Maverick, escoltados por cazas F16I, destruyeron la central

[24] Esta consideración unilateral, es quizás una grave muestra de necedad, a la hora de adoptar medidas de seguridad cibernética.
[25] El Tor es conocido en occidente como SA 15 Gauntlet. Es un sistema autónomo montado sobre un chasis modificado del tanque T 72. Dispone de su propio radar de detección y de guiado, aunque se asocia a un sistema de alerta de mayor alcance. Posee 8 misiles listos para el tiro con un alcance máximo de 12 km, estando en condiciones de combatir aviones, helicópteros, UAV y otros misiles. Ver http://www.military-today.com/missiles/tor.htm
[26] El Pantsyr-S1 (designación NATO SA-22 Greyhound) es un sistema antiaéreo mixto, ya que combina 4 cañones de 30 MM y gran cadencia de tiro, con 12 misiles superficie aire 57E6, de gran velocidad. De forma similar al Tor, puede operar en forma aislada aunque normalmente se emplea en el marco de una red de defensa aérea. Se atribuye al Pantsyr, la capacidad de detectar y combatir exitosamente, aeronaves tipo Stealth (invisibles) tales como el F22 Raptor y el F35 JDF. (Military Today, 2016) http://www.military-today.com/missiles/pantsyr.htm

nuclear, ubicada en el norte de Siria a 85 km de la frontera con Irak.

Aunque la destrucción en si misma se logró mediante un ataque aéreo clásico para la época, Israel anuló el sistema de defensa aéreo sirio, mediante la ejecución aparente de operaciones cibernéticas, lográndose apoderar del control de todo el sistema de defensa aérea. Ratifica esta afirmación el hecho de que no se registraron acciones de guerra electrónica tales como CME (Contra Medidas Electrónicas), no fue detectada aeronave alguna y el sistema de C^3I^2 [27] operó con absoluta normalidad.

Son tres las opciones cibernéticas que los analistas consideraron como posibles. En primer lugar, se sugirió la posibilidad del uso de técnicas de *chipping*. Se cree que el Mossad, habría introducido chips modificados durante la fabricación de los sistemas asociados al control del espacio aéreo sirio (Marke, 2011, pág. 3). La capacidad tecnológica de Israel, hace factible la producción (y eventualmente la introducción mediante el pago de sobornos) de chips modificados que permitan la activación de backdoors. Estos programas podrían asegurar el acceso remoto y el control a voluntad de cualquier sistema informático, sin que el usuario lo percibiera.

Otras opciones, sugieren el empleo de dos técnicas adicionales de intromisión. La primera, sostiene que Israel dispone de un sistema aerotransportado en condiciones de detectar y penetrar en redes informáticas dentro de un alcance determinado. El sistema sería similar al Suter, desarrollado por EEUU y Gran Bretaña, aunque a diferencia de éste, que está montado en un avión tripulado de gran porte, los israelíes lo habrían instalado en un avión sin piloto (UAV) de tamaño mediano. El sistema Suter se ha empleado con éxito en Afganistán y las posibilidades de desarrollo de un sistema similar, por parte de Israel, encajan dentro de sus capacidades tecnológicas,

Por último, la última versión sugiere que comandos de las Fuerzas de Defensa Israelíes (IDF), detectaron y penetraron físicamente en los enlaces de fibra óptica del sistema de defensa aérea sirio y tomaron el control con programas desarrollados específicamente con esa finalidad[28]. En todos los casos, la operación habría sido ejecutada o habría tomado parte en ella, la Unidad 8200 de las IDF, elemento responsable de las acciones de guerra cibernética.

---

[27] C^3I^2 Siglas de Comando, Control, Comunicaciones, Informática e Inteligencia.
[28] Fulghum, David A. "Israel used electronic attack in air strike against Syrian mystery target", Aviation Week & Space Technology, 2007-10-08.

2. Ciberataque a la central nuclear de Busher (Irán) :

Entre junio y septiembre de 2010, un potente virus conocido como Stuxnet, atacó la central nuclear iraní de Busher en Natanz. Según expertos, Stuxnet marca el inicio de los ciberataques con daños físicos definidos.

El mayor efecto fue alcanzado el 27 de junio. Su principal objetivo, fueron los sistemas de comando y control de la central nuclear. El virus, penetró (virtualmente) en el complejo aprovechando un fallo de seguridad del sistema de control SCADA[29], dejando fuera de servicio más de cuatro mil centrifugadoras para enriquecer uranio. Aunque los daños fueron solucionados parcialmente en tres días, las consecuencias pudieron haber sido catastróficas.

Como es clásico en las operaciones en el ciberespacio, no pudo definirse el origen del ataque, aunque, parafraseando a Sánchez Medero, se cree que sólo un equipo de expertos con *"medios y el dinero suficiente y en no menos seis meses de tiempo",* pudo hacerlo.

Según analistas de la empresa de seguridad informática Kaspersky Lab, aunque el Stuxnet fue diseñado para atacar sistemas industriales, afectó también computadoras personales y de empresas en un ataque a gran escala. Se cree que perdió el control y se autodiseminó infectando computadoras, aparentemente sin daños mayores.

La primera versión efectiva, el Stuxnet A fue creada aparentemente en junio de 2009. Después de varias horas de activado, logró infectar una computadora de la empresa iraní Foolad Technic Engineering Co (FIECO), productora de sistemas de automatización para compañías industriales. Es improbable (según Kapersky Lab), que se empleara un dispositivo del tipo pendrive para infectar la computadora original.

FIECO pudo haber sido elegida por ser una especie de atajo seguro hacia el blanco final, ya que además recopilaba datos de la industria nuclear iraní. Un segundo ataque se reiteró en 2010 por la tercera versión de Stuxnet.

El blanco siguiente, fue atacado en tres oportunidades por Stuxnet B (junio de

[29] SCADA es el acrónimo de Syncronization Control And Data Adquisition. Es un sistema desarrollado originalmente por Siemens de Alemania, que permite el control y la regulación de sistemas de distinto tipo a través de la instalación de sensores a lo largo de todos sus elementos esenciales. A diferencia de los sistemas analógicos que requieren la intervención humana en distintas etapas de un proceso, para control y mantenimiento del standard de operación del subsistema, el SCADA permite el control de procesos complejos desde una central remota. Es ampliamente empleado en el control de instalaciones petrolíferas, de producción y distribución de energía eléctrica, represas, acerías, etc.

2009, marzo y mayo de 2010). El segundo ataque, inició la diseminación descontrolada del malware. La víctima fue la empresa Behpajooh Co, productora de sistemas de control automatizados y sensores, bajo licencia Siemens. Luego se registraron ataques contra otras compañías vinculadas al programa nuclear de Irán, incluyendo Mobarakeh Steel (Irán), la sudafricana NEDA (Stuxnet C) -sospechada de exportar insumos ilegales- y Control Gostar Jahed (Irán, Stuxnet D). Finalmente, Kalaye Electric Co (Irán), la mayor productora de centrifugadoras de uranio IR 1 (Stuxnet E) y todas ellas con vinculaciones con otras empresas similares en otros países.

Gracias a estas conexiones, Stuxnet inició una epidemia global, logrando infectar en 2010, corporaciones de Rusia y Bielorrusia.

"A pesar de todos los inconvenientes, el malware se las arregló muy bien para ser eficiente. Tanto así que se sus creadores lograron convertirlo en la cibersubversión más importante del planeta, inaugurando una nueva era en el mundo de las armas cibernéticas" (Kapersky Lab, 2014).

Siemens, confirmó que fueron atacados 5 dominios en Irán, mientras que la empresa de seguridad informática Symantec, reconoció que al menos 15 sitios en distintos países, fueron afectados. Solo en Irán, fueron infectadas unas 62867 computadoras (cifra considerada reducida). La tabla siguiente muestra la cantidad de sistemas infectados por Stuxnet entre el año 2009 y 2011.

País	Sistemas infectados
Irán	62.867
Indonesia	13.336
India	6.552
EEUU	2.913

Figura 22: cantidad de ordenadores afectados por Stuxnet (Siemens).

Varios especialistas consideran que Stuxnet no fue efectivo, ya que Irán incluso aumentó la producción de uranio enriquecido después del ataque. Sin embargo, esto se debió a la instalación de centrifugadoras más avanzadas con una capacidad 3 veces superior. También se cree que se buscó un efecto limitado para evitar que Irán considerara el ataque como una agresión que justificara una represalia militar (Zetter, 2014, pág. 365).

El proceso de infección se muestra en la siguiente infografía de Kaspersky Lab.

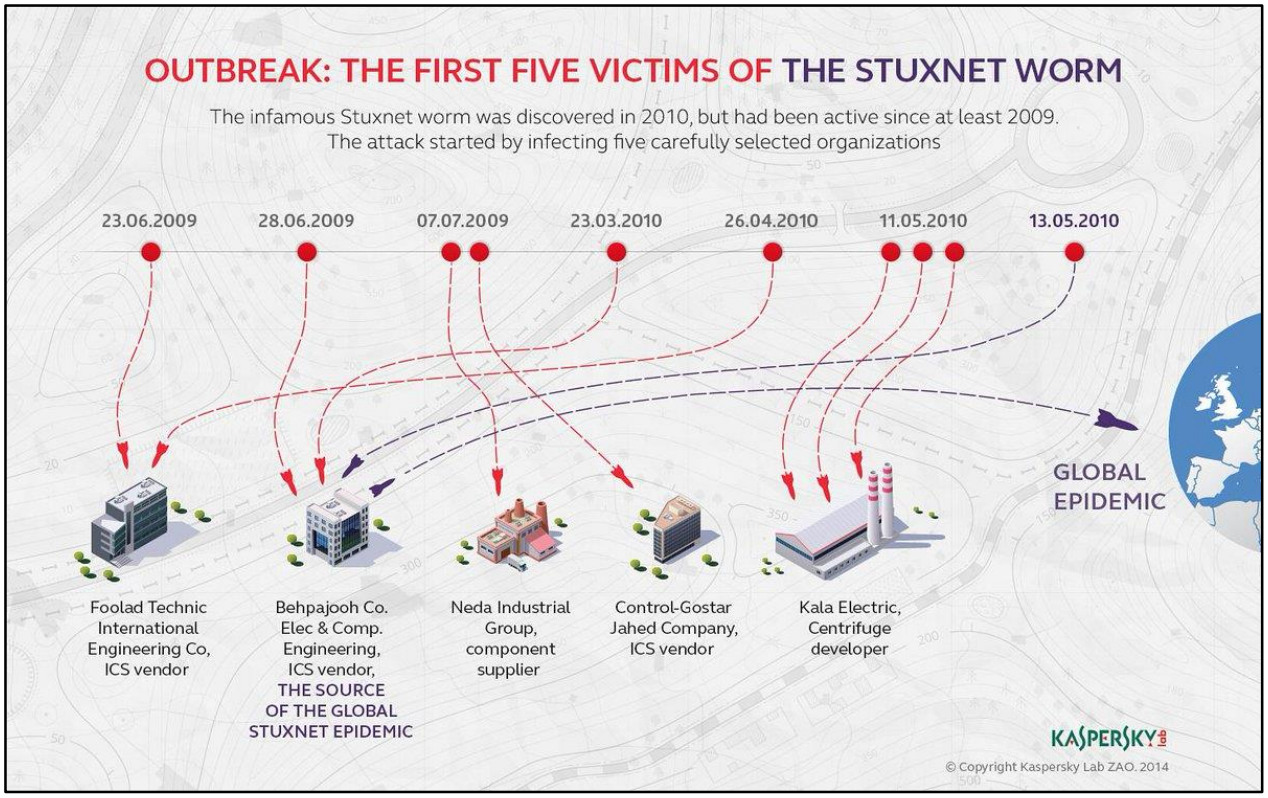


Figura 23: Proceso de infección de Stuxnet (Kaspersky Labs).

3. Los informes MANDIANT[30] APT1 y FIRE EYE APT29:

La empresa norteamericana Mandiant (hoy Fire Eye), ha investigado desde el año 2010, brechas en la seguridad en cientos de organizaciones en todo el mundo, provocadas en su mayoría por amenazas llamadas APT[31] (Amenaza Persistente Avanzada).

Las APT, representan un serio desafío para cualquier organización, ya que normalmente se desarrollan desde múltiples vectores y con variadas formas de ataque, pueden penetrar o navegar entre las programas de seguridad, penetrar la red en pocos minutos y evadir su detección y neutralización por meses (Fireeye, 2016).

[30] Mandiant: fue una empresa de seguridad informática de los EEUU, creada en 2004 por un oficial retirado de la USAF, con el nombre de Red Cliff Consulting. Adquirió el nombre de su creador en 2006, hasta ser adquirida en diciembre de 2013 por la empresa de seguridad informática Fire Eye. La empresa ha recibido numerosos galardones por su constante perfeccionamiento en materia de seguridad y por los aportes que en general ha hecho contra las ciberamenazas.

[31] Del Inglés *Advanced Persistent Threat*.

En enero de 2010, Mandiant informó sobre supuestas acciones cibernéticas chinas contra empresas y organismos de los EEUU, en tanto que en febrero de 2013, en su informe Mandiant APT 1, aportó pruebas concretas contra China.

Entre esas pruebas identificó y clasificó como APT1 a la unidad 61398 del Ejército Popular de Liberación Nacional[32].

Con alrededor de 20000 efectivos especializados en informática, esta unidad realizó desde 2006 espionaje cibernético, atacando a 141 empresas norteamericanas con más de 40 familias de malware propias. Otro tanto hizo con empresas multinacionales.

En el gráfico siguiente, extraído del informe Mandiant APT1, se muestran por país, la cantidad de empresas y organismos atacados.

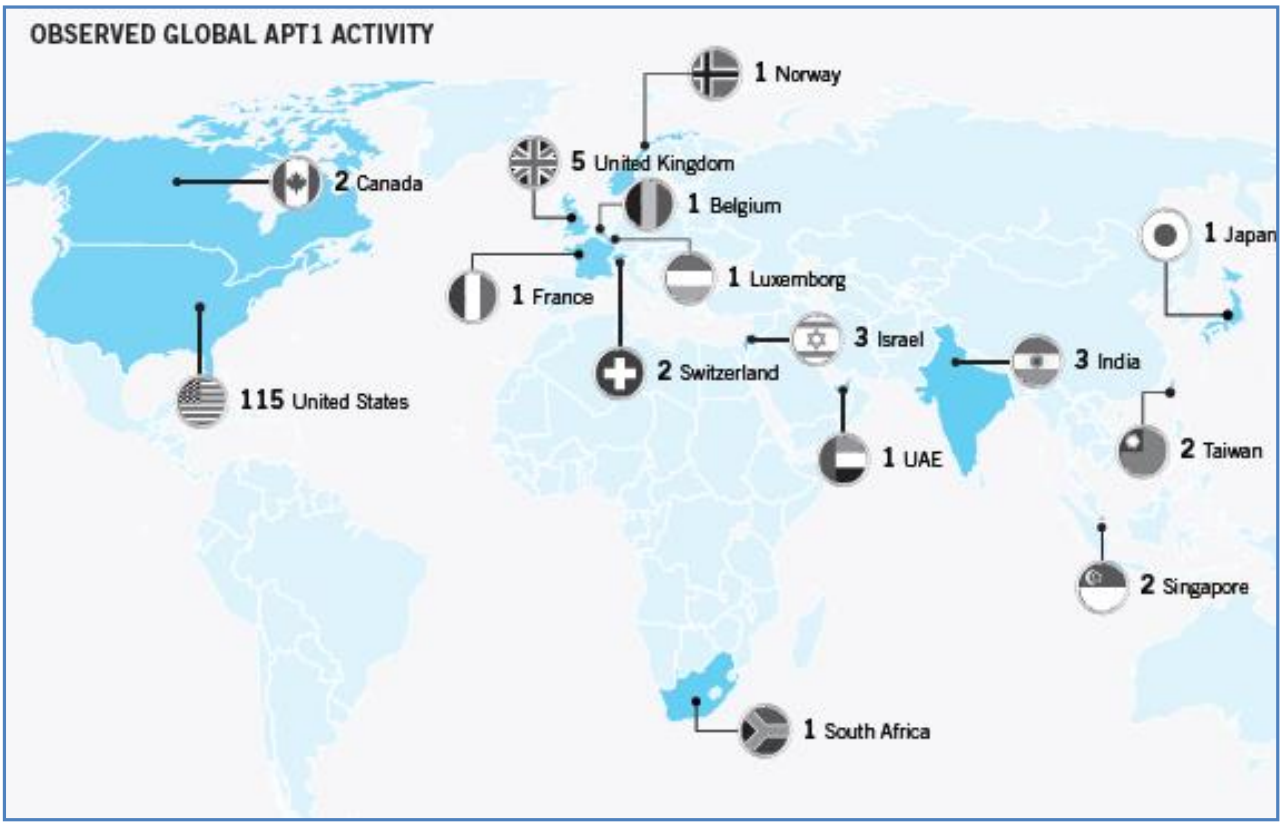


Figura 24: países atacados y cantidad de ataques (Informe Mandiant APT 1)

Las operaciones identificadas de hackers chinos más notables, fueron *Titan Rain*

[32] La naturaleza de los trabajos de la Unidad 61398 es considerada secreto de estado en China. Sin embargo, los técnicos de Mandiant pudieron determinar que realizaba operaciones en redes informáticas. La unidad tiene su comando en Datong Road, ubicada en el área de Pudong en Shangai. El edificio central de 12 pisos de alto, fue construido en 2007. Esta unidad depende directamente de la Plana Mayor 2 (equivalente al área responsable de Inteligencia en cualquier estado mayor. La empresa ChinaTelecom, provee enlaces especiales de fibra óptica e infraestructura de comunicaciones a la unidad, en nombre de la defensa nacional (Mandiant APT1).

entre 2003 y 2006, *Night Dragon* (2010 y 2011) y *Aurora* (desde 2010) (Castillo, 2013).

Night Dragon (Dragón Nocturno), consistió en la penetración de los sistemas de control y distribución de energía eléctrica de EEUU. Durante más de 6 meses, esta red fue objeto de intervenciones externas que ocasionaron fallas en el proceso de distribución y facturación, produciendo además cortes de suministros importantes en varias grandes ciudades de los EEUU.

Todas estas fallas, habrían sido ocasionadas, según Mandiant, por hackers chinos, quienes después de navegar a voluntad dentro de los sistemas, concluyeron la operación y se retiraron, dejando registros de su actividad.

En relación al tema, la empresa de seguridad informática McAfee, indicó en un informe que los hackers aprovecharon servidores de comando y control situados en Estados Unidos y servidores ubicados en Holanda. Además de las empresas energéticas de EEUU, realizaron ataques contra empresas mundiales de petróleo, gas y petroquímica, así como individuos y ejecutivos en Kazajistán, Taiwán, Grecia y Estados Unidos, obteniendo información confidencial.

Los principales recursos empleados por los atacantes consistieron en varias herramientas de hackers, algunas de ellas desarrolladas en el ámbito privado y herramientas personalizadas de RAT (*Remote Administration Too*l – Herramienta de Administración Remota) que le dieron a los hackers al atacante recursos completos de administración a distancia y la posibilidad de controlar totalmente al sistema afectado. Para instalarlas, se emplearon troyanos en los servidores de extranet de las empresas, además de ataques dirigidos de *spear-phishing* a laptops de empleados itinerantes. Una vez comprometidas algunas cuentas corporativas de VPN[33], se penetraron los sistemas de seguridad de las empresas atacadas (DMZ[34] y firewalls) para realizar el reconocimiento de las computadoras en red de esas empresas (McAfee, 2011).

Aurora, implicó la violación de casillas de correo personales y oficiales de miles de

[33] Una VPN o Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.

[34] Cuando ciertas máquinas de la red interna tienen que ser accesibles desde el exterior (servidor web, un servidor de mensajería, un servidor FTP público, etc.), normalmente es necesario crear una nueva política para una nueva red, accesible tanto desde la red interna como desde el exterior, sin correr el riesgo de comprometer la seguridad de la empresa. Se habla entonces de una "zona desmilitarizada" (DMZ para DeMilitarized Zone) para designar esta zona aislada que aloja aplicaciones a disposición del público. El DMZ sirve como una zona intermedia entre la red a proteger y la red hostil.

individuos en los EEUU (se estima en unas 10 millones de casillas de correo electrónico), para la obtención de datos confidenciales. La mayoría de ellos pertenecientes a empresarios de renombre, políticos y hombres de ciencia. La mayor cantidad de correos violados, fueron correspondientes a cuentas de Gmail, el correo electrónico de Google.

Finalmente *Titan Rain* consistió en la mayor operación de ciberespionaje conocida a la fecha.

Costosos proyectos de defensa, aeroespacio, comunicaciones e informática, fueron robados por los chinos, quienes emplearon los datos obtenidos en sus propios proyectos.

Los más notables ejemplos de la eficiencia de la operación se puede observar en el campo de la aeronáutica

Con poca experiencia en el diseño y construcción de aeronaves de caza avanzados, China había producido bajo licencia rusa, el caza Shukhoi SU27 Flanker y posteriormente, desarrolló su propia versión mejorada con componentes chinos, llamada Shengyang J11.

Sin embargo iban a ir más lejos aún y como parte de Titan Rain, realizaron exitosamente operaciones de ciberespionaje, teniendo como blanco principal al avión de combate F 35 o *Joint Strike Fighter*, el más avanzado del mundo. Su desarrollo estuvo rodeado de un enorme secreto y costó varios miles de millones de dólares (se aprecia que se invirtieron más de 13000 millones en su desarrollo).

Los chinos desarrollaron su propia versión, en menos tiempo que los norteamericanos y aunque se aprecia que sería de menor calidad y prestaciones, la relación costo beneficio de la operación resulta altamente favorable, logrando China disponer de un caza de 5ta generación, hecho igualado solo por EEUU y Rusia.

Imágenes difundidas en sitios de internet chinos, relacionados a temas de defensa, muestran entre otras noticias, los últimos diseños de alguno de sus sistemas aéreos.

Ente ellos, resultan particularmente útiles para confirmar el éxito de las actividades de espionaje cibernético chinos, unas fotografías del avión norteamericano F 35 y su gemelo chino, el caza J31 Falcon Eagle.

Las similitudes resultan más que evidentes.

Figura 25 y 26: imágenes de los JSF y J31. La fotografía inferior es un foto montaje de una futura versión naval, modificada a partir de un aterrizaje de la versión convencional (fotografías libres de internet).

En materia de copia, algo similar ocurrió con el transporte militar estratégico C17, habiendo desarrollado los chinos, una aeronave similar conocida como Y 20. Las imágenes de los originales estadounidenses y la similitud con sus versiones chinas, son

más que elocuentes.

Figura 27 y 28: imágenes de los C17 y Y20 (fotografías libres de internet).

La confirmación de las operaciones *Night Dragon* y *Titan Rain*, se puede observar en el siguiente gráfico introducido en el informe Mandiant APT1. En él se detallan, por tipo de actividad y fecha, la cantidad de ataques sufridos. Se refieren también, numerosos ataques contra empresas energéticas y otras relacionadas con el aeroespacio.

Figura 29: gráfico de ataques cibernéticos por rubro y fecha (informe Mandiant APT 1)

En julio del 2015, ya con su nombre actual “Fire Eye”, difundió otro informe conocido como “*Hammer Toss: Stealthy Tactics Define a Russian Cyber Threat Group*” (Lanzamiento de Martillo: La invisibilidad de las tácticas, define un grupo de ciberamenaza rusa). A ese grupo, lo designó con la identificación APT 29.

Según Fire Eye, APT 29 emplea una variedad de herramientas de hacking, incluyendo un algoritmo con comandos que se inserta fácilmente en archivos de imágenes de Twitter o GitHub, a partir de lo cual, puede penetrar redes y sistemas para

extraer datos de computadoras o servicios de almacenamiento en la nube (*Google Drive, DropBox, WeTransfer*, etc).

Para evitar su detección, utiliza recurso de enmascaramiento del malware o de imitación de otro software normal.

El proceso consta de cinco etapas:

a. Penetración: el grupo ATP 29 utiliza normalmente el *backdoor Hammer Toss* a través de la activación de cuentas de Twitter.
b. Reconocimiento: *Hammertoss* visita la cuenta de Twitter seleccionada y busca algún mensaje con una URL y un hashtag[35] que indica la ubicación en la web y el tamaño mínimo de un archivo de imagen a partir del cual, utilizará los códigos para descifrar su malware.
c. Captura de Imagen: a través de exploradores de internet, *Hammertoss* captura la imagen del hashtag.
d. Descifrado y contaminación: el malware inserta en la imagen un código malicioso y reemplaza la original con la modificada. Aunque parezca normal, la imagen posee un código modificado a través del cual, se iniciará el ataque mayor.
e. Ejecución y captura de datos: a través de la ejecución de los comandos insertos, el APT 29 crea un sitio de almacenamiento de datos en la nube y captura los datos de las víctimas, incluidos los de su disco duro y aquellos que suba a sitios de almacenamiento en la web.

4. Otros casos recientes:

Las acciones delictivas en el ciberespacio, han encontrado blancos muy rentables desde el punto de vista financiero. Una de las empresas más conocidas internacionalmente, dedicadas a la venta de artículos para el hogar, de construcción y otros, es Home Depot.

El día 06 de noviembre de 2014 un grupo de hackers no identificado, capturó

[35] HASHTAG: es una cadena de caracteres formada por una o varias palabras concatenadas y precedidas por una almohadilla o numeral (#). Es, por lo tanto, una etiqueta de metadatos precedida de un carácter especial con el fin de que tanto el sistema como el usuario la identifiquen de forma rápida. Si bien para los usuarios son palabras legibles, para el sistema, es un código binario.

Se usa en servicios web tales como Twitter, Telegram, FriendFeed, Facebook, Google+, Instagram, Weibo o en mensajería basada en protocolos IRC para señalar un tema sobre el que gira cierta conversación.

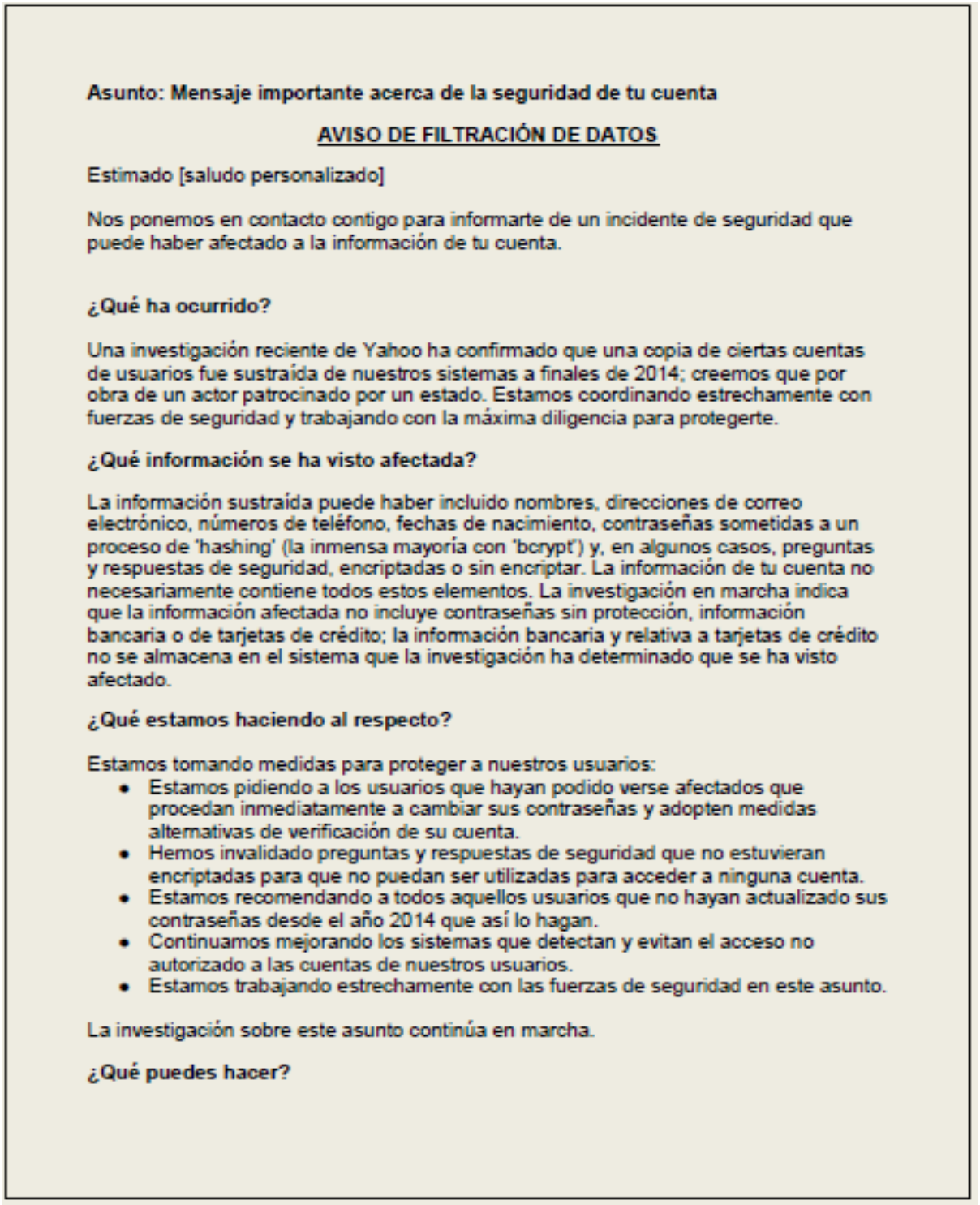
datos de tarjetas de crédito y direcciones de correo electrónico de entre 53 y 56 millones de clientes. Según lo informado por la compañía, los hackers habrían penetrado la red de intranet de la empresa a través de la contraseña y nombre de usuario de un proveedor.

Un caso similar ocurrió con la compañía Target, otro minorista estadounidense que fue atacado por hackers en diciembre de 2013. Target señaló que filtraron pagos y datos personales de hasta 70 millones de clientes[36].

En diciembre de 2016, Yahoo reconoció que sufrió un "hackeo" que afectó a 1.000 millones de cuentas de usuario[37]. Ya en 2013 había sido objeto de un ataque similar. Lo extraño de este último ataque, es que sucedió en el medio del proceso de adquisición de Yahoo (sólo de sus negocios principales) por parte de la empresa de comunicaciones Verizon, ocasionando una caída del precio pactado de 4800 millones de dólares al finalmente pagado de 4480, unos 320 millones menos de lo que se ofertó inicialmente.

El mensaje difundido por Yahoo entre sus usuarios fue el siguiente:

[36] http://www.bbc.com/news/world-us-canada-29946792 consultado el 10 de noviembre de 2015.
[37] http://www.bbc.com/mundo/noticias-38324372 consultado el 16 de diciembre de 2016.



Asunto: Mensaje importante acerca de la seguridad de tu cuenta

AVISO DE FILTRACIÓN DE DATOS

Estimado [saludo personalizado]

Nos ponemos en contacto contigo para informarte de un incidente de seguridad que puede haber afectado a la información de tu cuenta.

¿Qué ha ocurrido?

Una investigación reciente de Yahoo ha confirmado que una copia de ciertas cuentas de usuarios fue sustraída de nuestros sistemas a finales de 2014; creemos que por obra de un actor patrocinado por un estado. Estamos coordinando estrechamente con fuerzas de seguridad y trabajando con la máxima diligencia para protegerte.

¿Qué información se ha visto afectada?

La información sustraída puede haber incluido nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento, contraseñas sometidas a un proceso de 'hashing' (la inmensa mayoría con 'bcrypt') y, en algunos casos, preguntas y respuestas de seguridad, encriptadas o sin encriptar. La información de tu cuenta no necesariamente contiene todos estos elementos. La investigación en marcha indica que la información afectada no incluye contraseñas sin protección, información bancaria o de tarjetas de crédito; la información bancaria y relativa a tarjetas de crédito no se almacena en el sistema que la investigación ha determinado que se ha visto afectado.

¿Qué estamos haciendo al respecto?

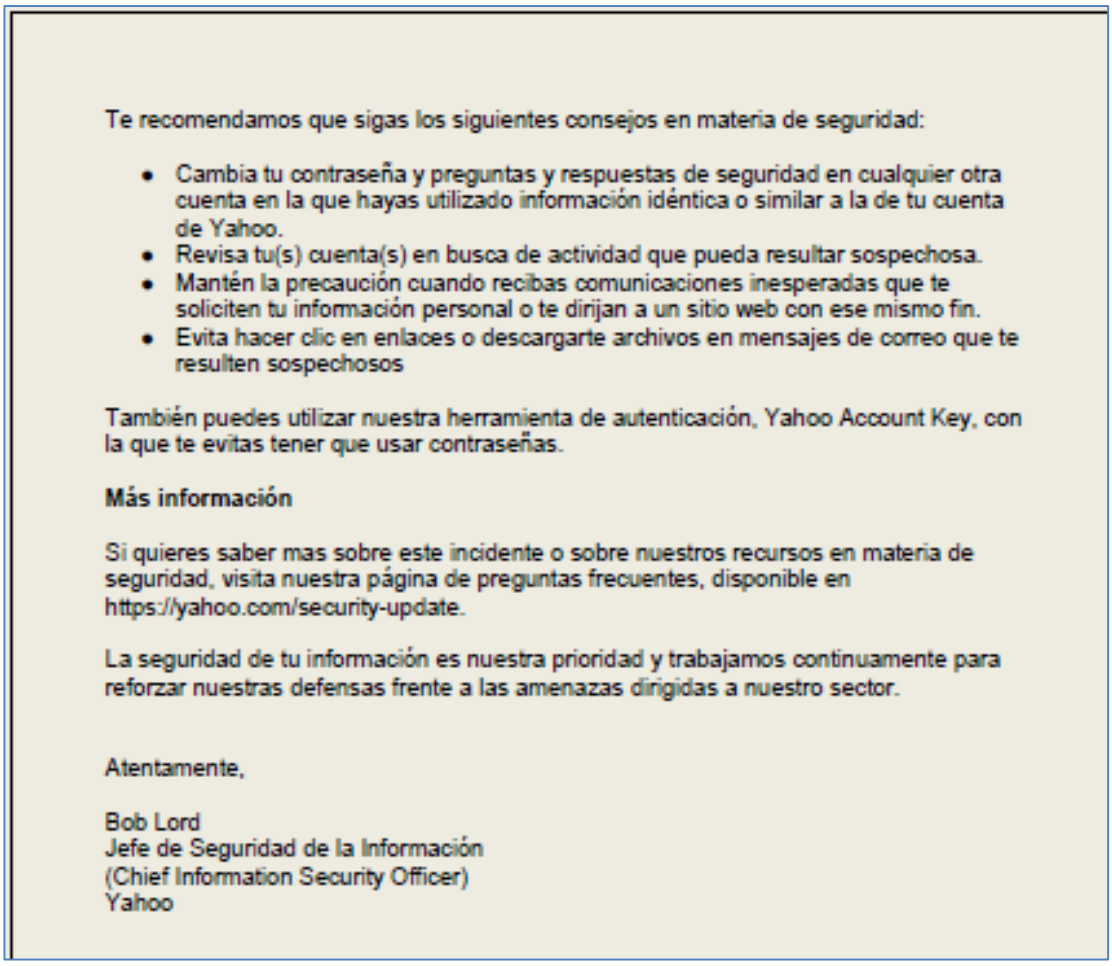
Estamos tomando medidas para proteger a nuestros usuarios:

- Estamos pidiendo a los usuarios que hayan podido verse afectados que procedan inmediatamente a cambiar sus contraseñas y adopten medidas alternativas de verificación de su cuenta.
- Hemos invalidado preguntas y respuestas de seguridad que no estuvieran encriptadas para que no puedan ser utilizadas para acceder a ninguna cuenta.
- Estamos recomendando a todos aquellos usuarios que no hayan actualizado sus contraseñas desde el año 2014 que así lo hagan.
- Continuamos mejorando los sistemas que detectan y evitan el acceso no autorizado a las cuentas de nuestros usuarios.
- Estamos trabajando estrechamente con las fuerzas de seguridad en este asunto.

La investigación sobre este asunto continúa en marcha.

¿Qué puedes hacer?

Figura 30 y 31: Advertencia del sitio Yahoo a sus usuarios, sobre que ha sido hackeado. La imagen fue levantada del sitio oficial en 2015.



Te recomendamos que sigas los siguientes consejos en materia de seguridad:

- Cambia tu contraseña y preguntas y respuestas de seguridad en cualquier otra cuenta en la que hayas utilizado información idéntica o similar a la de tu cuenta de Yahoo.
- Revisa tu(s) cuenta(s) en busca de actividad que pueda resultar sospechosa.
- Mantén la precaución cuando recibas comunicaciones inesperadas que te soliciten tu información personal o te dirijan a un sitio web con ese mismo fin.
- Evita hacer clic en enlaces o descargarte archivos en mensajes de correo que te resulten sospechosos

También puedes utilizar nuestra herramienta de autenticación, Yahoo Account Key, con la que te evitas tener que usar contraseñas.

Más información

Si quieres saber mas sobre este incidente o sobre nuestros recursos en materia de seguridad, visita nuestra página de preguntas frecuentes, disponible en https://yahoo.com/security-update.

La seguridad de tu información es nuestra prioridad y trabajamos continuamente para reforzar nuestras defensas frente a las amenazas dirigidas a nuestro sector.

Atentamente,

Bob Lord
Jefe de Seguridad de la Información
(Chief Information Security Officer)
Yahoo

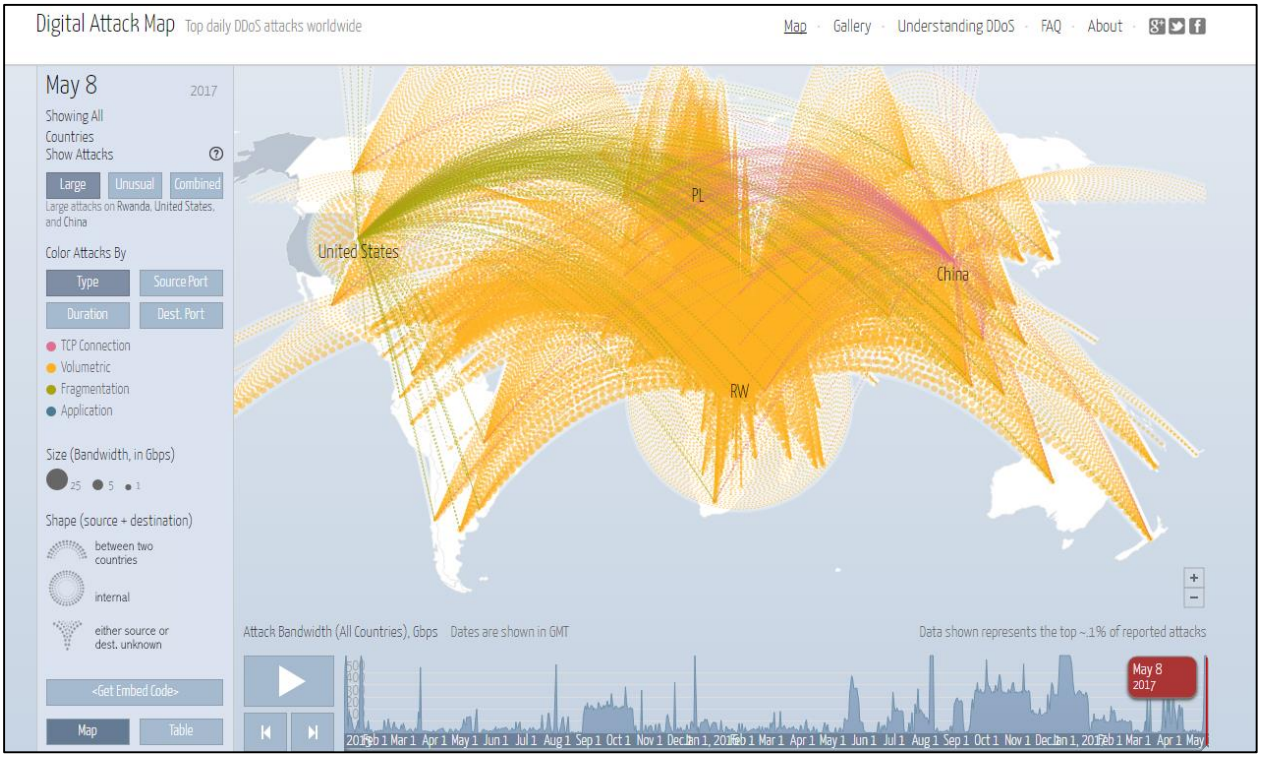
En el conflicto entre Rusia y Estonia originado por la demolición del monumento al soldado soviético de la Segunda Guerra Mundial, en Tallinn, hackers rusos realizaron un ataque masivo a organismos gubernamentales de Estonia entre el 24 de abril y el 18 de mayo de 2007. Hechos similares ocurrieron durante el conflicto entre Rusia y Georgia (agosto de 2008) y durante el conflicto con Ucrania (iniciado el 23 de febrero de 2014).

En este último, distintos ciberataques aparentemente originados en Rusia, complementaron operaciones de tropas convencionales y fuerzas especiales rusas en apoyo a separatistas ucranianos[38]. Esta modalidad de combinar medios cibernéticos con operaciones de fuerzas especiales y otras convencionales, encaja perfectamente dentro de las nuevas modalidades de guerra, denominadas “Guerras híbridas o de 4ta generación”, tal como se mencionara precedentemente.

No obstante, el problema no queda agotado en acciones como las mencionadas. Millones de computadoras personales, estatales y privadas, son penetradas diariamente.

[38] Ver http://www.bbc.co.uk/mundo/noticias/2014/03/140306_tecnologia_guerra_cibernetica_rusia_ucrania_aa.shtml

A modo de muestra, existe un mapa interactivo en la Web que informa diariamente, la detección de ataques cibernéticos y que puede ser consultado en el sitio: http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16273&view=map



Figuras 32: captura de pantalla de un mapa en tiempo real de ciberataques.

Mapas similares pueden encontrarse en los siguientes sitios:

1. https://www.fireeye.com/cyber-map/threat-map.html
2. https://threatmap.fortiguard.com/

Entre otros datos puede mencionarse como ejemplo, la penetración en 1996 de archivos secretos del Pentágono, por parte de un hacker argentino de 18 años, hecho que fuera denunciado y juzgado por EEUU[39]. En este caso, Julio César Ardita, irrumpió en computadoras que contenían información confidencial en el Centro Naval de Control y Vigilancia Oceánica, a través de un servidor de la empresa de comunicaciones Telecom, y aunque no destruyó ni se apropió de información con fines delictivos, su caso fue resonante.

[39] Lawrence Greenberg y otros, *Information Warfare and International Law*, National Defense University, Institute for National Strategic Studies, 1997, P. 27. El texto mencionado puede ser consultado en: http://www.dodccrp.org/files/Greenberg_Law.pdf

Según un informe del U.S Cybercom[40], el 27 % de las computadoras en los EEUU, fueron afectadas seriamente por ataques cibernéticos. Existen unas 68000 herramientas de hacking y los *botnets*, envían diariamente unos ochenta y nueve mil millones de mails (AFCEA, 2012).

Desde el año 2013, el informe anual "*Statement for the Record Worldwide Threat Assessment of the US Intelligence Community - Senate Armed Services Committee*" (Declaración de la Evaluación Mundial de Amenazas de la Comunidad de Inteligencia de los Estados Unidos), ubica a las amenazas cibernéticas en primer lugar respecto a los tres intereses vitales de los EEUU[41].

Se definen los tipos de amenaza y se identifican en orden de peligrosidad a Rusia, China, Irán, Corea del Norte y actores no estatales, como los principales actores que ejecutan operaciones cibernéticas contra los Estados Unidos.

Con respecto a Rusia, en su edición de 2015, enfatiza que "el Ministerio de Defensa está creando su propio comando cibernético…el cual será responsable de conducir ciberacciones ofensivas, incluyendo operaciones de propaganda, e introducción de malware en los sistemas de comando y control enemigos"[42] (Clapper, 2015, pág. 17)[43].

La preocupación de la gravedad de la amenaza, alcanza incluso a sistemas de armas individuales. La empresa norteamericana Raytheon, está desarrollando un sistema para la detección de intrusiones cibernéticas para pilotos de aeronaves, tanto civiles como de combate, aunque el esfuerzo inicial se centra en la protección del caza de 5ta generación F35. Se han detectado varias vulnerabilidades de los sistemas informáticos y del software del avión.

La posibilidad de que hackers ataquen sus sistemas de navegación, lanzamiento de armas, de conciencia situacional y logístico, hacen imperioso el desarrollo de este

[40]United States Cyber Command. Se describe más adelante.

[41] Los tres intereses son: la defensa del territorio de los EEUU, la conclusión victoriosa de una guerra que pueda afectar los intereses de los EEUU en cualquier lugar del mundo y la libertad de acción para operar en los Global Commons (dominios globales), mar, aire y espacio exterior, lugares en donde se desarrolla el comercio internacional y las actividades humanas relacionadas.

[42] "Russia. Russia's Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems."

[43] En los capítulos siguientes se desarrolla la organización, misión y funciones del Cybercommand y otras organizaciones dependientes.

sistema de detección de ciberamenazas. “Disponer de un sistema que pudiera alertar al piloto que su avión está sufriendo un ciberataque, antes de que este ocasione daños a la aeronave, podría significar una capacidad significante y vital” (Fein, 2017). La empresa está desarrollando asimismo, una versión para vehículos terrestres.

La Organización del Tratado del Atlántico Norte (OTAN), en la misma dirección seguida por el principal aliado de la organización, está aumentando su enfoque en la lucha contra las actividades de guerra híbrida rusa, sin dejar de lado la esperanza de que las relaciones con el gobierno de Moscú mejoren. (Willett, 2017).

La representante permanente de la delegación del Reino Unido ante la OTAN, embajadora Sarah MacIntosh, mencionó ante el Royal United Services Institute (RUSI – Instituto Real de los Servicios Unidos), que la guerra híbrida se había convertido en el mayor desafío para la seguridad desde la Cumbre de Gales en 2014. Según MacIntosh, desde la crisis de Ucrania, y otras crisis estatales o no estatales recientes en 2014, la comunidad internacional había visto surgir a la guerra híbrida como una nueva forma de enfrentamiento, incluyendo una intensificación de las intrusiones y ataques cibernéticos.

La guerra híbrida se convirtió en uno de los más importantes desafíos en el trato con los rusos, siendo la guerra cibernética, la parte central de esa nueva forma de operaciones.

Para MacIntosh, la guerra cibernética significa “el fin de la protección geográfica contra la amenaza, la cual ahora está a un click de distancia”[44].

Según la embajadora, desde 2014, la NATO ha dado tres importantes pasos en la arena cibernética[45]: en primer lugar, ha definido que un ciberataque, puede alcanzar el nivel del uso de la fuerza armada, en segundo lugar, la promesa de todos los aliados de mejorar la capacidad defensiva individual y colectiva contra estas amenazas y finalmente, la consideración del ciberespacio como un nuevo ambiente operacional.

El paso siguiente, sería determinar cómo disuadir a los ataques cibernéticos y cómo usar una capacidad ofensiva cibernética para disuadir a otras formas de ataques. Una pregunta clave para MacIntosh, es “¿cómo disuadir los ataques que no puedes

[44] “Cyber warfare, said MacIntosh, means “the end of geographical protection from the threat, wich is “now just a click away”.
[45] “Arena cibernética” en referencia al campo de combate en el ciberespacio.

atribuir, usando armas que no puedes demostrar?[46].

Argentina es también origen y blanco de ataques cibernéticos. En los últimos veinte años, A modo de ejemplos se pueden mencionar los siguientes:

- El 24 de octubre de 2016 y por espacio de más de 24 horas, fueron hackeados varios sitios del Poder Judicial de la Nación, bloqueándose el acceso. Se presume que habrían sido modificadas, varias causas tramitadas digitalmente[47].
- El 31 de mayo de 2016, se informó sobre una filtración de datos procesales mediante "31.300 accesos remotos", es decir hackeos, que derivaron en la obstaculización de procedimientos judiciales en el Juzgado Federal de Paso de los Libres (Corrientes). Posteriormente se informó que obedeció a una falla técnica, aunque nunca se desmintió que los procesos fueron obstaculizados y en qué modo[48].
- El 20 de abril de 2014, la empresa La Barranca SRL, grupo propietario de estaciones de servicio en varias localidades de Córdoba, denunció ante la Justicia que fue objeto de una extorsión informática. Desde el exterior, un hacker con el seudónimo “Jack Williams”, le encriptó todos los archivos de sus sistemas debiendo pagar un rescate de 2.500 dólares para recibir las claves que les permitieron desbloquear sus datos y registros contables[49].
- El 19 de julio de 2017, la página oficial del Ejército Argentino, fue hackeada mediante el reemplazo de las imágenes de la página de inicio, por otras en las que se reivindicaba el accionar de Estado Islámico (ISIS), al tiempo que se diseminaba una amenaza acerca de próximas acciones terroristas en el país.
  Si bien desde la fuerza se informó que no habían sido penetradas las redes internas, dicha página permite el acceso al correo webmail, a partir del cual, es factible acceder a la intranet.

Estos son solo algunos ejemplos, cada día en aumento.

---

[46] The nex step, MacIntosh said, “is determinig how to deter cyberattacks and how to use an offensive cyber capabilities to deter other forms of attacks. A key question she continued is how to deter attacks you can not attribute , using weapons you can not demonstrate. A key question she continued is how to deter attacks you can not attribute , using weapons you can not demonstrate.

[47] http://tn.com.ar/politica/hackearon-la-red-del-poder-judicial-de-la-nacion_749312 consultada el 05 de enero de 2017.

[48] http://www.lavoz.com.ar/sucesos/detectaron-31300-hackeos-al-juzgado-federal-de-paso-de-los-libres consultada el 25 de junio de 2016.

[49] http://www.lavoz.com.ar/ciudadanos/empresa-de-rio-cuarto-tuvo-que-pagar-rescate-por-sus-datos-tras-un-ataque-hacker consultada el 14 de abril de 2016.

De hecho y según lo informara el diario Clarín el 28 de octubre de 2016, Argentina está entre los países que sufren más ciberataques bancarios, figurando décimo en un ránking mundial[50].

Según el periódico, “desde la Unidad del Cibercrimen de la Ciudad advierten que los delitos más comunes son los robos de números de tarjetas de crédito y de las contraseñas que se usan para ingresar a las cuentas”.

Sin identificar al informe mencionado en el diario, resulta probable que no sea del todo cierto y se encuentre por debajo de ese ranking.

En el siguiente mapa de ataques en tiempo real de Kaspersky, tomado el 13 de mayo de 2017, Argentina figuraba en el ranking 23 a nivel mundial (inmediatamente detrás de Japón) y en el 5to lugar en América, detrás de Estados Unidos, Brasil, México y Colombia.

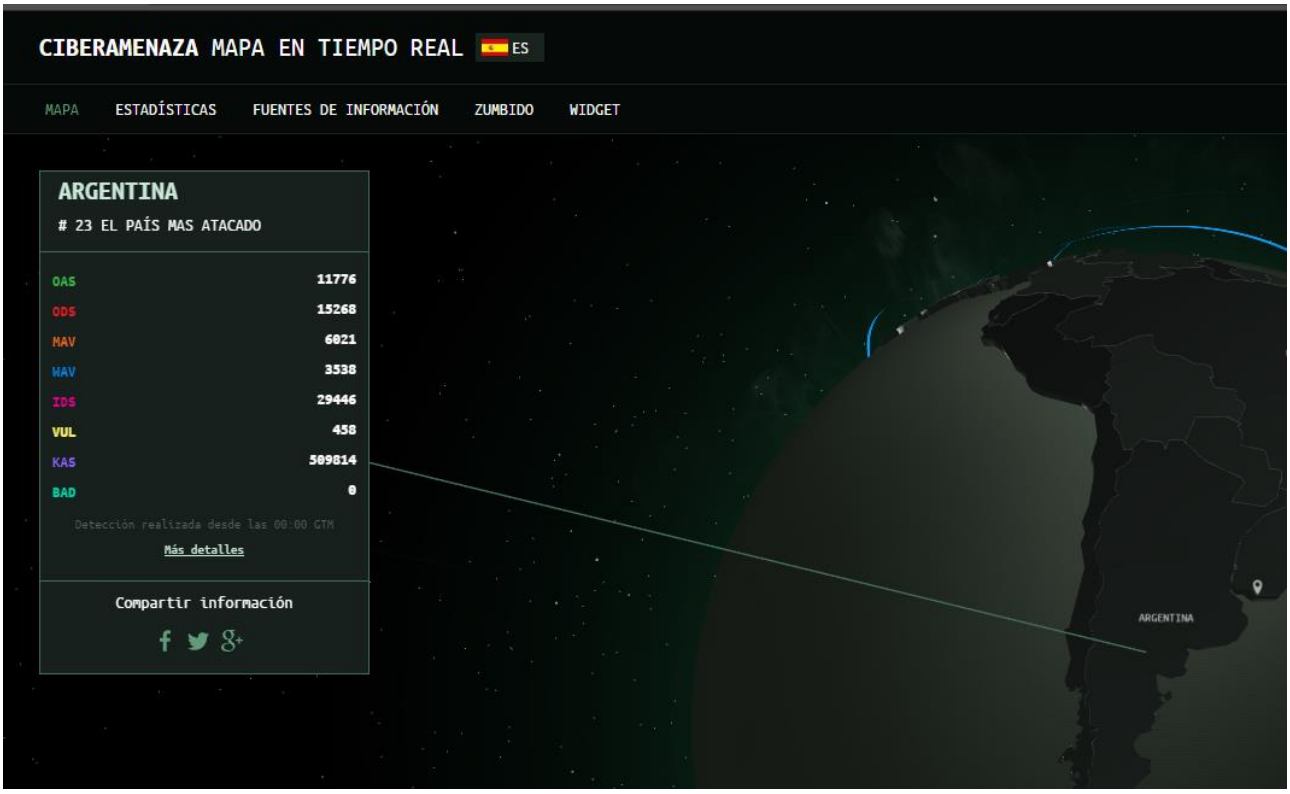


Figura 33: captura de pantalla del mapa en tiempo real de ciberataques de Kaspersky Lab, con el índice de ataques sufridos por Argentina.

[50] https://www.clarin.com/sociedad/Argentina-paises-sufren-ciberataques-bancarios_0_SkqThrVA.html .

Rusia figura para Kaspersky como el más atacado, lo cual puede resultar de algún modo engañoso, toda vez que esta empresa es de origen ruso.

Por su parte, la empresa Check Point Software Technologies Ltd., en su mapa digital referido a Argentina, reportó en el mes de mayo de 2017, lo siguiente[51]:

- El promedio de infecciones en relación a la cantidad de sistemas conectados a Internet, fue en todos los casos inferior a 0.22 %, una tasa considerada baja por los expertos.
- La mayoría de los ataques se produjeron a través de bots, o programas malignos diseñados para desarrollar tareas específicas en las computadoras.
- Estados Unidos, fue el principal país atacante

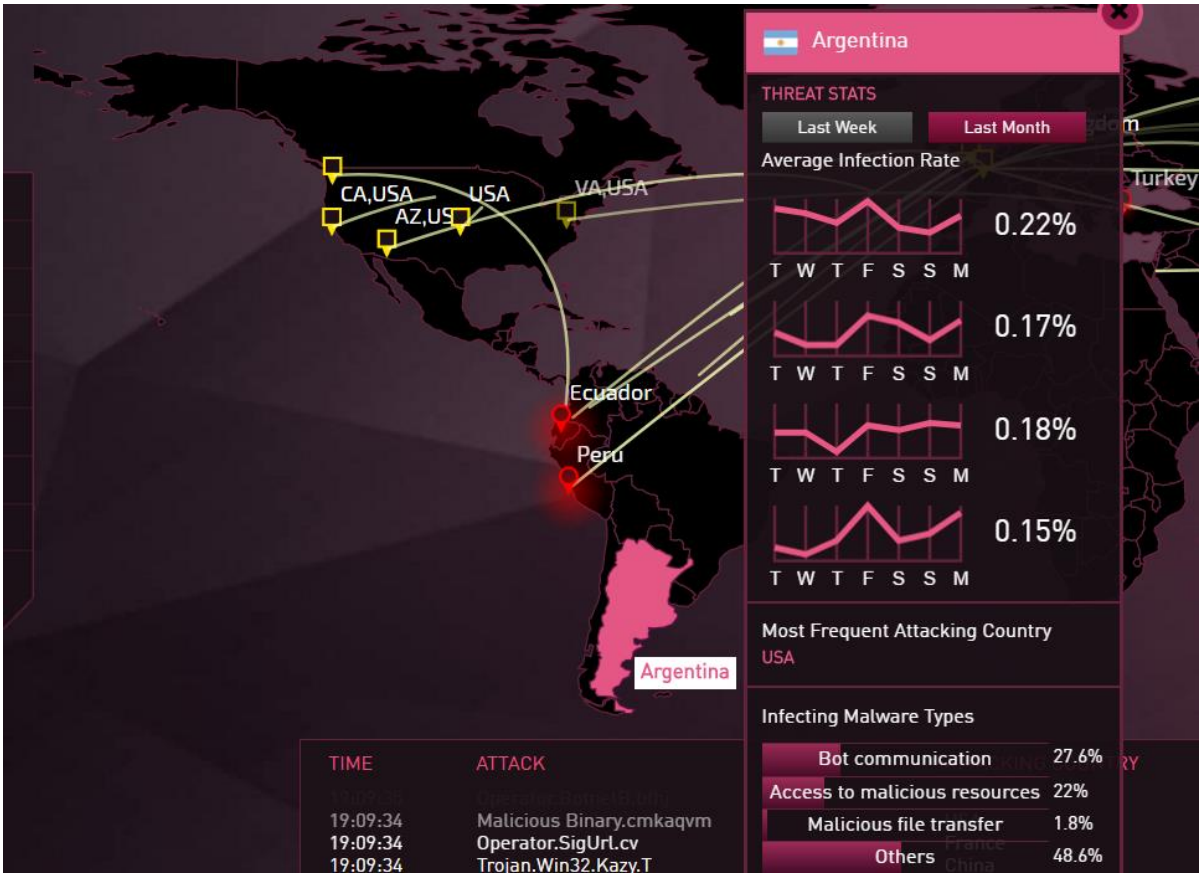


Figura 34: captura de pantalla con datos de ciberataques a Argentina (Kaspersky Lab).

5. El problema de las infraestructuras críticas de la información y comunicación:

[51] Ver https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Muchos de los ataques a los que estamos sometidos a diario, carecen de efectos importantes, excepto para el afectado. Incluso, los fraudes más graves, implican en el peor de los casos pérdidas millonarias en términos exclusivamente económicos.

Sin embargo, el riesgo más importante en el caso de los ataques cibernéticos, radica en la probable afectación, voluntaria o no, de infraestructuras vitales para el normal funcionamiento de un estado como así también para su desarrollo.

Muchas de estas infraestructuras, revisten extrema importancia, toda vez que su afectación, tiene incidencia en la vida de un gran número de habitantes. Estas infraestructuras se denominan Infraestructuras Críticas (IC) y aquellas IC normalmente controladas o gestionadas por sistemas informáticos, Infraestructuras Críticas de la Información y Comunicación (ICIC). Las ICIC incluyen las áreas de administración del estado, espacio, industria nuclear y química, defensa, investigación y desarrollo, suministro de agua, energía, salud, comunicaciones, transporte, sistema financiero e impositivo, seguridad, etc.

Las Infraestructuras Críticas de Información y Comunicación (ICIC), son aquellas instalaciones, redes, servicios y equipos físicos y de Tecnologías de Información, de funcionamiento indispensable para brindar servicios a los ciudadanos y las instituciones y cuya "…interrupción, perturbación o destrucción, podría tener un grave impacto y repercusión importante en la continuidad de las operatorias de los Organismos del Sector Público Nacional (SPN)…. El fallo de alguna ICI podría a su vez provocar fallos en otros sectores, generando efectos en cascada, a causa de las sinergias existentes entre las diferentes infraestructuras" (Stel, pág. 18).

"En Brasil, varios apagones se han relacionado con ciberataques y, en 2008 los piratas informáticos consiguieron entrar y tomar el control del sitio web del Gobierno durante una semana. Estos apagones en Brasil ilustran la posible magnitud de estos nuevos tipos de ciberataques: los informes se parecen a una escena de una película de ciencia ficción, dado que quedaron totalmente paralizados los trenes del metro, los semáforos e incluso la segunda central hidroeléctrica más grande del mundo, la represa Itaipú, y se vieron afectadas más de 60 millones de personas" (Unión Internacional de las Comunicaciones, 2011).

Tal como ocurrió con el ataque a la central de Natanz, la mayoría de las ICIC emplean sistemas SCADA o similares. Estas recaban información sobre los flujos,

consumos, estados de abastecimiento, y otros datos de una variedad de servicios, incluyendo servicios de gas, hidráulicos, energéticos, medios de comunicación masivos, procesos industriales de fabricación, distribución de productos, etc.

Para mensurar adecuadamente el riesgo, un ataque al sistema de control SCADA de la represa Yaciretá, que indujera a la apertura involuntaria y sin regulación, de las compuertas de la presa, podría provocar el vaciamiento del lago al noreste del muro de contención y el derrame del agua (sobreelevada 23 metros sobre el nivel del río aguas abajo), ocasionando el aumento del nivel en el curso inferior de entre 1,5 y 2 mts en un plazo de 36 a 48 horas.

Se producirían inundaciones hasta unos 10 km de ambas márgenes, las que llegarían casi a unos 1000 km al sur (San Nicolás), afectando a más de 2.500.000 habitantes por agua y a más de siete millones por cortes en el suministro de energía. Los efectos de un ataque de este tipo, sin duda serían catastróficos, con daños de magnitud nacional.

Del mismo modo, un ataque contra cualquier central nuclear nacional, podría afectar por escapes radiactivos (dependiendo los efectos de las condiciones meteorológicas) a los habitantes situados en un radio de más de 700 km, haciendo de un problema de origen local, uno internacional (se podría afectar a otros dos estados).

La República Argentina, se ubica a nivel mundial, en el puesto número 15, en cuanto a disponibilidad de material nuclear factible de ser empleado en armas de destrucción masiva, incluyendo las llamadas bombas sucias. Ocupa el mismo puesto en el nivel de seguridad general, incluida la prevención de robo y en el número 23 en cuánto a seguridad frente a sabotajes, entre los que se pueden incluir a los ataques cibernéticos. (Nuclear Threat Initiative, 2016, pág. 140).

Estos datos sin embargo no distinguen entre dos temas relacionados a la seguridad nuclear. El primero de ellos, está vinculado a la seguridad de los sistemas en cuándo a su correcto funcionamiento (conocida como *safety* en inglés). El segundo, se relaciona con la seguridad contra ataques o robos (conocida como *security* en inglés). Desafortunadamente, las amenazas cibernéticas pueden incidir en ambos sentidos.

En el mapa siguiente, se puede muestran los alcances de los efectos radioactivos que podrían producirse si ocurriese algún incidente en las centrales nucleares de Atucha I

o Embalse. En ambos casos, y con una radiación superior a 2000 milisieverts[52] al año, se podría afectar un mínimo de 3 países.

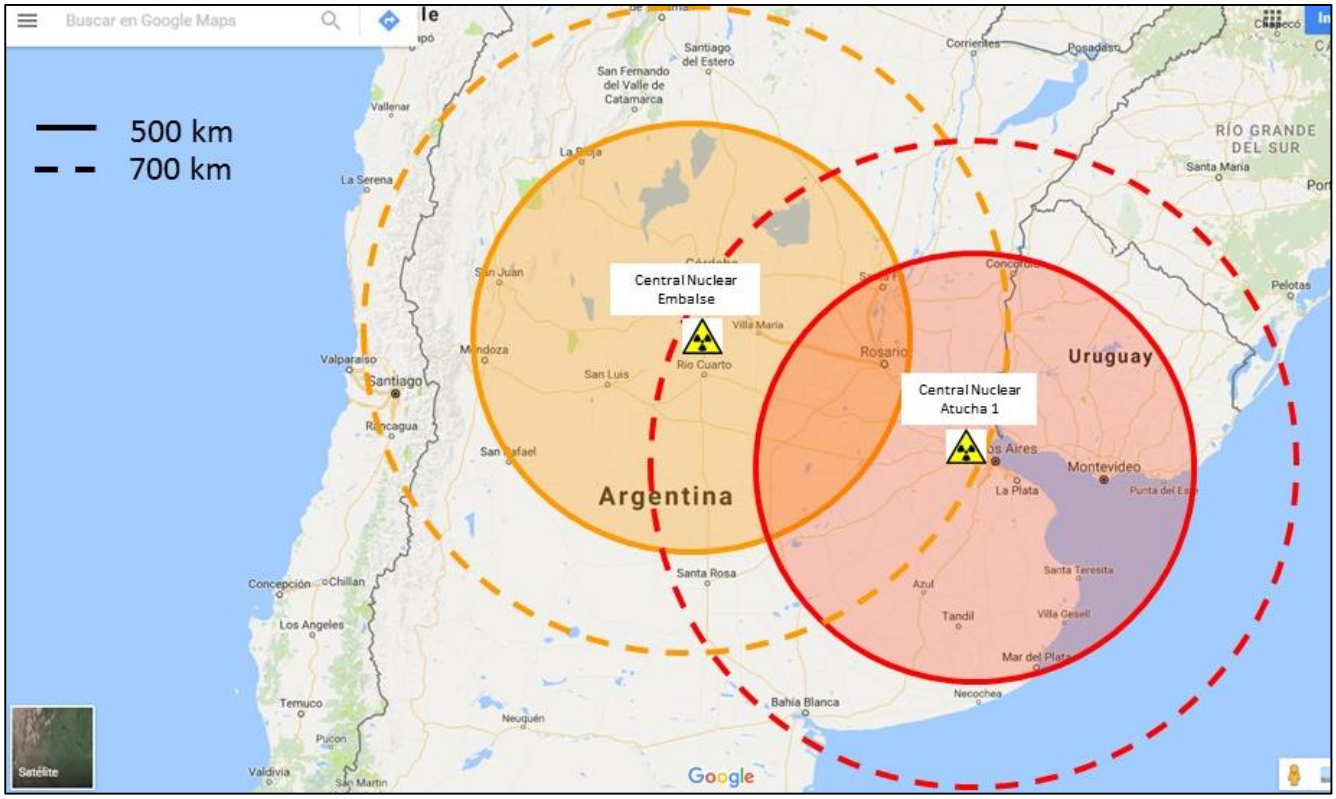


Figura 35: Alcances de radiación nociva de las centrales Atucha 1 y Embalse (gráfico del autor).

Problemas menores, aunque también catastróficos, se podrían generar sobre los controles de tránsito aéreo, redes ferroviarias, puertos, etc.

Una muestra de lo serio y complejo de la problemática está en las palabras del jefe del Centro de Capacidad de Respuesta de Incidentes Informáticos de la OTAN [53] (NATO CIRC) Alex Vandurme: *"Nuestro mayor desafío es un poco como defender un rascacielos. Tenemos que cerrar cada puerta y ventana, mientras que los hackers sólo necesitan abrir una abertura para entrar. Tenemos que pensar en todo, todo el tiempo, pensar como ellos y anticiparse".*

[52] El sievert (símbolo Sv) es una unidad derivada del SI que mide la dosis de radiación absorbida por la materia viva, corregida por los posibles efectos biológicos producidos. 1 Sv es equivalente a un joule por kilogramo (J kg-1).
[53] NCIRC (NATO COMPUTER INCIDENT RESPONSE CAPABILITY).

6. Ciberamenazas a redes y sistemas del ámbito de la defensa:

Tanto en tiempos de paz como durante el desarrollo de operaciones de fuerzas militares, los sistemas informáticos que empleados por fuerzas armadas y las redes que eventualmente se integren, están sujetas a las mismas amenazas enunciadas en este capítulo.

La cantidad de sistemas y redes empleados por una fuerza está en relación directamente proporcional con el nivel de desarrollo tecnológico del estado al cual pertenecen. Y del mismo modo, a mayor nivel de desarrollo y mayor cantidad de sistemas y redes, es más grande la cantidad de blancos que presentan frente a ciberamenazas.

Esto no significa en modo alguno que aquellas fuerzas con menor cantidad de sistemas y redes puestos en acción en un teatro de operaciones, lleven ventaja sobre las que poseen mayor cantidad.

Por el contrario, incluso aún bajo un riesgo elevado de ciberamenazas, las ventajas que fuerzas altamente informatizadas en el campo de combate, tienen sobre fuerzas no digitales ni aptas para desarrollar operaciones en red, son imposibles de compensar.

Si bien en los ejemplos citados precedentemente, solo unos pocos de ellos se refieren a redes específicamente militares (Operación Orchard, penetración al Servicio de Inteligencia Naval de EEUU, hackeo de la página web del Ejército y correo institucional de la Armada Argentinos), existen una gran cantidad de redes administrativas y operativas, pasibles de ser objeto de todo tipo de ataques cibernéticos.

La dependencia del ser humano y en particular del militar, de redes y sistemas informáticos, queda evidenciada en el siguiente gráfico.

Se enumeran en el cuadro siguiente, los sistemas y redes más comunes de empleo militar, con una breve descripción de sus funciones y de los riesgos implícitos en su vulneración.

TIPO DE SISTEMA O RED	CAMPO O ÁREA	FUNCIONES BÁSICAS
ADMINISTRATIVAS (operación y gestión de diferentes áreas de una organización para garantizar su funcionamiento en tiempos de paz)	De personal	- Legajos de personal y calificaciones. - Documentación funcional de uso diario. - Registros disciplinarios. - Documentación y legajos médicos. - Programas de mantenimiento de la moral, etc.
	Inteligencia	- Bases de datos de Inteligencia básica. - Estudios de seguridad de instalaciones propias. - Sistemas criptográficos, claves, etc, para comunicaciones clasificadas.
	Operaciones	- Archivo de planes (para operaciones y de seguridad de las propias instalaciones). - Documentación de educación y adiestramiento. - Registros de documentación clasificada. - Documentación y legajos médicos. - Apoyo a la navegación aérea y terrestre. - Sistemas de simulación
	Logísticas	- Inventarios, estados de mantenimiento y abastecimiento, documentación funcional. - Requerimientos. - Programas varios (Ab, Mant, etc).
	Presupuestarias y financieras	- Programación y ejecución presupuestaria. - Salarios y suplementos. - Procesos licitatorios.
	Investigación y Desarrollo	- Requerimientos operacionales de diseño. - Documentación de ingeniería y técnica. - Documentación técnica y administrativa relacionada a ofertas, precios, costos, etc.

OPERATIVAS (necesarias para la conducción y ejecución de operaciones militares, incluyendo desde redes a computadores individuales propios de un sistema de armas, vehículo, aeronave, etc.)		- Sistemas de comando y control digitales (incluyendo planes, cartas de situación, etc) - Sistemas de navegación terrestres, aéreos y navales. - Sistemas de dirección de tiro (aéreos, terrestres y navales) y de guiado de armas. - Sistemas de comunicaciones digitales (Radio y telefonía IP o satelital, sistemas troncalizadores, integradores, telefonía celular, etc). - Sistemas de conciencia situacional (SAS= Situational Awareness Systems) - Sistemas de Información Geográfico (SIG/GIS). - Sistemas de apoyo a la elaboración de planes. - Sistemas sanitarios. - Sistema relacionados a las funciones logísticas en campaña.

Figura 36: Tipos de redes informáticas militares y uso normal (gráfico del autor).

La figura siguiente[54], muestra el nivel de conectividad alcanzado por un soldado incluyendo su integración en redes militares administrativas y operacionales, tanto como las de uso civil. Hace referencia a las tres capas del ciberespacio.

[54] El cuadro es adaptado del que figura en el FM 3-12 *Cyberspace and Electronic Warfare Operations* en la página 1-14.

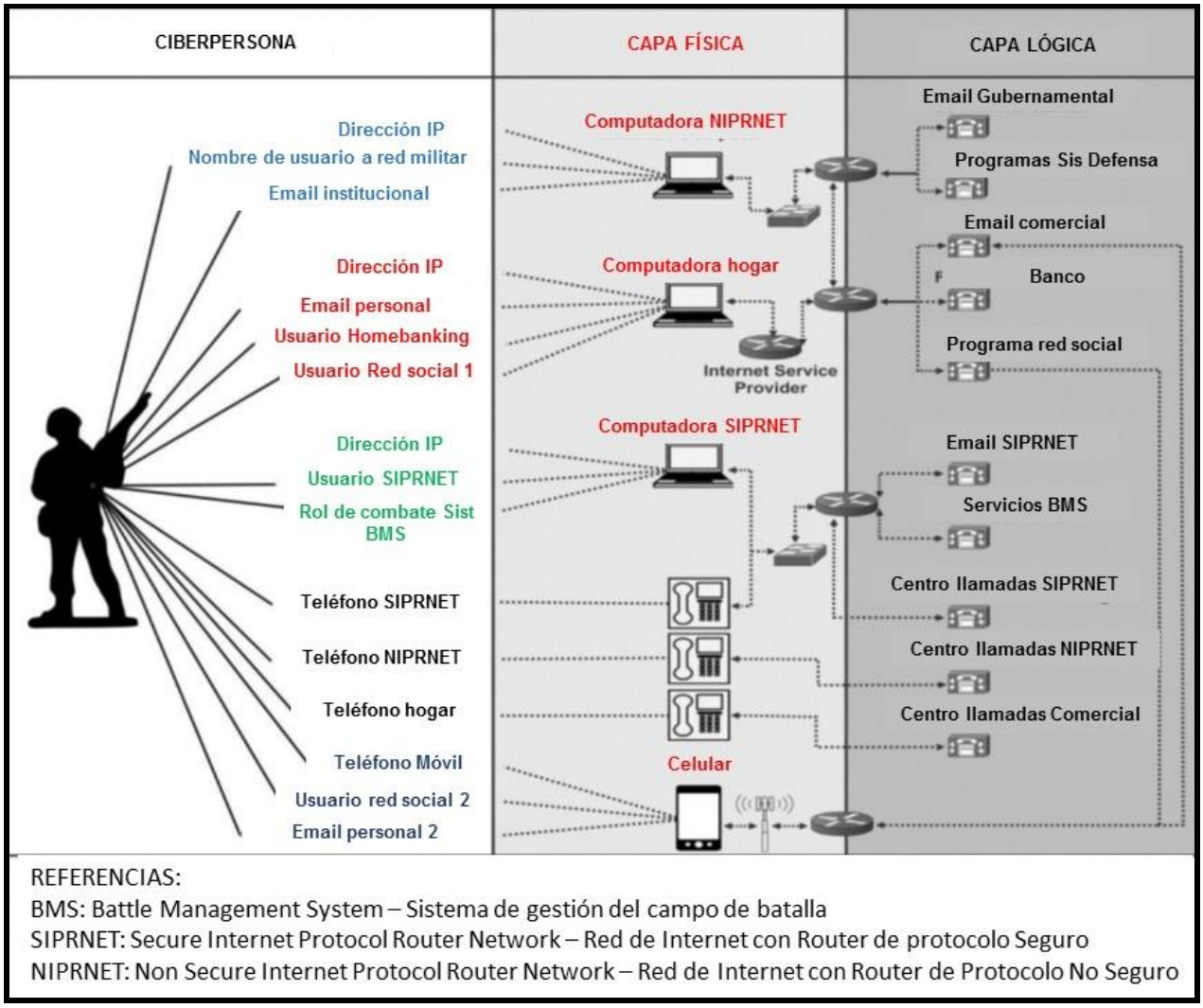


Figura 37: Nivel de conectividad de un soldado moderno (Tomado de FM 3-12 Cyberspace and Electronic Warfare Operations).

Un breve análisis del gráfico, permite concluir acerca de las múltiples posibilidades de penetración en las distintas redes a las que un solo individuo accede y emplea en forma diaria.

Si se considera incluso la pertenencia a varias redes sociales (Facebook, Pinterest, Instagram, etc), aplicaciones de celular con acceso en clave (Whatsapp, Telegram, Alo, Etc), direcciones comerciales para compras (Mercado Libre, Amazon, supermercados, etc) e instituciones bancarias (es raro operar exclusivamente en un banco), se puede inferir el nivel de vulnerabilidad individual y a partir de ello, de la red entera.

7. Las ciberamenazas y el riesgo de guerra preventiva:

"…debemos entender cómo distribuir y proteger nuestros intereses nacionales en el dominio cibernético y, aunque se trata claramente de una cuestión de gobierno, la defensa tiene un interés legítimo en el desarrollo de capacidades defensivas y ofensivas cibernéticas".[55]

Uno de los mayores problemas que se plantean a las naciones con capacidades de defensa cibernética reducidas, es la posibilidad de verse envueltos en conflictos con otros países más poderosos, por no poder garantizar la seguridad de sus servidores locales y convertirse en meras plataformas de lanzamiento de armas cibernéticas, contra esos países más poderosos.

El conflicto así generado, puede devenir o convertirse en lo que se denomina convencionalmente guerra preventiva.

Las operaciones de guerra preventiva, son las acciones llevadas a cabo por un Estado contra otro Estado o actor no estatal, que amenaza a los intereses vitales del primero. Normalmente se inicia sin declaración de hostilidades, aunque puede estar precedida por una serie de advertencias, notificaciones y ultimátums para influir en la decisión de quien será atacado y modifique su conducta respecto a lo que constituye la amenaza. Su empleo no es novedoso, registrándose en la historia militar numerosos ejemplos.

Los Estados del Continente Americano fueron pioneros en su consideración legal. En 1945, se celebró en México la "Conferencia Interamericana sobre Problemas de la Guerra y de la Paz". Su resultante fue la firma del "Acta de Chapultepec" la cual avalaba en la resolución sobre "Asistencia Recíproca y Solidaridad Americana", el "…uso de la fuerza armada para prevenir o repeler una agresión..."[56].

Por su parte, la Organización del Tratado del Atlántico Norte (OTAN) la incluyó como una tarea de sus fuerzas militares en su Concepto Estratégico de 1990,

[55] Discurso pronunciado en el Instituto Internacional de Estudios Estratégicos de la Defensa del Reino Unido por comandante en jefe de la Fuerza Aérea Británica Sir Stephen Dalton. Artículo publicado por el periódico The Independent – 16 Feb 2010 – http://www.independent.co.uk/news/media/online/twitter-is-a-weapon-in-cyber-warfare-1900535.html. Tomado de Guerra Cibernética – Stel, Enrique, Círculo Militar 2005

[56] Kenny, Alejandro. "Integración y capacidad disuasiva en materia de defensa en Suramérica"- Consejo Argentino de las Relaciones Internacionales- Boletín ISIAE Nro 52, pág 5- Feb 2010.

presentado en la Cumbre de Roma en 1991[57] . El reconocimiento del nuevo entorno de seguridad, fue fundamental:…" la Alianza no se enfrentaba a la amenaza de un enemigo que estuviese planeando un ataque contra los aliados, sino a riesgos, retos e incertidumbres, que tenían un carácter multifacético y multidireccional, más difíciles de predecir y valorar, que podían surgir de diferentes formas y que podrían provocar enfrentamientos armados afectando a la seguridad de los aliados…"[58.] Por ello, entre las tareas establecidas para las fuerzas, figura la de disuadir y defenderse de cualquier amenaza de agresión contra el territorio de cualquier Estado miembro de la OTAN "*To deter and defend against any threat of aggression against the territory of any NATO member state*."[59]." En 1999, un nuevo concepto estratégico, mantenía abierta la puerta a las operaciones preventivas.

El 11 de septiembre de 2001, el atentado terrorista ocurrido en New York contra el World Trade Center, marcó el inicio de una nueva etapa en el sistema internacional.

El 12 de septiembre, los Estados Unidos invocaron el Artículo 5to del Tratado de Washington de creación de la NATO, el que establece que cualquier ataque contra una o más de las partes en Europa o en América del Norte, deberá ser considerado como un ataque contra todas[60].

Por su parte, con la aprobación unánime de sus miembros, el Consejo de Seguridad de la ONU en su resolución 1368/2001, condenó el atentado, reafirmó el derecho inmanente de la legítima defensa y exhortó *"… a la comunidad internacional a que redoble sus esfuerzos por prevenir y reprimir los actos de terrorismo…*"[61].

---

[57] Las tareas establecidas para las fuerzas de la OTAN por ese concepto estratégico, incluían: 1.SEGURIDAD: Crear un entorno de seguridad Euro-Atlántico., 2. Servir de foro de consultas transatlántico. , 3. Disuadir y defenderse de cualquier amenaza de agresión., 4. Preservar el equilibrio estratégico en Europa.

[58] Conferencia pronunciada en Madrid por el Director del Instituto de Estudios Estratégicos del Reino de España, General Miguel Ángel Ballesteros, el 9 de octubre de 2009. La presentación puede descargarse de la página http://ebookbrowse.com/1256310418-concepto-estrategico-otan-ppt-d38848196

[59] Extraído de la página oficial de la NATO el 20 de abril de 2013. http://www.nato.int/cps/en/natolive/official_texts_23847.htm?blnSublanguage=true&selectedLocale=&submit.x=10&submit.y=8&submit=select .

[60] Extraído de la página oficial de la NATO el 20 de abril de 2013. http://www.nato.int/cps/en/natolive/official_texts_17120.htm .

[61]Texto de la resolución extraído de la página oficial de la ONU el 20 de abril de 2013. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/533/85/PDF/N0153385.pdf?OpenElement . Lo actuado en la reunión del Consejo, puede leerse en

Bajo ésta última premisa, EEUU invadió Afganistán el 7 de octubre de 2001 en una combinación de operaciones preventivas y punitivas. Estas continúan hasta el día de hoy, sin críticas o condenas por parte de la comunidad internacional en lo que a legitimidad de origen se refiere.

Sin embargo, es a partir de la difusión de la US National Security Strategy 2002 (NSSR 2002), en donde el concepto retoma vigencia internacional, originando críticas y adhesiones. Presentada por el gobierno del presidente George W Bush, el 17 de septiembre de 2002, expresa: "*Si bien Estados Unidos tratará constantemente de obtener el apoyo de la comunidad internacional, no dudaremos en actuar solos, en caso necesario, para ejercer nuestro legítimo derecho a la defensa propia, con* ***medidas preventivas*** [énfasis del autor] *contra esos terroristas, a fin de impedirles causar daños a nuestro pueblo y a nuestro país*". Agrega a continuación que "Estados Unidos ha mantenido largamente la opción de acciones preventivas para contrarrestar una amenaza suficiente a nuestra seguridad nacional. Cuanto más grande sea la amenaza, más grande es el riesgo de la inacción y es más necesaria la razón para tomar medidas preventivas para defendernos, incluso aunque sea incierto el momento y el lugar del ataque enemigo. Para impedir o evitar tales actos hostiles de nuestros adversarios, **Estados Unidos actuará preventivamente** [énfasis del autor], si es necesario."[62].

El NSSR 2006 mantuvo su validez como opción estratégica, pero en el Informe del año 2010 se descartan estas acciones, aunque mantiene abierto el recurso unilateral de la fuerza, si es necesario, para defender la nación o sus intereses.

La guerra preventiva, aunque no definida por el Derecho Internacional, ha sido y es en la actualidad una práctica de uso común, generalmente reservada a Estados con un poderío militar importante. Su justificación en el sistema internacional ha sido exitosa en algunos casos. En otros, aunque no fuera aceptada, no impidió su realización ni trajo aparentadas sanciones de algún tipo para la potencia que la inició[63].

Particularmente, la ejecución de operaciones ofensivas cibernéticas y las acciones de represalia (incluso con fuerzas convencionales) contra aquellos estados que ejecuten, propicien o permitan (incluso sin conocimiento expreso) la realización de

---

http://www.un.org/es/comun/docs/?symbol=S/PV.4370 .

[62]Traducción libre del autor de la página oficial del Gobierno de los EEUU el 17 de abril de 2013. http://www.state.gov/documents/organization/63562.pdf

[63] El resaltado en ese párrafo y otros siguientes, es del autor.

ataques cibernéticos, están contempladas en las estrategias de defensa de numerosas potencias. Se abre la posibilidad así de intervenir militarmente en cualquier país bajo la sola y difícilmente comprobable suposición de una amenaza (Baretto, 2013, pág. 6).

CAPÍTULO III

MARCO LEGAL RELACIONADO CON LA SEGURIDAD Y LA DEFENSA CIBERNÉTICA.

Uno de los mayores problemas a la hora de enfrentar la problemática de las amenazas cibernéticas, radica en la ausencia de un marco legal internacional que regule el uso del ciberespacio.

Las razones para ello son variadas, pero se pueden citar las siguientes:

- La extrema lentitud de las legislaciones nacionales e internacionales frente a la velocidad inusitada de los avances tecnológicos, provocada fundamentalmente por falta de preparación.
- Las diferencias manifiestas en cuánto al nivel de regulación exigible e imponible. En la práctica, el enfrentamiento entre las posturas que favorecen la libertad absoluta en el uso del ciberespacio frente quienes propician el uso condicionado y limitado, con una amplia gama de opiniones intermedias.

A pesar de ello, existen una serie de acuerdos y convenios internacionales, que pueden servir de base en el futuro para generar un consenso legal a nivel mundial.

Entre ellos se pueden citar a la Carta de las Naciones Unidas, esencialmente en sus artículos 41 (…*el Consejo de Seguridad podrá adoptar medidas que no impliquen el uso de fuerza armada, para hacer cumplir sus decisiones, incluyendo la interrupción parcial o total de comunicaciones*….) y 51 (derecho a legítima defensa), el Tratado del Espacio (prohibe el despliegue y empleo de armas de destrucción masiva en el espacio), el Convenio sobre Ciberdelincuencia de Budapest (2001), que será mencionado más adelante, algunas resoluciones de la OEA sobre Seguridad Cibernética y finalmente el Manual Tallinn[64], que en forma académica, sienta bases para regular la ley internacional de seguridad cibernética y de los ciberconflictos armados.

El “Manual Tallinn de Ley Internacional Aplicable a Guerra Cibernética”[65], fue propuesto por el *NATO Cooperative Cyber Defence Centre of Excellence* en 2013 y tiene como objetivo principal, dar los primeros lineamientos legales en materia de guerra

[64] Tallinn es la capital de Estonia. El *NATO Cooperative Cyber Defence Centre of Excellence*, tiene su sede en esa ciudad, a raíz del ataque llevado a cabo supuestamente por hackers rusos, durante el conflicto con ese país, ya mencionado.
[65] Puede ser consultado en http://www.ccdcoe.org/249.html de fecha 03 May13.

cibernética

Fue elaborado por un grupo de expertos, a requerimiento de la OTAN, pero aún no constituye un documento oficial de esa organización ni fue adoptado por otros estados.

Se divide en dos partes principales; la primera de ellas, se explaya sobre el Derecho a la Seguridad Cibernética Internacional, la cual incluye una serie de definiciones relacionadas con los estados y el espacio cibernético.

Hace mención a la “Soberanía, jurisdicción y control”, estableciendo que cada estado puede ejercer el control sobre la estructura cibernética y las actividades relacionadas dentro de su territorio soberano, sobre las personas empeñadas en realizar actividades cibernéticas en su territorio y conforme al derecho internacional, fuera de su territorio, incluyendo la infraestructura cibernética en buques, plataformas en espacio aéreo, alta mar o en el espacio exterior.

En tal sentido, cualquier interferencia con la estructura cibernética estatal o privada, cualquiera sea donde esté ubicada, constituye una violación de la soberanía.

Sin embargo, esto crea una obligación, y es la de no permitir que cualquier infraestructura cibernética, sea empleada para afectar negativamente o fuera de la ley a otros estados. Esto, según el manual Tallinn, es una responsabilidad legal internacional y cualquier estado que permita ello, aunque no sea atribuible en forma directa a él, está dando una clara indicación de que está asociado a la operación (aunque más adelante aclara que no se le atribuye la responsabilidad primaria).

Cualquier acto que afecte a un estado, lo habilita a responder con contramedidas proporcionales, incluyendo medidas cibernéticas, contra el agresor.

Una de las definiciones más claras es la calificación que en materia cibernética, hace del uso de la fuerza. Al respecto señala que “Una operación cibernética constituye un uso de la fuerza cuando su escala y efectos son comparables con operaciones no cibernéticas que conduzcan al uso de la fuerza”.

El manual Tallinn no toma posturas respecto a la ejecución de operaciones cibernéticas como parte de las acciones propias de una guerra preventiva, aunque algunos de sus postulados de hecho, dejan cierto grado de libertad y ambigüedad al respecto.

La posibilidad de acciones preventivas, se manifiesta al expresar que “El derecho a usar la fuerza en defensa propia surge si ocurre un ataque armado cibernético o es inminente. Es además un tema de exigencia de la inmediatez”.

La segunda parte está referida al derecho del conflicto cibernético armado y constituye una adaptación del Derecho Internacional de los Conflictos Armados, a las particularidades y exigencias propias de las operaciones en el ciberespacio.

A modo de síntesis, en sus dos partes, establece entre otros, los siguientes postulados:

- Los Estados no pueden permitir a sabiendas que la infraestructura cibernética situada en su territorio sea utilizado para actos que afectan negativamente a los demás Estados.
- Los Estados serán responsables de las operaciones cibernéticas dirigidas contra otros Estados, aunque no fueron realizadas por sus organismos de seguridad. Cada Estado será responsable por las acciones de los individuos o grupos que actúan bajo su dirección como si se las hubiere realizado él mismo.
- La prohibición del uso de la fuerza en el derecho internacional se aplica plenamente a las operaciones cibernéticas (que cause daños a personas o a bienes).
- Las operaciones cibernéticas que sólo causen molestias o irritación no son actos de fuerza.
- Los estados pueden responder a operaciones cibernéticas ilegales que no llegan al nivel de un uso de la fuerza, como contramedidas.
- Un Estado que es víctima de un ciberataque puede responder mediante el uso de la fuerza. La fuerza puede ser cibernética o convencional. En el derecho internacional, un "ataque armado" es un uso "grave" de la fuerza. Cualquier operación cibernética que da lugar a la muerte o un daño significativo a la propiedad, es un ataque armado[66].
- Los actores no estatales, como los terroristas cibernéticos, son capaces de llevar a cabo ataques armados, a los que el Estado víctima podrá responder en defensa propia, siendo aceptable usar la fuerza contra los terroristas en otros Estados.
- Tiene plena vigencia en ciberguerra, el Derecho Internacional Humanitario.

[66] Este artículo es particularmente riesgoso dado lo analizado en el Capítulo 1. ¿Es posible identificar el origen de la amenaza y el propósito, con tanta precisión que una respuesta militar, sea justa desde el punto de vista legal y ético?. Particularmente y es opinión del autor, se abren puertas a intervenciones difícilmente justificables, las que podrían ocultar propósitos ajenos a los de este manual.

- Durante un conflicto armado, jefes y superiores pueden ser penalmente responsables por ordenar operaciones cibernéticas que constituyan crímenes de guerra o por no detener este tipo de operaciones cuando sean cometidos por sus subordinados.
- Aunque no hay ninguna prohibición en el Derecho Internacional Humanitario contra civiles hacktivistas (Hackers) para realizar operaciones cibernéticas durante un conflicto armado, éstos pueden convertirse a veces en blancos legítimos.
- Un ataque cibernético es una operación que causa lesiones o la muerte a personas o daños o destrucción de objetos o que interfiere con el funcionamiento de la infraestructura cibernética de una manera que requiera reparación. Por lo tanto, las operaciones cibernéticas dirigidas contra la población civil o bienes de carácter civil no están prohibidas por el Derecho Internacional Humanitario cuando sólo causan disrupción, irritación y molestias.
- Es ilegal utilizar ataques cibernéticos para sembrar el terror entre la población civil.
- Las Armas cibernéticas deben ser objeto de una revisión legal antes de que se pueda emplear en el campo de batalla[67].
- Es ilegal lanzar un ataque cibernético que no se dirija a un objetivo legítimo y que por lo tanto podría causar daño a la población y los bienes civiles.
- La protección especial que el personal sanitario y religioso, sus unidades y sus medios de transporte tienen en el Derecho Internacional Humanitario se aplican con todo rigor a las operaciones cibernéticas dirigidas contra ellos. Lo mismo es aplicable con respecto a "los bienes indispensables para la supervivencia de la población civil", como suministros médicos, tiendas de alimento y las instalaciones de tratamiento de aguas.

De la lectura de estas y otras regulaciones, surgen vacíos legales originados en la necesidad insatischa de definir con precisión, algunos conceptos, algo que en la práctica es imposible dada la complejidad del tema.

No obstante, este primer intento de regulación, deberá ser aceptado internacionalmente. La mayor dificultar para ello, radica en que por limitar de algún modo a las estrategias de seguridad de las potencias, podría (tal como ocurre en el caso del Tratado de No proliferación Nuclear), ser solo imponible para aquellos Estados con

[67] Esto es a criterio del autor, inaplicable en términos prácticos, ya que ningún estado se arriesgaría a revelar las capacidades y debilidades de sus propios sistemas de armas cibernéticos. En ciertos aspectos, el manual Tallinn, peca de ingenuidad.

capacidades limitadas en materia de defensa y seguridad cibernética.

El día 08 de febrero del 2017, fue presentado el "*Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations*" (Manual Tallin 2.0. Sobre el Derecho Internacional Aplicable a las Operaciones Cibernéticas). Publicado por Cambridge University Press, constituye el análisis más completo existente sobre legislación relacionada a las operaciones en el ciberespacio. Fue supervisado y autorizado por diecinueve expertos en derecho internacional y constituye la versión actualizada del Manual Tallin de 2013.

En su elaboración, tuvo participación activa el Centro de Ciber Defensa Cooperativo de Excelencia, de la NATO (ubicado en Tallinn precisamente). Una de sus premisas básicas es reconocer que el derecho internacional previo a la era de la informática, es aplicable a las operaciones cibernéticas realizadas contra los estados. Esto implica que los estados tienen en ese sentido, tanto derechos como obligaciones en función de ese derecho internacional.

En ese sentido, las amenazas o ataques cibernéticos más graves se encuadran en violaciones al uso de la fuerza y por ende, facultan a lo estados amenazados o atacados, a ejercer el derecho de legítima defensa, sea en el ciberespacio o mediante el uso de la fuerza armada. Se tipifican también en él, los ataques y acciones que no habilitan para el uso de la fuerza.

El manual Tallinn 2.0. cubre el espectro completo del Derecho Internacional aplicable a las operaciones en el ciberespacio, tanto en tiempo de paz como en tiempos de guerra. Desarrolla asimismo aspectos relacionados con la soberanía en el ciberespacio, bases para el ejercicio de la jurisdicción, responsabilidad estatal y otros aspectos especializados, tales como derechos humanos en el ciberespacio, derecho aeronáutico y espacial, derecho marítimo, deplomático y consular (CCDCOE, 2017).

Su mayor falencia radica en no tener carácter vinculante, es decir, de cumplimiento obligatorio, pese a haber sido reconocido por todos los miembros de la OTAN.

A nivel continental, se han producido algunos avances en la materia. Dentro del marco propiciado por la Organización de Estados Americanos (OEA), se realizaron

reuniones en las que se definieron lineamientos de seguridad cibernética[68]. Estos fueron difundidos mediante declaraciones de aplicación para los estados miembros, aunque como en otros casos, no tienen carácter excluyente y su cumplimiento no es obligatorio.

Se pueden mencionar entre ellas a las siguientes:

- Resolución de la Asamblea General de la OEA para el "Desarrollo de una Estrategia Interamericana para combatir las amenazas a la seguridad cibernética" AG/RES. 1939 (XXXIII-O/03). A partir de la Resolución 57/239 sobre los elementos para la Creación de una Cultura Mundial de Seguridad Cibernética para Sistemas y Redes de Información, de la Asamblea General de las Naciones Unidas, en diciembre de 2002, y del ofrecimiento de Argentina para el desarrollo de un taller sobre ciberamenazas, la Asamblea General de la OEA resolvió encarar la elaboración de una estrategia de ciberseguridad regional.

- Declaración de Panamá sobre "La Protección de la Infraestructura Crítica en el Hemisferio frente al Terrorismo". Comité Interamericano Contra el Terrorismo (CICTE-OEA) (aprobada en la tercera sesión plenaria, el 1 de marzo de 2007).

- Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas". Comité Interamericano Contra el Terrorismo (CICTE - OEA) (aprobado durante la cuarta sesión plenaria, el 7 de marzo de 2012).
  Entre los quince puntos que incluye esta declaración, es de utilidad destacar los siguientes aspectos:
  1) La firme condena al terrorismo en todas sus formas[69]. Adicionalmente y en relación a ello, expresa la necesidad de cooperación internacional y su exhortación a firmar y adherir a la declaración a quienes no lo hayan hecho.
  2) En relación a la problemática de la seguridad cibernética, desarrolla ocho puntos, incluyendo entre ellos el compromiso a implementar la Estrategia Interamericana

[68] Ver a modo de ejemplo, http://www.cicte.oas.org/rev/en/Documents/Declarations/DEC%201%20rev%201%20DECLARACION%20CICTE00749S04.pdf de fecha 03 de mayo de 2013.

[69] "Su más enérgica condena al terrorismo, en todas sus formas y manifestaciones, por considerarlo criminal e injustificable, bajo cualquier circunstancia, en dondequiera y por quienquiera sea cometido, y porque constituye una grave amenaza a la paz y la seguridad internacionales, a la democracia, estabilidad y prosperidad, de los países de la región."

de Seguridad Cibernética, adoptada mediante la resolución AG/RES. 2004 (XXXIV-O/04), la insistencia a crear, mejorar y fortalecer los CSIRT nacionales, la importancia de que los mismos se integren a un sistema de seguridad cibernético hemisférico, la necesidad de reforzar la seguridad y la resistencia de tecnologías de infraestructura crítica de información y comunicaciones (TIC) ante las ciberamenazas y su voluntad de continuar desarrollando estrategias nacionales de seguridad cibernética integrales e involucrar a todos los actores de necesaria intervención. (CICTE, 2012, pág. 8)

Todas las declaraciones establecen conceptos básicos relacionados al combate contra las amenazas cibernéticas en un marco cooperativo.

Entre otros conceptos, se menciona la necesidad de integrarse regionalmente como un método eficiente para el aumento de la seguridad cibernética, la integración pública y privada, la protección de las infraestructuras críticas y la necesidad de que todos los miembros adhieran a lo resuelto y se integren entre sí.

Del mismo modo, condena a los ataques cibernéticos como una amenaza terrorista emergente, haciendo referencias expresas a la posibilidad de dar una respuesta militar convencional o a realizar operaciones cibernéticas ofensivas[70] contra ellos, sin prohibirlas expresamente.

Y como sucede con el manual Tallin, estas declaraciones no tienen el rigor de ley, fundamentalmente por incumplir una de las características básicas de cualquier ley, la coercibilidad, esto es, la capacidad del/los estado/s para aplicar por medio de la fuerza pública, una sanción si la persona la incumple. ¿cómo es posible sancionar, aunque si dispusiera de la capacidad de hacerlo, sino puede identificarse cabalmente al agresor?.

Nuevamente el caso Ardita, ejemplifica la problemática legal y tal como lo expresa Lawrence Greenberg, *"…los Estados Unidos no pudieron obtener su extradición, a pesar de que la Policía argentina cooperó con las autoridades estadounidenses. El sistema jurídico argentino, ante la nueva tecnología, no había clasificado a las Intrusiones como criminales…*[71]".

[70] Se refiere concretamente a la ejecución de ataques cibernéticos por parte de los estados miembros, contra fuentes de amenazas del mismo tipo. La generalidad de la declaración, dejan la puerta abierta al desarrollo de ciberarmas tanto como a la ejecución de operaciones de carácter preventivo. De nuevo, a criterio del autor, se aumenta la posibilidad de conflictos.

[71] Lawrence Greenberg y otros, *Information Warfare and International Law*, National Defense University, Institute for National Strategic Studies, 1997, P. 27. El texto mencionado puede ser consultado en:

Es a nivel intraestatal, el ámbito en el que generalmente se encuentran mayores consideraciones legales relacionadas a la seguridad y a la defensa cibernética. Sin embargo en la mayoría de los casos, son de aplicación principalmente al ámbito de la prevención y punición de ciberdelitos.

CAPÍTULO IV

http://www.dodccrp.org/files/Greenberg_Law.pdf

LA SITUACIÓN INTERNACIONAL: LOS ESTADOS FRENTE A LA AMENAZA CIBERNÉTICA.

Cualquier estado es responsable de desarrollar, fundamentalmente ante sus ciudadanos, una serie de funciones básicas que garanticen la satisfacción de las necesidades básicas de la población, el normal desarrollo de la vida en sociedad, la prosperidad y el progreso.

Entre ellas se pueden citar la educación, la salud, la justicia, la seguridad social, la comunicación, el transporte, la seguridad y la defensa.

Para desarrollarlas adecuadamente, el gobierno central, debe interactuar a través de la integración y coordinación con los gobiernos y organismos de los estados provinciales o departamentales dependientes y con organizaciones privadas, fundamentalmente las responsables de la administración y gestión de aquellas infraestructuras, servicios, e instalaciones relacionadas con esas funciones básicas.

Muchas de estas infraestructuras, revisten extrema importancia, toda vez que su afectación, tiene incidencia en la vida de un gran número de habitantes. Estas infraestructuras se denominan *Infraestructuras Críticas* (IC) y aquellas IC normalmente controladas o gestionadas por sistemas informáticos, *Infraestructuras Críticas de la Información y Comunicación (ICIC)*[72].

Las ICIC están presentes en diversas áreas, entre las que se puede destacar las de administración del estado, del desarrollo y gestión del espacio, industrias estratégicas como la nuclear, la petroquímica o la militar, defensa y seguridad nacional, investigación y desarrollo, suministro de agua, energía eléctrica, salud, comunicaciones, transporte, sistema financiero e impositivo, etc.

La concientización frente a la problemática de la amenaza cibernética, sigue, en general, un proceso general de cuatro etapas, el cual, pueden sintetizarse en el vocablo IDEO:

[72] Infraestructuras críticas de información (ICI): instalaciones, redes, servicios y equipos físicos y de TI de funcionamiento indispensable para brindar servicios a los ciudadanos y las instituciones y cuya "…*interrupción, perturbación o destrucción, podría tener un grave impacto y repercusión importante en la continuidad de las operatorias de los Organismos del Sector Público Nacional (SPN). El fallo de alguna ICI podría a su vez provocar fallos en otros sectores, generando efectos en cascada, a causa de las sinergias existentes entre las diferentes infraestructuras".*

I: **I**dentificar y Reconocer la Amenaza.

D: **D**efinir Políticas y Estrategias.

E: **EI**aborar El Marco Legal Necesario.

O: **O**rganizar Agencias Especializadas.

No obstante y aunque el orden establecido responde a una lógica elemental de razonamiento, se puede verificar que en muchos casos, se ha producido una alteración del orden y normalmente, la creación y organización de agencias especializadas, último paso en el proceso, suele preceder a la definición de políticas y estrategias y a la elaboración de un marco legal adecuado.

En los capítulos desarrollados previamente, se detallaron numerosos casos, que permiten mensurar acabadamente los riesgos de operar en el ciberespacio.

También se analizó someramente la legislación existente, la aún necesaria y los problemas que para su elaboración y fundamentalmente su aplicación, existen sobre todo a la hora de lograr consenso internacional.

En el presente capítulo, se describirá la forma en la cual abordaron y respondieron otros países a la problemática.

A. Los organismos internacionales frente a la amenaza cibernética.

Si bien puede decirse que la respuesta ante las amenazas, es una cuestión individual propia de cada estado, existen organizaciones internacionales[73] que realizan esfuerzos en pos de mejorar, de manera colectiva, el estándar de seguridad cibernética de los estados que integran esa organización. Y si bien, sus acciones no se refieren necesariamente al ámbito específico de la defensa cibernética, cubren una parte importante de ella.

Entre ellas es sin dudas la Unión Internacional de las Comunicaciones (UIT o ITU por sus siglas en inglés), la organización de las Naciones Unidas especializada en las

[73] Quedan excluidas de esta consideración, las organizaciones internacionales militares, tales como la OTAN, la cual desarrolla con plenitud, conceptos de defensa cibernética propiamente dichos.

Tecnologías de Información y Comunicación, quien lleva adelante los más ambiciosos programas en la materia.

La UIT desarrolla un programa internacional de seguridad al cual adhirieron la casi totalidad de sus ciento noventa y tres estados miembros.

Las siglas en inglés ICT (*Information and Comunication Techonologies*), preceden el nombre de sus programas y de todos ellos, el conocido por las siglas ICT4SDG[74], incluye al Programa Mundial de Ciberseguridad de la UIT conocido como *Global Cibersecurity Agenda* (GCA).

Este programa fue lanzado en 2007 por el entonces secretario general de la UIT, el Dr Hamadoun Touré y constituye, en el marco el marco de cooperación internacional, una herramienta cuya finalidad es mejorar la confianza y la seguridad en la edad de la información.

La CGA fue diseñada para incrementar la cooperación, la eficiencia y la colaboración con todos y entre todos los miembros, aprovechar las iniciativas existentes y evitar la duplicación de esfuerzos. Mediante proyectos de cooperación con los miembros, implementa en la actualidad, apoyo a soluciones de seguridad cibernética en varios países del mundo.

La mencionada agenda, basa su trabajo en cinco lineamientos estratégicos o áreas de trabajo (AT), a saber:

- **AT 1 Medidas legales**:
  Busca proporcionar asesoramiento sobre el modo en que debieran regularse las TIC[75] (s), mediante el desarrollo de una legislación consensuada internacionalmente.
- **AT 2 Medidas técnicas y procedimentales**:
  Aplicando para el software existente o en desarrollo, esquemas de acreditación, protocolos y estándares que garanticen que un alto nivel de seguridad en su empleo.
- **AT 3 Estructuras organizacionales**:
  Asesorando sobre el desarrollo de organizaciones y estrategias de respuesta para la prevención, respuesta y gestión de crisis producidas por ciberataques, incluyendo la protección de las ICIC.

[74] ICT4SDG: Siglas en inglés de *Information And Communication Techonolgies For Sustainable Development Goals* – Tecnologías de la Información y Comunicación Para Objetivos de Desarrollo Sustentable).
[75] TIC: Tecnologías de la Información y Comunicación.

- **AT 4 Creación de capacidades**:
  Creando mecanismos de generación de capacidades tendientes a concientizar, transferir conocimientos (Know How) e implementación de la temática en las agendas políticas nacionales.
- **AT 5 Cooperación Internacional**:
  Desarrollando estrategias de cooperación, diálogo y coordinación internacional frente a las amenazas cibernéticas.

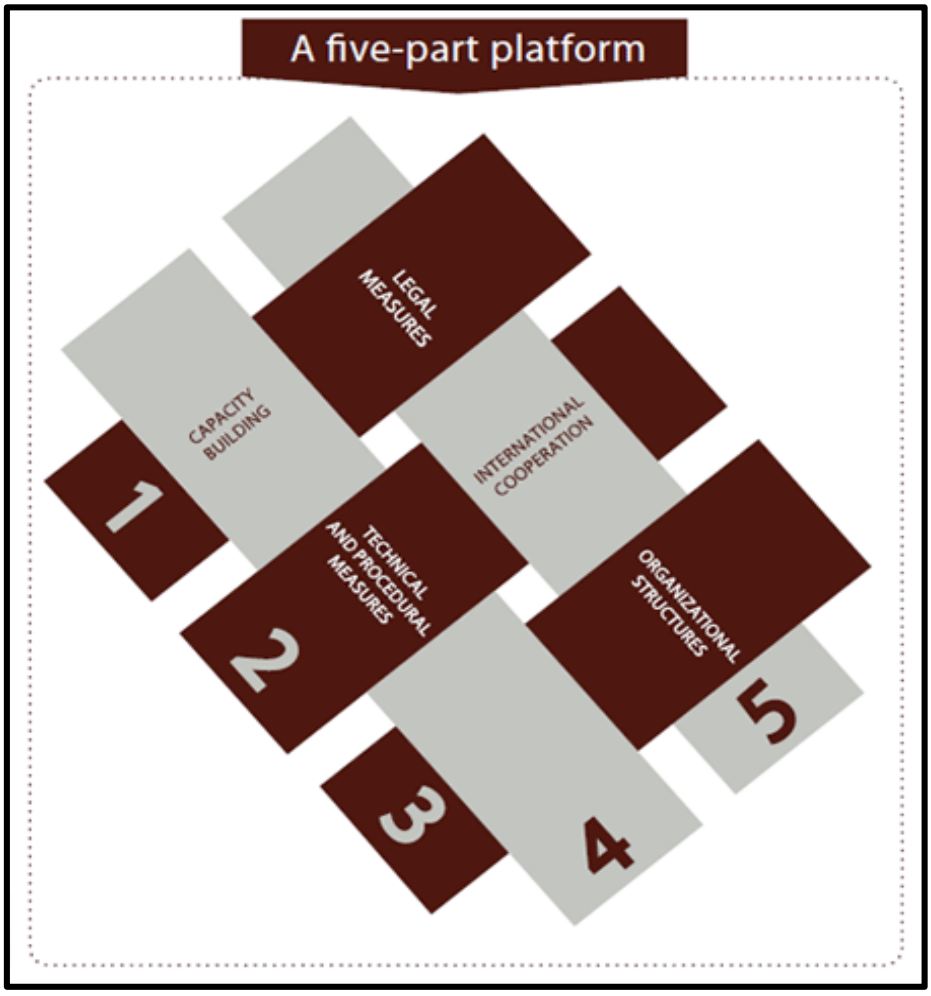


Figura 38: Áreas de Trabajo de la UIT (fuente UIT).

El logo de la GCA, muestra con claridad las cinco áreas de trabajo y expresa gráficamente la interacción imprescindible entre ellas.

El lanzamiento de la GCA y las recomendaciones que de ella surgen, fue apoyado por un grupo de expertos en seguridad informática, conocido como HLEG (*High Level Experts Group* – Grupo de Expertos de Alto Nivel), una comisión de trabajo integrada por más de cien expertos pertenecientes a sectores estatales y privados. Su

primer informe, fue entregado al Presidente de la GCA, luego de tres reuniones, finalizando el último de ellos el 28 de junio de 2008 (Report of the Chairman of HLEG to ITU – Secretary General, pág. 21).

Entre las recomendaciones que el HLEG dio en dicho informe, por área de trabajo, se pueden mencionar[76]:

AT 1:

- La UIT es un organismo líder en la materia y puede desarrollar un modelo de legislación sobre seguridad cibernética, compatible con las legislaciones nacionales factible de ser adoptado por los estados miembros.
- Los gobiernos deben cooperar con otras agencias para elaborar la legislación necesaria que permita la investigación y enjuiciamiento de los delitos cibernéticos, observando los marcos existentes.[77]
- El Convenio sobre Ciberdelincuencia de Budapest, constituye un marco de referencia importante, por lo cual debiera ser suscripto por la totalidad de los países o empleado para desarrollar las legislaciones nacionales respectivas.
- Dada la velocidad de desarrollo de las TIC(s) y las posibilidades cada día mayores de la ciberdelincuencia, es imprescindible el trabajo integrado de gobiernos, policías nacionales, Interpol y organizaciones privadas, para adecuarse constantemente a las amenazas.
- Durante la investigación y los procesos judiciales que se desarrollen frente al ciberdelito, los estados deberán asegurar el respeto de los derechos humanos y la privacidad individual, ateniéndose al derecho internacional que los regula.

AT 2:

- La UIT debería trabajar con otros centros de expertos a nivel mundial, para identificar, promover y fomentar la adopción de mejores procedimientos de seguridad y medidas técnicas. En tal sentido, se propusieron distintas normas de certificación internacional (Ej Normas y estándares ISO/IEC[78], JTC 1/SC 27, entre otros).

[76] Sólo se detallan aquellas sobre las cuales los expertos obtuvieron consenso total.
[77] Se citan a modo de ejemplo en el informe, las resoluciones de la Asamblea general de la ONU Nro 55/63 y 56/121, ambas con el título “Lucha contra la utilización de la tecnología de la información con fines delictivos”, de fechas 22 de enero de 2001 y 23 de enero de 2002. (ONU, RESOLUCION DE LA ASAMBLEA GENERAL NRO 55/63 Lucha contra la utilización de la tecnología de la).

[78] La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Entre ellas se

- La UIT debiera convertirse en un centro de excelencia para la recopilación y distribución oportuna de información relacionada con la seguridad cibernética.
- La UIT debería colaborar con organizaciones nacionales, fabricantes, desarrolladores y otros expertos para: 1) lograr la concientización sobre las respuestas anticipadas de incidentes; 2) la promoción y apoyo para que los CSIRT[79], se integren en un sistema global y 3) la colaboración para el desarrollo de herramientas y materiales que permitan establecer CSIRT nacionales, así como los medios de intercomunicación con ellos.
- Sugerencias respecto de la aplicación de la Identidad Digital.

AT 3:

- Se propuso desarrollar un "Índice de seguridad cibernética de cada país", la designación de un representante de Seguridad cibernética en cada estado, para tareas de coordinación internacional y la implementación de un CERT/CSIRT por cada estado miembro como organización básica y representativa de la ciberseguridad nacional.
- La mayoría de las recomendaciones, se refieren a la colaboración que la UIT debe proporcionar a los países en desarrollo y a los menos desarrollados, en las áreas técnicas, legal, organizativas y de concientización y aplicación de prácticas de ciberseguridad.

AT 4:

- La UIT, como centro de excelencia mundial, debería promover el desarrollo y la adopción de medidas y procedimientos de ciberseguridad, incluyendo procedimientos generales, medidas técnicas generales y medidas específicas para problemas o incidentes puntuales.
- Se debería incentivar a proveedores de productos y servicios de TIC(s) a aumentar sus medidas de seguridad informática y a apoyar las que deban emplear los usuarios finales de sus sistemas y programas.
- La UIT debe ser responsable de la educación de los actores involucrados en los distintos niveles de la sociedad de la información.

---

destacan las ISO/IEC 27001 (Estándares a cumplir por los Sistemas de gestión de Seguridad de la Información – SGSI) y la ISO/IEC 27035 (Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad). Esta última se enfoca en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Fue publicada en agosto de 2011.

[79] CSIRT: Computer Security Incident Reponse Team – Equipo de Respuesta de Incidentes de Seguridad Informática.

- La UIT debe continuar desarrollando la capacidad humana en todos los aspectos de ciberseguridad, como una forma de ayudar a la formación de una cultura global.
- UIT debe promover la formación de asociaciones público-privadas cuando sea necesario, para: incrementar la seguridad cibernética, desarrollar la cultura de seguridad y luchar contra el delito cibernético.
- La UIT debería hacer pleno uso de OONGG, bancos, bibliotecas, organizaciones comerciales locales, centros educativos, entes estatales administrativos, etc, para difundir y promover campañas de concientización de ciberseguridad.

AT 5:

Fueron diversas y numerosas las recomendaciones de esta área, las que se pueden resumir en la necesidad de que la UIT debiera crear un organismo dentro de ella que se convierta en un punto global de coordinación.

Como productos de las distintas áreas de trabajo, la UIT ha implementado programas de ayuda para estados miembros, que incluyen cooperación para el desarrollo de estrategias relacionadas, marcos legales, organizaciones tipo CSIRT/CERT, la difusión de estándares de cumplimiento, campañas de concientización, seminarios y reuniones, índices de desarrollo de seguridad informática nacionales y bibliotecas de consulta de documentos e informes, de fácil acceso a través de Internet.

Asimismo y con colaboración de la empresa de ciberseguridad IMPACT, propone el empleo de dos herramientas de seguridad conocidas como HORNET y AWARE.

Ambas pueden ser empleadas como parte de un CERT/CSIRT o en forma independiente en redes locales. HORNET[80] es en una red de sensores instalados en redes que alimentan en tiempo real, información relacionada a ataques o amenazas cibernéticas. Consisten en servidores señuelo cuya penetración por parte de amenazas, es facilitada de exprofeso y que permite una vez atacada, capturar información sobre malware y ataques en red, facilitando a quien lo emplea, comprender y mensurar las amenazas a las que se expone e implementar las contramedidas necesarias.

[80] HORNET: ***Honeypot Reaserch Network***. La traducción literal sería Red de Investigación Tarro de Miel. El término se define así por el hecho de constituir un sistema “enlatado”. Para más datos ver http://www.itu.int/en/ITU-D/Cybersecurity/Pages/HORNET.aspx

Por su parte AWARE[81] sirve a los CERT/CSIRT proporcionando alertas y datos de ataques a redes propias o a otras redes, procesando los datos y transmitiendo en tiempo real la información. Ambas herramientas se ofrecen en una variedad de opciones y en versiones gratuitas o con costo según el nivel de seguridad deseado.

Figura 39: HORNET y AWARE. Características y diferencias (fuente UIT).

Si bien la NATO es una organización eminentemente militar, la naturaleza cambiante del conflicto y la aparición de nuevas formas de amenaza a la seguridad nacional, la han llevado a involucrarse en forma directa en aspectos relacionados a la seguridad y defensa cibernética de las estructuras militares de la organización como así también otras estatales de cada estado miembro. Se han mencionado ya las consideraciones en que en relación a la amenaza que plantean los nuevos formatos de

[81] AWARE: **Abuse Watch Alerting & Reporting Engine**. Motor de alerta, control y reporte de abusos. Para más datos ver http://www.itu.int/en/ITU-D/Cybersecurity/Pages/AWARE.aspx

guerra, en particular las guerras híbridas, había definido la NATO (Ver Pag 57).

Desde sus orígenes esta organización, siempre ha hecho esfuerzos por la protección de sus sistemas de comunicación e información. Sin embargo fue recién en la Cumbre de Praga de 2002, cuando se incluyó por primera vez la problemática de la ciberdefensa en la agenda de la Alianza. La necesidad de incrementar la protección, quedó establecida en la Cumbre de Riga en 2006.

Los ataques sufridos por instituciones gubernamentales y privadas en Estonia, entre abril y mayo de 2007, provocaron que en junio de ese año, se iniciaran trabajos tendientes a lograr una rápida respuesta frente a ellos, presentándose en enero del 2008, la primera política de defensa cibernética de la Organización. En la Cumbre de Lisboa de 2010, se presentó un nuevo concepto estratégico de la NATO, el cual preveía el desarrollo de una política de defensa cibernética más profunda, con un plan de trabajo detallado para implementarla.

Este primer ensayo de una política de defensa cibernética de la organización, tuvo lugar en el año 2011 (NATO C. , s.f.). El objetivo de dicha política era el siguiente:

"Implementar una visión coordinada de ciberdefensa, que acompañe aspectos de planeamiento, capacidad de desarrollo y mecanismos de respuesta frente a ciberataques. Para ello es necesario:

a) *incorporar e integrar medidas de ciberdefensa para todas las misiones de la Alianza.*
b) *desarrollar una capacidad de defensa cibernética, incluyendo en los procesos de planeamiento de defensa de la NATO (NDPP[82]), guías para su integración en los marcos de referencia de defensa nacionales.*
c) *Proteger en forma centralizada, las redes propias, las de agencias dependientes y las de las misiones desplegadas en el exterior, para garantizar una infraestructura segura dentro de la cual puedan operar dichas redes."*

Los aspectos centrales de dicha política, incluían los siguientes conceptos:

- Integrar consideraciones relacionadas a la defensa cibernética en las estructuras de la OTAN y en sus procesos de planeamiento, a fin de ejecutar las acciones propias de la gestión de crisis y de la defensa.

[82] NDPP: *Nato Defense Planning Process*. Proceso De Planeamiento de Defensa de la Nato.

- Centrar los esfuerzos en la prevención, resiliencia y defensa de los activos cibernéticos críticos para la OTAN y sus aliados.
- Desarrollar capacidades de ciberdefensa y centralizar la protección de las redes propias de la organización.
- Desarrollar capacidades mínimas para la ciberdefensa de las redes nacionales críticas, que resulten necesarias para las tareas básicas de la OTAN.
- Proporcionar asistencia a los aliados para lograr un nivel mínimo de ciberdefensa y reducir las vulnerabilidades de las infraestructuras críticas nacionales.
- Participar en calidad de asociados, con organizaciones internacionales, sector privado y con el mundo académico en temáticas relacionadas a la ciberdefensa.

En abril del 2012, comenzó la integración de las tareas de ciberdefensa en los procesos de planeamiento de la defensa de la NATO, en los cuales, se identificaban y priorizaban los requisitos a satisfacer. En mayo (Cumbre de Chicago), se formalizó la centralización de todas las redes de la alianza y la actualización del NCIRC[83] (NATO, NATO Rapid Reaction Team to fight cyber attack, s.f.) y posteriormente la agencia NCIA[84].

En mayo de 2014, el NCIRC alcanzó Capacidad Operacional Plena (NCIRC FOC – *Full Operational Capability),* proporcionando una mayor protección a las redes y usuarios de la OTAN. El NCIRC se encuentra en el SHAPE (*Supreme Headquarters Allied Powers Europe* – Cuartel Supremo de las Potencias Aliadas de Europa), en Moms, Bélgica.

Este centro es responsable de la defensa de la totalidad de los sitios de la NATO, tanto de las instalaciones fijas como de las fuerzas desplegadas en misiones operacionales o ejercicios (NATO, NATO *Rapid Reaction Team to fight cyber attack*, s.f.).

En caso de un ataque a un sistema informático de la NATO, un equipo de expertos[85] se reúne para desarrollar un plan de trabajo, con el objetivo de recuperar el sistema afectado y devolver su funcionamiento normal lo antes posible. Para ello se analizan los sistemas afectados y el tráfico de la red atacada, con las intenciones de determinar el blanco inicial del ataque (entrada), la magnitud del daño ocasionado,

[83] NATO Computer Incident Response Capability.
[84] NCIA (*Nato Comunication And Information Agency*).
[85] Aunque no es público el nivel de experticia alcanzado, a modo de referencia, el jefe de la sección de ingeniería informática del NCIRC, Alex Vandurme, tiene el título de magister en tecnologías de información.

detener y reducir los efectos y de ser factible, determinar el origen y el atacante.

Los equipos de expertos, son conocidos como RRT (*Rapid Reaction Team* – Equipo de Reacción Rápida) y consisten en un núcleo permanente de seis miembros especializados, a los que se suman los expertos del país miembro atacado inicialmente. La cantidad definitiva, depende de la misión y magnitud del ataque. Cada RRT dispone del equipamiento necesario para las tareas, incluyendo equipos informáticos y de comunicaciones, telefonía satelital segura, equipos para recopilación de pruebas digitales, criptografía y forensia digital, análisis de tráfico, gestión de vulnerabilidades, etc.

Todos los miembros están entrenados en los procedimientos NATO STANAG[86].

En septiembre de ese año, 2014, durante la cumbre de Gales mencionada previamente, los aliados lanzaron una nueva política de defensa cibernética, la que incluía un plan de acción mejorado (NATO, *Wales Summit Declaration,* s.f.)

Entre los puntos salientes de esta política, pueden citarse los siguientes:

- Se mantiene inalterable el principio de indivisibilidad de la seguridad aliada, la prevención, detención, resiliencia, recuperación y defensa.
- La defensa cibernética constituye para los aliados, una parte de la tarea central de la OTAN. La asistencia a los aliados, debe hacerse con solidaridad, asumiendo cada estado, la responsabilidad de la protección de las propias redes nacionales.
- La OTAN reconoce que el derecho internacional se aplica en el ciberespacio, incluyendo al Derecho Internacional Humanitario y a la Carta de la ONU. El Consejo del Atlántico Norte, decidirá si un ataque cibernético, es causa para la aplicación del artículo 5 de la carta de la OTAN
- Cada estado miembro es responsable de la protección de sus propias redes.
- Se considerará al Ciberespacio como un Teatro de Operaciones más, integrando a la ciberdefensa en las operaciones de la OTAN, tanto en la planificación operacional como en las operaciones de contingencia[87].
- Ciberdefensa: es una cuestión prioritaria (responsabilidad e Interoperabilidad).
- Se reforzarán las capacidades educación cibernética, capacitación y ejercicios.
- Se deberán incrementar los esfuerzos para prevenir, mitigar y recuperarse de los

[86] STANAG: Siglas en inglés de *STAndarization Nato AGreement*.
[87] Operaciones de contingencia refiere a aquellas operaciones que no necesariamente impliquen el uso de la fuerza militar para el cumplimiento de sus propósitos. Pueden incluir operaciones de apoyo en caso de desastres naturales, operaciones de seguridad, apoyo a refugiados, operaciones de paz, etc.

ataques cibernéticos.

- Se reforzará la cooperación en materia de ciberdefensa a través de un mayor Intercambio de información, formación, investigación y ejercicios, entre los aliados y a nivel UE[88].
- Se intensificará la cooperación con la industria en materia de seguridad y de defensa cibernética.

Es en el caso de la NATO en el cuál se aprecia plenamente el proceso mencionado para enfrentar las amenazas cibernéticas.

La **identificación**, realizada a través de las distintas opiniones y consideraciones sobre los riesgos emitidas en informes, estudios y exposiciones de fin de conferencias.

El **desarrollo de políticas y estrategias**, demostrado en las elaboradas en 2011 y 2014, con actualizaciones constantes.

La elaboración del **marco legal** de referencia, primero con el Manual Tallinn y posteriormente con el Manual Tallinn 2.0..

Finalmente, la creación de **organismos especializados**, incluyendo al CCDCOE (NATO *Cooperative Ciberdefense Center of Excelence* – Centro Cooperativo de Ciberdefensa de Excelencia de la OTAN) ubicado en Tallin, capital de Estonia, al NATO CIRC mencionado y a los centros de defensa cibernética propios de cada estado miembro (por ejemplo el CCDE de Chievi – Italia, la ANSSI (*Agence Nationale de Sécurité des Systèmes d'Information*) y el Ciber Comando Operacional franceses o el

[88] Lo expresado en la política se concreta en hechos. Desde el año 2010, se viene desarrollando en el CCCDOE, el ejercicio de ciberdefensa "*Locked Shield*". El ejercicio es el mayor y más avanzado del mundo. Se desarrolla a dos partidos, su realización es anual y consiste en organizar una defensa de la red de la OTAN en tiempo real, de acuerdo a distintos escenarios planteados por la dirección del ejercicio y coincidentes con las previsiones de empleo de la organización. La intención es la de capacitar a los expertos en seguridad que protegen los sistemas nacionales de los estados miembros. Cada año, los equipos son sometidos a una intensa presión para mantener las redes y servicios de un país ficticio. Esto incluye manejar e informar incidentes, resolver desafíos forenses, y responder a comunicaciones legales y estratégicas y proyectos de escenarios. Las fuerzas enemigas en *Locked Shield* emplean tecnologías, redes y métodos de ataque realistas y de vanguardia.
El último, fue realizado entre el 24 y 28 de abril de 2017. Las fuerzas azules debían mantener los servicios y redes de una base aérea militar en un país ficticio que, según el escenario del ejercicio, experimentaría graves ataques a su sistema de red eléctrica, vehículos aéreos no tripulados, Sistemas de control, componentes de infraestructuras de información y comunicación y otras infraestructuras operacionales. Debido a que se emplean las últimas técnicas y procedimientos de agresión, las fuerzas azules (con cerca de 3000 sistemas informáticos) pueden ser atacadas por más de 2500 ciberarmas. Se desplegaron en Tallin cerca de 800 participantes de 25 naciones mientras que otros equipos azules, participantes tendrán acceso en línea seguro a las redes del ejercicio desde sus bases de origen. Además de elementos netamente militares, participan compañías civiles asociadas tales como Siemens AG, Threod Systems, Sistemas de Prueba Cibernética, Seguridad Clarificada, Iptron, Bytelife, BHC Laboratorio, GuardTime y otros.

Centro Criptológico Nacional (CCN) y el Centro de Respuesta ante Incidentes de Ciberseguridad del Ministerio de Defensa (ESPDEFCERT) españoles.

B. Los países frente a la amenaza cibernética.

A efectos de limitar el estudio, sólo se analizará y concluirá sobre estrategias, políticas y organizaciones específicas de los ámbitos de la defensa. Para Ello se considerará válido el concepto de "Seguridad Nacional", de aplicación generalizada en la mayoría de los estados[89].

Se analizarán los casos de EEUU, en función de ser uno de los estados que mayor desarrollo ha logrado y de Brasil, como un referente regional y por constituir en el marco de organizaciones regionales, un aliado con el cual la integración en la materia, sería muy beneficiosa para nuestro país.

1. Defensa cibernética en Estados Unidos:

a. Estrategias y organizaciones de la administración gubernamental, seguridad y públicas.

Si bien existe la percepción de los Estados Unidos como una potencia tecnológica e innovadora, está a la zaga de muchas otras naciones industrializadas modernas en términos de acceso a Internet y conectividad. La Unión Internacional de Telecomunicaciones lo ubica en el puesto 28 en el orden mundial en términos de porcentaje de personas con acceso a Internet en 2013, con un 84% de ellas conectadas *(CCCDOE N. , National Cyber Security Organisation*, s.f.).

Estados Unidos está hoy comprometido en fomentar la innovación tecnológica, enfocándose estratégicamente, en el aumento de Internet y el acceso a Internet de banda ancha.

El Congreso de los Estados Unidos ordenó a la Comisión Federal de Comunicaciones (FCC) desarrollar un Plan Nacional de Banda Ancha (NBP) a principios

[89] Las leyes Nro 23554 "Ley de Defensa Nacional" y Nro 24059 "Ley de Seguridad Interior", establecen claras distinciones entre la defensa (frente a agresiones externas) y la seguridad (orden dentro del territorio). Esta concepción, se aleja de las tendencias mundiales en las que la Seguridad Nacional, es el concepto empleado y que comprende a cualquier agresión contra el estado, sin importar su origen, finalidad y medios. Esta última definición, es particularmente adecuada para analizar la respuesta de los estados en materia de ciberdefensa.

de 2009 para contribuir a este objetivo. El plan, presentado en marzo de 2010, señaló el efecto positivo del acceso a Internet de banda ancha, como "una base para el crecimiento económico, la creación de empleo, la competitividad global y una mejor forma de vida" y asumiendo que el gobierno podría desempeñar un papel crucial, al acelerar el proceso de crecimiento de la infraestructura de telecomunicaciones del país. De acuerdo a este plan, para el año 2020, cien millones de ciudadanos tendrán la velocidad mínima de descarga de 100 Mbps[90] y de carga de 50 Mbps[91]. Este plan, deberá asegurar una mayor participación de los servicios electrónicos que el gobierno nacional y los estatales, brindan a los ciudadanos. En este sentido, EEUU se ubica en el séptimo lugar mundial en disponibilidad de servicios de gobierno a través de Internet. En 2002, se elaboró la *E-Governance Act* (Acta de gobierno electrónico), la cual sirvió de marco para su desarrollo y crecimiento e incluyó conceptos de ciberseguridad.

A pesar de que las calificaciones de la UIT no son tan altas como se podría pensar, sigue siendo un objetivo altamente rentable para todo tipo de amenazas.

Los EEUU fueron alertados sobre los peligros de la guerra cibernética desde los años 90, tal el caso de Arquilla y Rondfeldt.

Estados Unidos fue el primer país del mundo en desarrollar, publicar y difundir, una Estrategia de Seguridad Cibernética, en el año 2003. Para mensurar lo avanzado de su elaboración en su momento, los países que lo siguieron fueron Alemania en 2005 y Suecia en 2006.

Esta estrategia tenía tres objetivos básicos:

- Prevenir ciberataques contra las infraestructuras críticas de información y comunicación de los EEUU.
- Reducir la vulnerabilidad de los EEUU a los ciberataques.
- Minimizar los daños y el tiempo de recuperación en caso de ataques cibernéticos.

Para alcanzarlos, se fijaron cinco prioridades: asegurar los sistemas informáticos y redes de la administración federal, implementar un sistema de respuesta, desarrollar un programa de reducción de amenazas y vulnerabilidades, implementar un programa de

[90] Mbps: Megabytes por segundo: es una medida de velocidad de transferencia de datos.

[91] Las velocidades promedio ofrecidas a la fecha de presentación de esta tesis, por los prestadores de Internet en Argentina, varían de entre 6 Mbps (Arnet) y 50 Mbps (Fibertel) a un costo de entre 25 a 100 U$D mensuales. El plan de Fibertel requiere además disponibilidad de fibra óptica de esa capacidad en el área de instalación.

concientización y educación sobre ciberseguridad y finalmente, desarrollar un sistema de cooperación internacional.

La guerra cibernética ya fue definida como uno de los riesgos más importantes a los EEUU, en la Estrategia de Seguridad Nacional del año 2006, y desarrollada aún con más énfasis en el año 2010.

Si bien no es una política específica en materia de ciberdefensa, la Estrategia de Seguridad Nacional del año 2010 (NSSR 2010), fue la primera de su tipo que incluyó a las ciberamenazas como un elemento determinante en condiciones de afectar la seguridad de los EEUU.

Esta estrategia establece como una de las prioridades para alcanzar la seguridad nacional (esencialmente la del propio territorio), la siguiente:

"Salvaguardar y asegurar el ciberespacio".

En mayo de 2011, la Casa Blanca difundió la *International Strategy For Cyberspace* , la cual refleja la forma en que EEUU considera a los socios internacionales en a materia y comunica las prioridades nacionales.

El objetivo principal enunciado en esta estrategia es el siguiente:

"Los Estados unidos trabajarán internacionalmente para promover una infraestructura de información y comunicaciones abierta, interoperable, segura y confiable, que apoye el intercambio y comercio internacional, fortalezca la seguridad internacional y que fomente la libertad de expresión e innovación. Para alcanzar este objetivo, nosotros construiremos y sostendremos un ambiente en el cual, normas de comportamiento responsable guíen las acciones de los estados, sostengan las organizaciones internacionales, y apoyen la aplicación de la ley en el ciberespacio" (*The White House*, pág. 8).

Esta estrategia divide las metas en diplomáticas, de defensa y de desarrollo, estableciendo prioridades para la totalidad del gobierno federal en siete áreas de actividad (economía, protección de redes nacionales, ley y orden, militar, gobierno electrónico, desarrollo internacional y libertad de empleo de internet).

También describe y ordena cronológicamente los principales documentos estratégicos relacionados con ciberseguridad, permitiendo así alcanzar una visión integral de cómo el gobierno enfrentará los desafíos en la materia. Los documentos han sido

también agrupados dentro de ella, en tres grupos: los que regulan la ciberseguridad de las redes federales, los que apuntan a la protección de infraestructuras críticas (CIP – *Critical Infraestructure Protection*) y aquellos documentos militares relacionados a aspectos de ciberseguridad que hacen a la Seguridad Nacional y a la Defensa.

La Estrategia Nacional de Seguridad, emitida en 2017, reconoce el creciente riesgo que los ciberataques disruptivos[92] y destructivos tienen para los EEUU, comunica la intención de fortalecer la protección de las infraestructuras críticas, incrementar la inversión en ciberseguridad y ciberdefensa e imponer "costos[93]" a los actores maliciosos en el ciberespacio[94].

También expresa el objetivo de los EEUU de promover normas internacionales para regular el empleo del ciberespacio.

Tal como se expresó precedentemente, la creación de organismos especializados en seguridad cibernética, fue simultánea con las estrategias y en algunos casos, previas.

El principal organismo responsable de la seguridad cibernética de las redes federales y de las infraestructuras críticas, es el FISMA[95], creado como consecuencia del Acta de Gobierno Electrónico de 2002. Este organismo impuso la aplicación de un sistema de gestión de riesgos desarrollado por el *National Institute of Standars and Technology* (NIST), con la intención de estandarizar los procedimientos de ciberseguridad en todas las agencias de gobierno.

El FISMA fue duramente criticado y en 2014 se emitió una enmienda tendiente a su optimización. Se promulga entonces la *National Response Framework* (Marco de Respuesta Nacional), tendiente a regular las acciones preventivas y reactivas para enfrentar amenazas. Además de guías, exigencias y metas a alcanzar por los distintos organismos de la administración federal, se establecen responsabilidades de coordinación y ejecución de acciones ante incidentes, bajo la dirección del *National Cybersecurity and Communications Integration Center* (NCCIC) y su organismo dependiente, el US-CERT.

---

[92] Si bien el significado literal es "que produce disrupción", el término se asocia al concepto de dislocamiento empleado en la doctrina del Ejército, como un efecto que corta los lazos tácticos entre elementos.

[93] Se refiere específicamente a daños.

[94] En este sentido, se mantiene lo enunciado por la NSS 2015 con la administración Obama.

[95] *Federal Information Security Management Act.*

En la actualidad, la estructura de ciberseguridad nacional queda estructurada de acuerdo al siguiente organigrama:

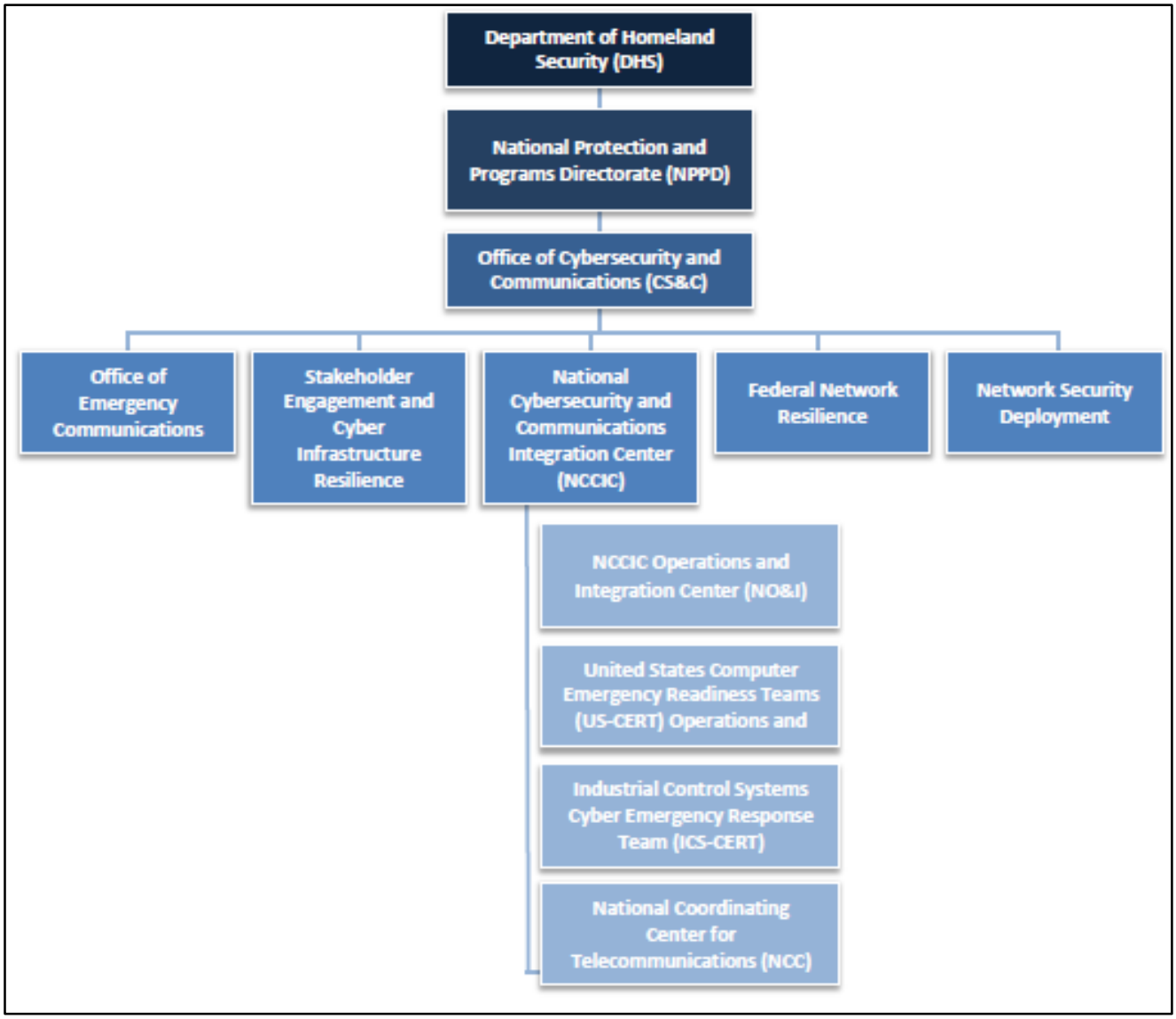


Figura 40: Estructura de seguridad y defensa cibernéticas de EEUU. (NATO CCDCOE).

La responsabilidad directiva de las acciones recaen en el Departamento de Justicia (DoJ), a través de la División de Seguridad Nacional (NSD - *National Security Division*). Esta ha creado la Red de Seguridad Nacional de Especialistas en Cibernética (NSCSN – *National Security Cyber Specialists Network*), la que integra redes de otras agencias para una mejor gestión de las amenazas, incluso las originadas en otros

estados y en grupos terroristas.

La ejecución de acciones de protección específicas, no obstante, son responsabilidad del Departamento de Seguridad Interior (DHS – *Department of Homeland Security*) y su dependencia ejecutiva, la Oficina de Ciberseguridad y Comunicaciones (CS&C – *Office of Cybersecurity and Communications*), en todo lo relacionado a organismos de gobierno y administrativos, redes civiles e infraestructuras críticas (fundamentalmente a través de empresas de ciberseguridad asociadas). De ella depende el Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC – *National Cybersecurity and Communications Integration Center*) con dos organismos especializados en respuestas a ciberataques, el US CERT (*United States Computer Emergency Readiness Team*) ya mencionado y el *Industrial Control System Cyber Emergency Reponse Team* (ICS-CERT). Aunque parezca un aspecto menor, la diferencia de ambos CERT radica entre los términos *Readiness* (en el sentido de alistados rápidamente) y *Reponse* (respuesta, en el sentido de atención integral).

Cabe mencionar que el NCCIC y sus dependientes, tienen responsabilidad en actividades de inteligencia, prevención, detección y respuesta ante todo tipo de amenazas, dejando a las organizaciones del DoD (*Department of Defense*), las relacionadas específicamente al ámbito de la defensa.

b. Estrategias y organizaciones del ámbito de la Defensa.

El Departamento de Defensa (DoD) tiene la misión de asegurar todas las redes de dominio *.mil* y la infraestructura de comunicación e información global frente a ciberataques. Adicionalmente, tiene la responsabilidad de realizar inteligencia sobre amenazas cibernéticas extranjeras, asegurar redes y sistemas de seguridad nacional y militar e investigar los ciberdelitos ocurridos bajo jurisdicción militar.

Se elaboraron diversas estrategias específicas, para operaciones en el ciberespacio. La primera de ellas, se presentó en el año 2006 y fue difundida por el Jefe del Estado Mayor Conjunto. Conocida como *National Military Strategy for Cyberspace Operations,* fue el primer documento que describió una aproximación conceptual de las operaciones de las FFAA estadounidenses en el ciberespacio. Asimismo define que el rol de las fuerzas armadas es asegurar los intereses de EEUU, desarrollando operaciones en el ciberespacio. Según el documento, el DoD depende del ciberespacio para alcanzar

los objetivos militares en el área militar propiamente dicha, en inteligencia y en operaciones comerciales.

En julio de 2011, se difundió la Estrategia del Departamento de Defensa (DoD) para Operar en el Ciberespacio (*Department of Defense Strategy for Operating in Cyberspace*). De manera directa, desarrolla cinco iniciativas estratégicas en materia de ciberdefensa.

Ellas son:

- Tratar al ciberespacio como un ámbito operacional para organizar, entrenar y equipar fuerzas, a fin de que el Departamento de Defensa puede aprovechar al máximo su potencial.
- Emplear nuevos conceptos defensivos para proteger las redes y sistemas del DoD (Departamento de Defensa) y las asociadas.
- Colaborar con otros departamentos y agencias del gobierno y del sector privado para permitir una elevada ciberseguridad a todos los niveles del gobierno.
- Construir relaciones sólidas con aliados y socios internacionales para reforzar la ciberseguridad colectiva.
- Aprovechar el ingenio, mano de obra cibernética excepcional y la innovación tecnológica de la nación.

En consonancia con ello, en 2014 se da a conocer la *Quadrennial Homeland Security Review* (Revisión Cuadrienal de Seguridad de la Nación[96]), la cual prioriza inversiones para apoyar los intereses y misiones relacionadas al control del ciberespacio y describe a las ciberamenazas como un serio riesgo a la seguridad nacional. Asimismo, fija al Departamento de Defensa (DoD) la tarea de desarrollar y expandir capacidades para desarrollar cualquier tipo de operaciones en el ciberespacio, tanto para la defensa del territorio como para apoyar operaciones militares en todo el mundo.

Establece también el rol principal del DoD en el ciberespacio: *"defender la integridad de las redes, proteger nuestros sistemas y redes claves, conducir operaciones cibernéticas en todo el mundo a orden y defender a la nación contra un ciberataque destructivo inminente[97] contra los intereses vitales de los EEUU."*

[96] Traducción del autor.

[97] De nuevo la controversia de cuáles son los parámetros para definir el nivel de destrucción potencial para definirlo como destructivo, cómo y cuándo se lo considera inminente y finalmente, la "defensa contra ese

En 2015, el DoD emitió la *Department of Defence Cyber Strategy of 2015*, una actualización de la original del 2011 en la que se establecen una serie de metas a alcanzar en la materia. Ellas son:

- Crear y mantener fuerzas alistadas y capacidades para conducir operaciones en el ciberespacio.
- Defender las redes de información, asegurar los datos y mitigar los riesgos de las misiones del DoD.
- Estar preparado para defender la nación y sus intereses vitales de ataques disruptivos o destructivos de consecuencias significativas.
- Construir y mantener opciones cibernéticas viables y previsiones para su empleo a fin de lograr controlar la escalada del conflicto y conformar el ambiente del conflicto en todas sus etapas.
- Construir y mantener alianzas internacionales robustas y socios para detener amenazas compartidas e incrementar la seguridad y estabilidad internacional.

Dentro del DoD, uno de los elementos claves para operaciones en el ciberespacio, es el CIO (*Chief Information Officer*) u Oficial Jefe de Información. Esta es una dependencia cuya misión es “asegurar el acceso a la información en cualquier dispositivo, en cualquier oportunidad, en cualquier condición, donde quiera que sea que el guerrero lo necesite”. Si bien abarca un espectro de funciones que excede la temática en sí, las responsabilidades son amplias.

Para tener una idea de la magnitud de personal y medios a los cuales el CIO/DoD debe asegurar la disponibilidad de información, hacia principios de 2014, el DoD incluía al personal y medios que se detallan (CIO):

1. Personal:
   - Militares: aproximadamente 1.4 millones.
   - Civiles: aproximadamente 783000.
   - Guardia Nacional y Reserva: aproximadamente 1,2 millones.
   - Familiares de personal activo: aproximadamente 5.5 millones

2. Infraestructura:
   - Despliegue: en 146 países.

---

ataque inminente” contempla acciones de guerra preventiva (sean con medios militares convencionales o con medios cibernéticos).

- Cuarteles: más de 5000
- Construcciones y estructuras: más de 600000

3. Sistemas relacionados a Información y comunicaciones:
   - Más de 10000 sistemas desplegados en operaciones reales permanentemente.
   - 1700 centros de datos.
   - 65000 servidores.
   - Más de 7 millones de computadoras y sistemas de tecnología de información.
   - Cerca de 550000 teléfonos móviles (493000 Blackberries, 41000 Iphone (iOS) y 8700 móviles con sistema Android.

El CIO ha producido una serie de directivas y documentos que incluso, regulan el empleo de telefonía celular y ordenadores personales en el campo de combate.

Existen otros documentos que si bien carecen de la entidad de una estrategia del máximo nivel, se han desarrollado reglamentos y manuales equivalentes a directivas, marcos y normativas de ciberseguridad aplicables en ámbitos no militares.

Ellos son:

- *Information Operations* (JP 3-13): es una publicación doctrinaria conjunta para el planeamiento, la preparación la ejecución y la evaluación de operaciones de información en todo el espectro de operaciones que desarrollan las fuerzas armadas. Fue implementado en 2012 y actualizado en 2013 con un anexo de lecciones operacionales aprendidas.
- FM 3-38 - *Cyber Electromagnetic Activities* (2014): es un manual del Ejército que brinda orientación doctrinaria para conducir actividades cibernéticas y electromagnéticas, así como tácticas y procedimientos para su planeamiento, integración con operaciones convencionales y sincronización.
- FM 3-12 – *Cyberspace and Electronic Warfare Operations* (abril de 2017): Este manual que derogó al anterior, establece conceptos generales y definiciones sobre las operaciones electrónicas y cibernéticas, su interrelación con operaciones convencionales, su planeamiento y conducción, etc. Entre las definiciones, se destacan las operaciones ciberofensivas (aquellas destinadas a proyectar el poder militar en el ciberespacio), las que solo se ejecutarán bajo la orden del CCMD (comando a cargo de las operaciones) y del *United States Cyber Command* (USCYBERCOM).

  Otro de los aspectos de interés, es la existencia de un formulario para requerir a

niveles Cuerpo de Ejército e inferiores, efectos cibernéticos sobre blancos enemigos.

En el gráfico siguiente, se muestran los efectos sugeridos en un ejemplo del manual.

Table 3-9. Examples of simultaneous and complimentary effects

Target Description	Target System Components	System Subcomponent Aimpoint	Desired Effects by Various Army Capabilities
Integrated air defense forces	Early warning radars	Supporting network	Destroy (primary equipment) Disrupt (cueing flow) Degrade (sensor integrity) Deceive (operators and leadership)
	Support facilities	Public switched telephone network	Destroy (supporting nodes) Disrupt (command and control systems) Deny (secondary battery access)
Enemy safe haven	Virtual locations	Host server	Destroy (supporting nodes) Exploit (data and information) Degrade (content) Disrupt (data flow) Deceive (through false bonafides)
	Key personnel (for example, leaders, facilitators, and enablers)	Smartphone	Disrupt (command and control systems) Deny (access) Deceive (through false persona)

Figura 41: Tabla de efectos simultáneos o complementarios en el ciberespacio (FM 3-12 – *Cyberspace and Electronic Warfare Operations)*.

- Plan X: es un programa de guerra cibernética de la Agencia de Investigación de Proyectos avanzados DARPA (*Defence Advanced Research Projects Agency*), tendiente al desarrollo de procesos de planeamiento y conducción de ciberguerra de forma similar a una guerra convencional.

Las operaciones en el ciberespacio, son realizadas a través de varias agencias a saber: el USCYBERCOM *Join Operations Center (United States Cyber Command*), el Centro de Servicios de Seguridad Central (*Central Security Service Center*) dependiente de la Agencia de Seguridad Nacional (NSA – *National Security Agency*), el Centro de Ciberdelito de la Defensa (*Defense Cybercrime Center*) y la DISA (*Defense Informacion*

System Agency – Agencia de Sistemas de Información de la Defensa),ésta última responsable, de la protección de las redes militares.

Cada una de las fuerzas, tiene un comando cibernético que depende funcionalmente del USCYBERCOM[98]. Éste tiene su sede en Fort Meade, Maryland, compartiendo instalaciones con la NSA. De hecho el comandante del USCYBERCOM es a su vez Director de la NSA.

El USCYBERCOM fue creado el 21 de mayo de 2010, alcanzando capacidad operacional inicial (IOC) en el mismo año (Ortiz, 2012).

. Su misión es *"planear, coordinar, integrar, sincronizar y conducir actividades para dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acción a los Estados Unidos y sus aliados en el ciberespacio e impedir lo mismo a los adversarios*"[99].

Sus comandos dependientes pertenecen a cada una de las fuerzas y son el ARCYBER (*Army Cyber Command / 2nd Army*), la *US Fleet Cyber Command 10th Fleet* (FCC/C10F), AFCYBER (24th Air Force), el MARFORCYBER (*US Marine Corps Forces Cyberspace*) y el *Coast Guard Cyber Command* (CGCYBER) cada uno de ellos al mando de un oficial del rango de general de tres estrellas o equivalente. Existen otros dos comandos subordinados aunque de menor entidad (CCCDOE, 2016). Estos son el 9th *Signal Command* (NETCOM), y el *U.S. Intelligence and Security Command* (INSCOM), ambos conjuntos.

USCYBERCOM tiene la responsabilidad primaria de comando y control de operaciones en el ciberespacio, incluyendo su planeamiento, sincronización con otras operaciones y ejecución.

Además lidera la seguridad de las redes del DoD, mediante la coordinación con otras agencias del DoD, apoya la ejecución de operaciones y conduce la ejecución de

[98] El USCYBERCOM es un comando subordinado al USSTRATCOM (United States Strategic Command).

[99] azMD5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT. La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. Como anecdóta, en su escudo figura un texto codificado en el algoritmo MD5que expresa "9ec4c12949a4f31474f299058ce2b22a", y cuyo significado es la misión del comando.

operaciones militares en el ciberespacio que se le ordenen.

Si bien cada comando dependiente realiza sus misiones en forma ligeramente diferente, el USCYBERCOM asegura la coordinación y coherencia de todas las operaciones y actividades cibernéticas.

Sus dos objetivos básicos son: *"garantizar la defensa de la propia estructura de TI para permitir el logro de la superioridad en el comando y control"* y *"ejecutar operaciones de guerra electrónica, inteligencia de señales e informática en todos los ámbitos de actuación de sus componentes".*

Entre sus cinco prioridades de trabajo, se destacan las siguientes:

- Crear una fuerza cibernética capacitada y preparada, conocida como CMF (*Cyber Mission Force*).
- Emplear herramientas que creen una verdadera conciencia de la situación en el ciberespacio.
- Asegurar disponer de políticas, leyes adecuadas y autoridades que permitan ejecutar operaciones en el ciberespacio, en todo el espectro del conflicto.

La CMF completa alcanzará un efectivo de 6000 militares y civiles y dispondrá de cuatro diferentes tipos de equipos de trabajo[100].

Finalmente entre sus planes de evolución, se desarrollará un polígono de armas cibernéticas, para desarrollar simulaciones sobre operaciones en el ciberespacio y probar nuevos sistemas y tecnologías y un Centro de Operaciones Conjunto (*Joint Operations Center*) para el año 2018.

Cabe aclarar que cada comandante en operaciones, dispone de su propio Centro de Comando Conjunto de Combate en el Ciberespacio (*Combatant Command Joint Cyberspace Centre* o CCJCC), los cuales reciben apoyo del USCYBERCOM, incluyendo el establecimiento de las redes de operaciones y su seguridad durante las acciones.

El *Army Cyber Command* (2nd Army) por su parte, y en forma similar a la Fuerza

[100] A fines de 2016, se preveía desarrollar la *Cyber Mission Force* (CMF). La CMF dispondrá de cuatro tipos de equipos: los *National Mission Teams*, para apoyo en caso de ataques de impacto nacional, los *Cyber Protection Teams* para la defensa de las redes y sistemas prioritarios y para apoyar operaciones militares en todo el mundo; los *Combat Mission Teams*, en apoyo a planes operacionales de comandos estratégicos y en operaciones de contingencia y finalmente los *Support Teams*, para apoyar procesos de análisis y el planeamiento.

de Oposición (OPFOR)[101], dispone de la WCCO o *World Class Cyber* OPFOR (Fuerza Enemiga de Clase Mundial), la cual participa como ciberenemigo en ejercicios con tropas convencionales, para instruirlas y concientizarlas respecto a la nueva amenaza.

En la misma dirección, la Armada de los EEUU (US NAVY), está planificando desarrollar el "Top Gun de la guerra de la información, a través del nuevo *Naval Information Warfighting Development Center* (NIWDC)" (Cowan, 2017, pág. 27). Este centro alcanzó capacidad operacional inicial a fines de marzo del 2017, previéndose alcance capacidad operacional plena (FOC – *Full Operational Capability*) en abril de 2019.

El proyecto tiene tres metas principales. La primera de ellas, desarrollar instructores especializados en las distintas ramas de la ciberdefensa (WTI – *Warfare Tactics Instructor*), de manera similar a los pilotos instructores del USNSFTI (*United States Navy Strike Fighter Tacticts Instructor*). Las otras metas son la de proporcionar entrenamiento avanzado en todas las ramas de la guerra de la información y desarrollar la doctrina relacionada, la cual incluye la elaboración de tácticas y procedimientos operativos normales (PPOONN) y entrenamiento.

Si bien el concepto *Information Warfare*, es abarcativo del específico de ciberguerra, ésta ocupa un lugar central en el desarrollo del centro.

Los programas de concientización del DoD sobre los riesgos que se corren en el ciberespacio, han tenido un efecto aceptable. A modo de ejemplo, La Guardia Nacional de Louisiana, desarrolla actividades de entrenamiento de equipos de seguridad cibernética en un polígono instalado en la LSU (*Louisiana State University*). La idea común de que los ciberataques originados fuera del país son un problema de nivel nacional, no contempla que los blancos atacados son locales, diversos, masivos y distribuidos geográficamente en el territorio de un país. Para enfrentarlos con éxito o reducir sus efectos, es importante contar con capacidades locales (anillos de protección), siempre con el apoyo y supervisión de organismos nacionales. Con importantes infraestructuras críticas a lo largo del río Misissipi, las autoridades de Louisiana han detectado importantes fallas de seguridad, empleando a equipos de la Guardia Nacional

[101] La OPFOR, era un elemento de nivel brigada, organizada, equipada e instruida de acuerdo al modelo soviético yque actuaba de enemigo en el NTC (Centro Nacional de Entrenamiento) aplicando los procedimientos del Pacto de Varsovia. Aunque aún se mantiene, se ha reestructurado para oficiar de enemigo de acuerdo a las operaciones en curso actualmente (guerra contra el terrorismo, ambientes urbanos, guerra asimétrica, etc).

para detectarlas, subsanarlas y en caso necesario, efectuar tareas de seguridad ante ataques reales (Fryer-Bigss, 2017, pág. 22).

Como se señaló previamente y a pesar de la impresionante estructura física, tecnológica y organizativa de EEUU, el punto más débil sigue siendo el marco legal.

Sin existir la regulación de organismos internacionales, los congresistas Rogers y Ruppersberger[102], presentaron un proyecto de ley conocido con la sigla CISPA *(Cyber Intelligence Sharing and Protection Act*). Patrocinado por varias organizaciones de telecomunicaciones y compañías informáticas[103], el proyecto pretendía el intercambio de datossobre ciberamenazas entre empresas y gobierno, para aumentar su seguridad. En su formato original y por considerarla una seria amenaza a las libertades individuales (Govtech, 2013), la administración Obama, amenazó con vetarla. Su aprobación requirió realizar importantes modificaciones al proyecto inicial ((Portaltic Europress, 2013). Fue introducida en 2015.

Los esfuerzos de EEUU para lograr un marco legal adoptado internacionalmente, tienen la misma consistencia que cualquiera que pueda proponer el estado menos desarrollado.

En el ámbito específico de la defensa, el DoD ha publicado en junio del 2015 el DoD Law Of War Manual (Manual de leyes de guerra del Departamento de Defensa), cuyo capítulo 16, se refiere a Operaciones cibernéticas (Department of Defense, 2015, pág. 94).

En términos generales, sigue los lineamientos del Manual Tallin, respecto a la aplicación del Derecho Internacional de los Conflictos Armados, la aplicación del Artículo 51 de la carta de la ONU (Legítima defensa), el derecho que se reserva EEUU de responder en forma preventiva o reactiva ante ataques (de forma proporcional y equilibrada) y distintas consideraciones respecto a lo que el uso de la fuerza definido en el artículo 2 de la carta de la ONU, significa en el ciberespacio.

Cabe acotar que no impone restricciones para responder de manera cibernética

[102] Presidente y miembro de mayor rango del Comité de Inteligencia de la Cámara de Representantes, respectivamente.

[103] National Cable & Telecommunications, TechNet, Cellular Telecommunications Industry Association, Association, US Telecom Association y las empresas McAfee, AT&T, Comcast, IBM, Intel, Oracle, Verizon y Time Warner Cable. Facebook y Microsoft, inicialmente patrocinadores de la ley, restaron su apoyo en la actualidad.

ante acciones hostiles que no califiquen como uso de la fuerza.

2. Defensa cibernética en Brasil:

Brasil, con un grado de desarrollo menor, sigue un rumbo similar.

Uno de los precursores en el proceso de concientización, fue el profesor Fernando Sampaio, quien publicó en 2003 "*Ciberguerra. Guerra Eletrônica e Informacional – Um Novo desafio Estratégico*", advirtiendo sobre los riesgos potenciales y las medidas necesarias para reducirlos.

Años más tarde, el 18 de diciembre de 2008, el presidente de Brasil, a través del Decreto Nro 6703, difundió la "*Estratégia Nacional de Defesa*"(EDN). En ella se define al sector cibernético, como uno de los tres vectores de importancia estratégica para la defensa nacional, junto a los sectores espacial y nuclear.

Si bien el término cibernético está tomado en su máxima amplitud, es decir referido al dominio de todas las tecnologías que involucren sistemas informáticos (navegación, comunicaciones, guiado de armas, control de infraestructuras críticas, interoperabilidad entre organizaciones militares y con agencias civiles, operaciones en red, diseño y desarrollo de sistemas de armas, etc), el último punto referido al tema cibernético, establece como necesario, lo siguiente: *"…El perfeccionamiento de los dispositivos y procedimientos de seguridad que reduzcan la vulnerabilidad de los sistemas relacionados con la Defensa Nacional contra ataques cibernéticos y, en su caso, que permitan su pronto restablecimiento, a cargo de la Casa Civil de la Presidencia de la República, de los Ministerios de Defensa, Comunicaciones y Ciencia y Tecnología, y del GSI-PR[104]…"* (Presidencia de la República Casa Civil, 2008)

Si bien Brasil no tiene un organismo nacional oficialmente reconocido como el responsable de elaborar e implementar estrategias, políticas y agendas nacionales de seguridad cibernética, de manera centralizada, las responsabilidades son compartidas entre las siguientes instituciones:

- Consejo de Defensa Nacional encargado de planificar y conducir la política y estrategia de defensa nacional.

[104] GSI-PR: *Gabinete de Segurança Institucional da Presidência da República*. Gabinete de Seguridad Institucional de la Presidencia de la República.

- Gabinete de Seguridad Institucional de la Presidencia de la República, responsable de proponer directrices y estrategias relacionadas con la ciberseguridad en el ámbito de la Administración Pública Federal, a través del Departamento de Comunicación, Información y Seguridad.

- Centro de Defensa Cibernética del Ejército de Brasil

- Agencia Brasileña de Inteligencia (se presume realiza actividades de inteligencia cibernética)

- Ministerio de Justicia - Departamento de Policía Federal (actividades relacionadas con ciberdelito).

En 2009 y siguiendo las directrices establecidas en la EDN, se incluyó a la defensa cibernética en el ámbito del Ejército y un año más tarde, se creó el *Centro de Defesa Cibernética* (CDCiber), mencionado precedentemente.

Su misión principal, es la de "Planificar, dirigir y controlar las actividades operacionales, la inteligencia, la doctrina, la ciencia y la tecnología y la formación dentro del Sistema Militar de Ciberdefensa". Asimismo, es responsable de "desempeñar las actividades operacionales y de inteligencia dentro del Sistema Militar de Ciberdefensa".

En la actualidad y luego de un intenso proceso de capacitación de su personal[105], el CDCiber desarrolla diez proyectos, entre ellos la Red Nacional de Seguridad de Información y Criptografía (RENASIC) y la elaboración de doctrina específica relacionada.

Entre las actividades y productos del CDCiber, se pueden mencionar:

- Implementación de aspectos enunciados en la Política de Defensa Cibernética
- Desarrollo de la Doctrina Militar de Defensa Cibernética
- Curso de Guerra Cibernética
- Elaboración del Antivírus DEFESA.BR (BluePex)
- Desarrollo de un Simulador de Operaciones Cibernéticas (RustCom)
- Gestión de Riesgos (Módulo)
- Investigación y Análisis.

[105]Panda Security firmó un acuerdo con el Ejército de Brasil para la capacitación del personal, en total unos 700, con responsabilidad en la lucha contra el terrorismo cibernético, el delito cibernético y las acciones estratégicas propias de la guerra cibernética. Asimismo, provee protección para más de 37500 computadoras del Ejército. Más datos se pueden encontrar en http://www.securityweek.com/brazilian-army-get-cyberwarfare-training-and-security-support-panda-security de fecha 28 de septiembre de 2010, abierta por el autor el 30 May13.

- Autoridad Certificadora de Defensa

Una de sus primeras intervenciones, ocurrió en junio de 2012 con motivo del desarrollo de la Conferencia de la ONU para el Desarrollo Sustentable. En lo que se conoció como Operación Río +20, el CDCiber instaló, coordinó e integró la operación del Destacamento de Defensa Cibernética (DstDefCiber) en las instalaciones de Riocentro (Río de Janeiro), para la seguridad cibernética de la conferencia.

Esta operación, pionera en su tipo en Brasil, fue la primera en abordar la problemática de la defensa cibernética de forma integrada en el ámbito gubernamental. Se registraron cerca de 130 eventos de seguridad, no obstante los cuales, los activos de información del evento, permanecieron íntegros y a salvo durante toda la conferencia.

El CDCiber, participó además en otros eventos desarrollados en Brasil, entre los cuales se pueden mencionar la Copa de las Confederaciones de 2013, los ejercicios militares Agata, Panamax, las operaciones Dínamo, Amazonia, Lançador y Atlántico, el campeonato mundial de fútbol FIFA 2014 y los Juegos Olímpicos Río 2016.

Particularmente durante la copa mundial de fútbol, operó con un Destacamento de Defensa Cibernética Central (Brasilia) y doce Destacamento de Defensa Cibernética Remotos, ubicados en cada una de las sedes en las que se desarrollaban los encuentros deportivos. Durante el evento, se registraron 756 eventos de seguridad sin que los sistemas informáticos afectados a la organización, dejaran de funcionar correctamente.

Brasil, es otro de los tantos ejemplos en los cuales, la creación de organismos especializados en ciberseguridad o ciberdefensa, precedió a la elaboración de las políticas y estrategias que debieron haberlos originado.

Así, el 21 de diciembre de 2012, el Ministerio de Defensa, en su Portaria Normativa No- 3.389/MD, estableció la *Política de Defensa Cibernética*, la que alcanza a todos los componentes militares del poder nacional, y a otras entidades relacionadas con la Defensa o la CiberGuerra (DefesaNet, 2012).

Entre los postulados de esta política, se pueden mencionar los siguientes:

- La eficacia de las medidas de Ciber Defensa depende de manera fundamental de las actividades de colaboración de la sociedad brasileña,incluyendo no solo al Ministerio de Defensa, sino también a la comunidad académica, sectores público y privado y la base industrial de defensa.

- La capacidad tecnológica del sector cibernético debe llevarse a cabo en armonía con la Política de Ciencia, Tecnología e Innovación para la Defensa Nacional.
- La Seguridad de la Información y Comunicaciones es la base de Defensa Cibernética y depende directamente de las Acciones Individuales.

Al igual que EEUU, Brasil procura la integración y cooperación internacional, firmando un acuerdo con EEUU para unir capacidades en materia de ciberguerra. También, en una declaración conjunta entre los Ministros de Defensa de Argentina y de Brasil, [106]se introdujo una cláusula de cooperación tecnológica y de producción para la defensa, en materia informática y de ciberdefensa.

En lo relativo al desarrollo doctrinario, el 19 de noviembre de 2014, fue difundido el manual "*Doutrina Militar de Defesa Cibernética* - MD31-M-07 (1ª Edição/2014)".

Entre los aspectos de interés del manual, se establecen definiciones sobre las distintas actividades cibernéticas, relacionadas a los niveles de decisión, tal como se muestra en el siguiente gráfico:

NIVEL	ACTIVIDAD	ORGANISMO RESPONSABLE
POLÍTICO	Seguridad de la información y comunicaciones + ciberseguridad	Presidencia de la República
ESTRATÉGICO	Defensa Cibernética	Ministerio de Defensa, EMCFFAA, Comandos de las FFAA
OPERACIONAL	Guerra Cibernética	Comando Operacional
TÁCTICO	Guerra Cibernética	Componentes

Figura 41: Niveles, actividades y responsabilidades en ciberdefensa (*Doutrina Militar de Defesa Cibernética* - MD31-M-07).

Se fijan asimismo, principios de conducción de la defensa cibernética (*Principios relevantes de emprego da Defesa Cibernética*), definidos como de efecto, de disimulación, de rastreabilidad y de adaptabilidad.

[106] Fue firmada en Buenos Aires el 5 de septiembre de 2011, entre el Ministro de Defensa argentino Arturo Puricelli y su par brasileño, Nelson Jobim.

La definición del Sistema Militar de Defensa Cibernética (SMDC) y las responsabilidades de cada integrante, están establecidas con precisión. En esa definición se asigna al Estado Mayor Conjunto de las Fuerzas Armadas, la responsabilidad de asesorar al Ministro de Defensa en lo relacionado a la implementación y gestión del Sistema, con vistas a asegurar en el ámbito de la defensa nacional, la capacidad de operación en red, interoperabilidad de los sistemas y el nivel de seguridad necesario.

El órgano central del SMDC es el CDCiber bajo control operacional del Ministerio de Defensa. El CDCiber cuenta con un estado mayor conjunto para el planeamiento y control de las acciones tratando de lograr un efecto sinérgico si se consideran las capacidades y particularidades de cada fuerza. No obstante ello, el CDCiber mantendrá un canal técnico para coordinación e integración con otros organismos relacionados con la defensa cibernética (CERT.br, CTIR Gobierno estatales, organismos de ciberdefensa de cada fuerza, Ministerios, Agencias de gobierno, policía, etc). También mantendrá ese canal con los organismos centrales de inteligencia de las FFAA y como parte del Sistema de Inteligencia de la Defensa (SINDE) en lo relacionado a la obtención de información y producción y difusión de inteligencia relacionada al sector cibernético de los potenciales enemigos.

Finalmente, si bien se aprecia que el nivel de desarrollo tecnológico puede ser equivalente o ligeramente superior al propio, tanto el desarrollo de estrategias, su implementación y el cuerpo doctrinario brasileño, relacionado a ciberdefensa, es completo y orientador a la hora de determinar los pasos para evolucionar en la materia.

Con respecto al marco legal, existen una serie de leyes y normas que penalizan inconductas en o contra sistemas informáticos, todas ellas, actualizaciones de leyes anteriores. No obstante ello el 02 de abril de 2013, entró en vigencia la *Lei de crímenes en Internet, número 12.737/2012*[107], aunque sólo refiere a la invasión de dispositivos electrónicos (celulares, notebooks, desktops, etc) para obtener o adulterar datos y obtener ventajas ilícitas.

3. Comparación sintética de Estrategias de Defensa Cibernética:

En la tabla siguiente y en relación a las políticas y estrategias relacionadas, se

[107] Es también conocida como Ley Carolina Dieckmann, en referencia a la actriz, ahora diputada, cuyos correos electrónicos fueron hackeados difundiéndose una gran cantidad de datos íntimos y personales.

sintetizan las elaboradas por cuatro estados pioneros en la temática, Brasil Y Colombia a nivel regional y España y el Reino Unido, en Europa.

Brasil	España	Colombia	RU	ACCIÓN
X	X	X		**Fortalecer estructura estatal SC/DC**
X	X	X	X	**Uso Público-privado del Ciberespacio**
X	X	X	X	**Cooperación /integración - Sinergia**
X	X		X	**Reducir dependencia tecnológica (Más I+D)**
X	X	X	X	**Marco legal Defensa cibernética**
X			X	**Doctrina afín al nuevo Ambiente Operacional**
X	X	X	X	**Obtención y desarrollo de RRHH ***
	X	X	X	**Desarrollar Conciencia en Ciberseguridad**
	X		X	**Inversión Cap(s) de Ciberdefensa ***
			X	**Fuerza Especifica de Ciberdefensa ***

Figura 43: Principales líneas estratégicas en ciberseguridad (del autor).

Políticas y estrategias similares son adoptadas por otros estados, las que se concretan en organizaciones gubernamentales y de defensa afines, tales como el MAHER (IRÁN), el Grupo de Delitos Telemáticos de la Guardia Civil (ESPAÑA), el Centro de Ciber Defensa de Excelencia de Chievi (ITALIA) y el Colective Cyber Defense Center Of Excellence (CCDCE) de Tallinn, creado por la NATO.

C. La situación nacional.

La concientización sobre los riesgos en materia cibernética en Argentina, ha ocurrido simultáneamente con las de otros estados más avanzados. En la década del 90, los casos Ardita, Lanata y la violación de la página WEB de la Corte Suprema de Justicia, marcaron los primeros antecedentes.

Argentina ha sido pionera en Sudamérica en materia de seguridad criptográfica, por lo que era previsible que no fuera ajena a todo aquello relacionado con la seguridad informática, a partir de su generalización.

Junto a Chile, Costa Rica, República Dominicana y México, fueron los únicos Estados latinoamericanos invitados al Convenio del Consejo de Europa en Delito Cibernético (o "Convención de Budapest") mencionado precedentemente, realizado en

2001 y en vigor desde 2004. Ninguno de los países mencionados pudo adherir inicialmente, por no cumplir al momento de la firma, con los requisitos mínimos exigidos para el ingreso.

En el caso argentino, se debió a dos motivos. En primer lugar a la ausencia de un marco legal que cubriera todas las categorías de delito cibernético, tal como ya se había generalizado en Europa; de hecho, Argentina fue uno de los últimos estados de la región en promulgar una ley de seguridad informática (2008), seguido por Uruguay (2009) y Brasil (2013).[108]

En segundo lugar, por la ausencia de un organismo CSIRT (*Computer Security Incident Response Team* – Equipo de Respuesta ante Incidentes de Seguridad Informática). Si bien este fue uno de los argumentos esgrimidos por la organización, resulta extraño como fundamento ya que desde el año 1999, existía la Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (ArCERT), el cual será mencionado más adelante.

El "Observatorio de la Ciberseguridad en América Latina y el Caribe[109]", un estudio patrocinado por la OEA y el Banco Interamericano de Desarrollo (BID), informa sobre Argentina los siguientes datos:

- *Población total del país:* 42,980,026
- *Personas con acceso a Internet:* 27,937,016
- *Abonos a teléfonos celulares:* 66,356,509
- *Penetración a Internet:* 65%

El dato más relevante, la penetración a internet, indica el alto porcentaje de habitantes expuestos a ciberamenazas, sólo superado en Latinoamérica por Chile, con un 72 %.

El mencionado observatorio, expone en forma gráfica la realidad de cada estado

[108] El 24 de junio de 2008, se promulga la ley 26.388 – Delitos Informáticos, como una serie de modificaciones al Código Penal. Cabe aclarar que esta no es la única ley ni disposición regulatoria, sino que se complementa con otras previas y posteriores derivadas, que cubren casi la totalidad de la problemática de seguridad informática estatal, con la notoria excepción del ámbito de la Defensa Nacional.

[109] El Informe del Observatorio 2015: Seguridad cibernética en América Latina y el Caribe es el resultado de una gestión de colaboración entre el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) para presentar una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe. El uso de una herramienta en línea diseñada en conjunto con el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford facilitó la recolección de datos por parte de la OEA-BID de los interesados de seguridad cibernética que representan distintos sectores.

en materia de ciberseguridad de manera absoluta o comparativa, en base a una escala valorada de uno a cinco (Inicial, Formativo, Establecido, Estratégico y Dinámico), acorde cada valor, con el nivel de desarrollo alcanzado.

En la tabla siguiente y para el caso nacional, dicho observatorio asigna las siguientes calificaciones:

Política y estrategia	
Estrategia nacional de seguridad cibernética oficial o documentada	
Desarrollo de la estrategia	2
Organización	2
Contenido	3
Defensa cibernética	
Estrategia	2
Organización	3
Coordinación	1

Cultura y sociedad	
Mentalidad de seguridad cibernética	
En el gobierno	2
En el sector privado	3
En la sociedad	2
Conciencia de seguridad cibernética	
Sensibilización	2
Privacidad en línea	
Normas de privacidad	4
Privacidad del empleado	1

Educación	
Disponibilidad nacional de la educación y formación cibernéticas	
Educación	3
Formación	2
Desarrollo nacional de la educación de seguridad cibernética	
Desarrollo nacional de la educación	1
Formación e iniciativas educativas públicas y privadas	
Capacitación de empleados	2
Gobernanza corporativa, conocimiento y normas	
En las empresas estatales y privadas	3

Marcos legales	
Marcos jurídicos de seguridad cibernética	
Para la seguridad de las TIC	3
Privacidad, protección de datos y otros derechos humanos	3
Derecho procesal de delincuencia cibernética	3
Investigación jurídica	
Cumplimiento de la ley	3
Fiscalía	3
Tribunales	2
Divulgación responsable de la información	
Divulgación responsable de la información	1

Tecnologías	
Adhesión a las normas	
Aplicación de las normas y prácticas mínimas aceptables	2
Adquisiciones	2
Desarrollo de software	2
Organizaciones de coordinación de seguridad cibernética	
Centro de mando y control	4
Capacidad de respuesta a incidentes	2
Respuesta a incidentes	
Identificación y designación	4
Organización	3
Coordinación	2
Resiliencia de la infraestructura nacional	
Infraestructura tecnológica	3
Resiliencia nacional	2
Protección de la infraestructura crítica nacional (ICN)	
Identificación	2
Organización	2
Planeación de respuesta	2
Coordinación	2
Gestión de riesgos	2
Gestión de crisis	
Planeación	3
Evaluación	2
Redundancia digital	
Planeación	2
Organización	2

Mercado de la ciberseguridad	
Tecnologías de seguridad cibernética	2
Seguros de delincuencia cibernética	2

Figuras 44 a 48: Calificación de Argentina en aspectos de ciberseguridad (tomado del Informe del Observatorio 2015: Seguridad cibernética en América Latina y el Caribe).

La tabla y sus valores sugieren un limitado desarrollo y aunque se está por encima de la mayoría de los países de la región en términos generales (con excepción de Brasil), resulta aún insuficiente para crear un entorno de ciberseguridad aceptable, sea estatal o privado.

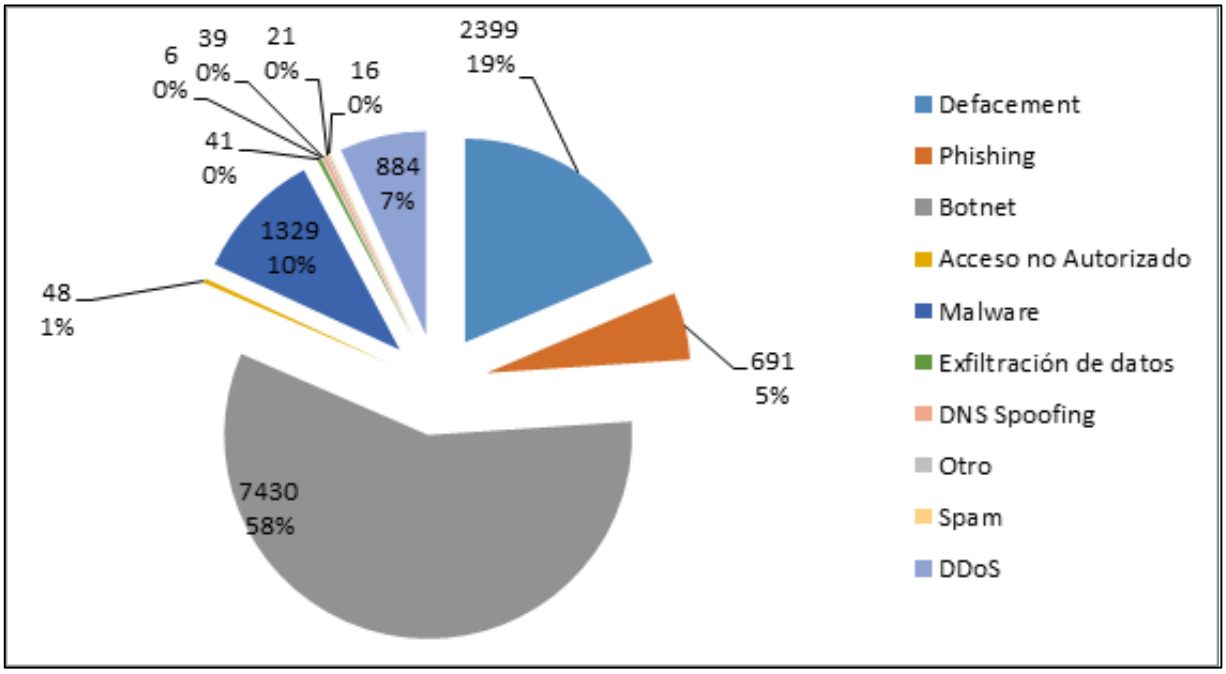
Si además se efectúa la comparación en términos exclusivos de Política y Estrategia, con Brasil y Colombia, Argentina se encuentra en condiciones de inferioridad manifiesta.

PAIS	Argentina	Brasil	Colombia
Política y estrategia			
Estrategia nacional de seguridad cibernética Oficial o documentada			
Desarrollo de la estrategia	2	2	3
Organización	2	2	2
Contenido	3	2	3
Defensa cibernética			
Estrategia	2	3	2
Organización	3	3	3
Coordinación	1	2	2

Figuras 49: Situación comparativa de Argentina con Brasil y Colombia en aspectos de ciberseguridad (tomado del Informe del Observatorio 2015: Seguridad cibernética en América Latina y el Caribe).

Según un informe de la ONTI (Oficina Nacional de Tecnologías de la Información), se registraron un total de 12908 incidentes entre el 01 de enero y el 19 de septiembre de 2016.

El número de ataques por tipo, fue el siguiente:



Figuras 50: Ciberataques por tipo en Argentina (ONTI).

La existencia de amenazas concretas sobre el país es similar a la de otros países incluso más desarrollados.

Con respecto al marco legal, existe una gran cantidad de normas que refieren a la problemática, aunque ninguna específica que la aborde en forma integral y atienda su complejidad.

Entre las leyes y disposiciones se puede enumerar a las siguientes:

- Ley N° 11.179 Código Penal de la Nación Argentina
- Ley N° 23.554 de Defensa Nacional
- Ley N° 24.059 de Seguridad Interior (Art 28 y 29) y su Reglamentación
- Ley N° 24.948 de Reestructuración de las FFAA
- Ley N° 25.326 de Protección de Datos Personales
- Ley N° 25.520 de Inteligencia Nacional
- Ley N° 26.690 Proveedores del Servicio de Internet
- Ley N° 26.388 de Delitos Informáticos
- Ley N° 25.506 de Firma Digital
- Decreto N° 1691 / 2006 Directiva de Organización y Funcionamiento de las FFAA
- Decreto N° 1729 / 2007 Ciclo de Planeamiento Defensa Nacional
- Decreto N° 1714 / 2009 Directivas de Políticas de Defensa

- Res JGM N° 580 del 2011 Programa Nacional ICIC
- Disposición N° 6 / 2005 de la ONTI: “Pol Seguridad de la Inf Modelo” para el SPN
- Disposición N° 3 / 2011 (ONTI), Adhesión ICIC y confidencialidad
- Convención de Budapest sobre Ciberdelincuencia (01-04)
- Dec “Fortalecimiento de la Seguridad Cibernética en las Américas” (OEA/CICTE) (01 Mar07)
- Declaración de Panamá: “La Protección IC frente al Terrorismo” (OEA/CICTE) (01 Mar07)
- Decisión Administrativa N° 669/04 de JGM - Org SPN: Pol Seg y Comités de Seguridad de la Información .

Aunque existen procedimientos y mecanismos para divulgar datos sobre violaciones a la seguridad informática, *“…el sector privado no está obligado por ley a reportar las violaciones a la seguridad cibernética. Sin embargo ha crecido de manera significativa entre las empresas una conciencia de riesgos de seguridad cibernética.”* (BID, 2016).

En relación a los organismos especializados en seguridad y/o defensa cibernética, se cita nuevamente al ArCERT (ver página 128). Éste había sido creado por medio de la Resolución N◦81/99, dentro de la ex-Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros; esta Secretaría tenía la facultad de establecer la política sobre tecnologías referidas a informática, teleinformática o telemática, multimediales y de telecomunicaciones asociadas con lo informático para el Sector Público Nacional (Presidencia de la Nación).

En 2011, se creó en el ámbito de la Jefatura de Gabinete de Ministros, el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)” cuya finalidad es impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, de organismos interjurisdiccionales y de organizaciones civiles y del sector privado que así lo requieran[110]. El organismo responsable es la ONTI, mencionada precedentemente. El programa, aunque prevé su aplicación a todos los ámbitos del estado y organismos asociados, no está generalizado en todo el ámbito gubernamental nacional ni provincial.

[110] Ver http://www.icic.gob.ar/paginas.dhtml?pagina=98 de fecha 03 de mayo de 2013.

Por otra parte, de los organismos e instituciones propios de la Defensa y de la Seguridad Interior, sólo el Ejército y la Gendarmería Nacional, estaban adheridos en abril de 2013.

Entre los objetivos perseguidos por el programa ICIC, se pueden mencionar los siguientes:

- Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante, fortaleciendo lazos entre los sectores público y privado, haciendo especial hincapié en las infraestructuras críticas.
- Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.
- Investigar nuevas tecnologías y herramientas en materia de seguridad informática.
- Incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional.
- Asesorar a los organismos sobre herramientas y técnicas de protección y defensa de sus sistemas de información.
- 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.
- Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno, al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica.
- Difundir información útil para incrementar los niveles de seguridad de las redes teleinformáticas del Sector Público Nacional.
- Interactuar con equipos de similar naturaleza.

Los objetivos mencionados se alcanzan a través de la ejecución de cuatro actividades básicas:

1. Relevamiento y monitoreo: esta actividad está a cargo del GICI (Grupo de Infraestructuras Críticas de la Información) y persigue la identificación y análisis de las infraestructuras criticas del país conectadas u operadas a través de sistemas

informáticos, tal el caso de las telecomunicaciones, energía, combustibles e hidrocarburos, servicios financieros, etc.

2. Investigación y prevención: esta responsabilidad recae en el GAP (Grupo de Acción Preventiva). El GAP estudia y analiza nuevas tecnologías y herramientas informáticas y de seguridad.
3. Respuesta a incidentes: a cargo del CERT (Coordinación de Emergencias en Redes Teleinformáticas).
4. Concientización y capacitación: basada en el grupo ICIC Internet Sano.

A través del Instituto Nacional de la Administración Pública (INAP), el ICIC brinda cursos, talleres y charlas enfocadas en la estrategia de capacitación diseñada por la Oficina Nacional de Tecnologías de la Información (ONTI). En 2012, ICIC propuso una política de seguridad modelo, aunque a la fecha aún no ha sido aprobada.

En el momento de su creación, la autoridad de aplicación del Programa ICIC era la Oficina Nacional de Tecnologías de Información (ONTI), la cual dependía de la Subsecretaría de Tecnologías de Gestión, Secretaría de Gabinete, de la Jefatura de Gabinete de Ministros.

En junio de 2015, el Poder Ejecutivo Nacional (PEN) mediante el Decreto N◦1067/2015, creó la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros.

El objetivo principal era el de implementar la estrategia nacional de protección de las infraestructuras críticas de la información y ciberseguridad, bajo el argumento de perfeccionar el uso de los recursos públicos para mejorar la calidad de vida de los ciudadanos, a través de resultados colectivamente compartidos y socialmente valorados (Milanes & Uciferri, 2016). No se aprecia en ello, referencia alguna a la mejora de la seguridad cibernética propia del ámbito de la defensa.

Para el cometido de las funciones de la nueva Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, se estimó necesario una nueva organización de los niveles políticos implicados *“…basado en criterios de racionalidad y eficiencia que posibiliten una rápida respuesta a las demandas de la sociedad, dando*

lugar a estructuras dinámicas y adaptables a los cambios permanentes…"[111]. Como se puede apreciar, lejos está la norma de establecer conceptos sólidos y concretos que faciliten su interpretación e implementación.

Este decreto estableció que el Programa ICIC pasara a depender de la Dirección Nacional de Infraestructuras críticas de la Información y Ciberseguridad, creada dentro del ámbito de la nueva subsecretaría de Protección de Infraestructuras críticas de Información y Ciberseguridad.

La responsabilidad primaria de la nueva Subsecretaría es la de entender en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, incluyendo la generación de capacidades de detección, defensa[112], respuesta y recupero ante incidentes de redes y sistemas del Sector Público Nacional.

Para ello, la subsecretaría ejecuta prácticamente las mismas acciones del Programa ICIC, por ejemplo:

- Entender, asistir y supervisar en los aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica;
- Elaborar normas y estándares destinados a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas;
- Dictar la Política de Seguridad Modelo de la Información;
- Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante;
- Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.

Por su parte, la Resolución N◦1046/15 de Jefatura de Gabinete de Ministros, creó tres direcciones y dos coordinaciones dependientes de la Dirección Nacional de Infraestructuras críticas de Información y Ciberseguridad, cada una con diferentes

[111] Decreto 1067/2015. http://www.cira.org.ar/index.php?option=com_content&view=article&id=6121:decreto-1067-2015&catid=112&Itemid=500

[112] Nota del autor: El término "defensa" es empleado aquí como equivalente a "protección" y no refiere a la Defensa como concepto de carácter general y uno de los cometidos de cualquier estado.

misiones: Dirección de Elaboración e Interpretación Normativa; Dirección Técnica de Infraestructuras críticas de Información y Ciberseguridad; Dirección de Capacitación, Concientización y Difusión; Coordinación de Procesos y Proyectos; Coordinación de Desarrollo e Investigación[113].

Nuevamente se aprecia la priorización de organizaciones de carácter político y dirigencial por sobre aquellas efectivamente ejecutivas.

En cuanto a la estructura nacional de seguridad cibernética, quedaría basada en la ONTI como elemento de dirección, en el programa ICIC en su ejecución y en organizaciones de seguridad informática de distintas agencias (División de Delitos Tecnológicos de la Policía Federal, de Gendarmería Nacional, CITEDEF, EST) o privadas (Universidad Católica Argentina).

Particularmente la División de Delitos Tecnológicos de la Policía Federal Argentina (PFA) es responsable de la investigación de delitos informáticos, disponiendo de capacidades, para la detección y reporte de ataques cibernéticos de magnitud. Asimismo se ha creado en la órbita del Ministerio Público Fiscal, la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), cuyo campo de acción incluye 1) casos de ataques a los sistemas informáticos, 2) delitos cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada, y 3) crímenes en los que sea necesario realizar investigaciones en entornos digitales[114].

Existe además una ONG de reciente creación conocida como *ArgentinaCibersegura*[115], que es patrocinada por la compañía de seguridad informática ESET en tanto que bajo la dirección del Ministerio de Justicia y Derechos Humanos, se desarrolla la campaña “Con vos en la Web”[116] que enseña sobre la amenaza de la captación de menores en línea conocida como grooming (crear lazos de amistad abusivos en la web con los niños para atraerlos al abuso sexual o la trata de personas)

---

[113] Resolución N◦1046/2015 disponible en http://www.informaticalegal.com.ar/2015/08/20/resolucion-10462015-jefatura-de-gabinete-de-ministros-estructura-organizativa-de-la-direccion-nacional-de-infraestructuras-criticas-de-informacion-y-ciberseguridad/

[114] Ver https://www.mpf.gob.ar/ufeci/

[115] Para mayores datos consultar https://www.argentinacibersegura.org

[116] Ver http://www.convosenlaweb.gob.ar/

(BID, 2016).

Sin embargo, la respuesta nacional aunque prolífica en materia de delitos cibernéticos, continúa presentando vacíos importantes en la temática más compleja de la ciberguerra.

Fue el Ejército quien definió hacia el año 2005, una directiva de Seguridad informática al máximo nivel, derivada de la que había elaborado la ONTI. Fue reemplazada en 2012 por una similar, aunque adaptada a la evolución de la amenaza. En 2012, se presentó en el marco del Estado Mayor Conjunto de las FFAA, el borrador de un Plan Estratégico de Ciber Defensa, el cual no fue finalmente aprobado.

La principal deficiencia del plan, era que, en función de lo establecido en el Decreto Nro 1691/06 Directiva sobre organización y funcionamiento de las Fuerzas Armadas, las acciones que en materia de ciberseguridad y ciberdefensa, efectuaran los organismos de las FFAA, estarían dirigidas a enfrentar “agresiones militares estatales de origen externo”, en este caso en el ciberespacio. Ni siquiera contemplaba accionar en el caso de ciberataques a la jurisdicción militar, tal como está contemplado en los artículos 28 a 30 de la Ley 24.059 – Ley de Seguridad Interior[117].

Como se ha visto, la dificultad o mejor dicho la enorme cantidad, tipo y finalidad de los ciberataques, como las dificultades para clasificar y establecer su origen, hacían de este plan, algo impracticable.

No obstante ello, por resolución del Ministro de Defensa 343, del 14 de mayo de 2014, se creó el Comando Conjunto de Ciber Defensa (CCCD), destinado a atender las crecientes necesidades de seguridad y defensa cibernética en el ámbito de la Defensa Nacional.

Entre los antecedentes que llevaron a su concreción, se pueden citar:

[117] La ley mencionada establece lo siguiente:
“ARTICULO 28. — Todo atentado en tiempo de paz a la jurisdicción militar, independientemente de poner en
forma primordial en peligro la aptitud defensiva de la Nación, constituye asimismo una vulneración a la seguridad interior.
ARTICULO 29. — En los casos previstos en el artículo 28 constituye una obligación primaria de la autoridad militar la preservación de la fuerza armada y el restablecimiento del orden dentro de la aludida jurisdicción, de
conformidad con las disposiciones legales vigentes en la materia.”
Estos artículos habilitarían incluso al empleo de ciberarmas como respuesta a ataques cibernéticos que sean ejecutados por individuos u organizaciones no militares, sean o no estatales.

- Resolución Nro. 08 del 2010 del Ministerio de Defensa para la creación de un Grupo de Tareas para abordar la temática de la Ciberdefensa desde el punto de vista de la Defensa Nacional.
- Resolución Nro. 59 del 2012 del Jefe del Estado Mayor Conjunto de las Fuerzas Armadas para la creación de un Elemento de Tareas para tratar Proyectos, Doctrina, Organización y Competencias vinculados con la Ciberdefensa.
- Resolución Nro. 385 del 2013 del Ministerio de Defensa. Creación de la Unidad de Coordinación de Ciberdefensa en el Ministerio de Defensa.
- Directiva Nro. 02 del 2013 del Jefe del Estado Mayor Conjunto de las Fuerzas Armadas. Elaboración de un Plan Estratégico de Ciberdefensa para el Instrumento Militar. Sobre este plan se harán referencias más adelante.

El CCCD tiene la siguiente misión: *"Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar"*[118].

Sus *funciones* incluyen la coordinación de sus acciones con los Centros de Ciberdefensa de las Fuerzas Armadas y el establecimiento de criterios rectores (a nivel del Instrumento Militar), para la determinación de infraestructuras críticas a ser protegidas.

Otras funciones adicionales incluyen:

1) Entender
   - En el establecimiento de estándares y procedimientos de Ciberdefensa, criptografía e informática forense.
   - En la supervisión de los centros de respuesta de cada Fuerza Armada.
   - En el proceso de capacitación de personal propio.
   - En la organización y desarrollo de actividades académicas (foros, seminarios, simposios, etc.).
2) Intervenir en la elaboración, revisión y experimentación de Doctrina de Ciberdefensa.
3) Participar:
   - A requerimiento del Ministerio de Defensa, en apoyo a otros Organismos.
   - En la concientización de las FF.AA. en materia de Ciberdefensa.

[118] Ver http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Mision.aspx

- En la determinación y supervisión de los estándares de seguridad y certificación de protocolos afines en las Fuerzas Armadas.

Sin embargo en lo expresado como la visión de la Organización, se menciona su aspiración a convertirse en la "…*máxima instancia militar de coordinación del Estado Mayor Conjunto*…" y no se menciona algo respecto a aquellas misiones y funciones que implican actividades propias de ejecución como por ejemplo, la protección de las redes militares propias del EMCO o la ejecución de operaciones de carácter ofensivo en el ciberespacio. Y esto no es considerado como una falencia en la organización, sino que simplemente no está contemplado.

La protección del resto de las redes militares y otras actividades relacionadas, son propias de los departamentos de Ciberdefensa de cada fuerza, como se verá más adelante. Esto incluye a la fecha, la adopción de los procedimientos técnicos de ciberseguridad, la selección del software de protección y eventualmente, la elección de los canales formales e informales de comunicación de incidentes, relaciones y/o coordinaciones varias con otras agencias, incluso fuera del ámbito de la defensa nacional.

Con efectivos ligeramente superiores al medio centenar (de ellos, un 36 % con algún tipo de capacitación avanzada en informática y/o seguridad cibernética), se aprecia que resultan escasos para cumplimentar con excelencia, su misión y las diferentes y múltiples funciones asignadas[119].

En la actualidad, su organización es la siguiente:

[119] Esto resulta obvio si se analizan los efectivos de organizaciones equivalentes en otros estados, como el caso del CDCyber brasileño, cuyo personal supera los 600 hombres y mujeres, y que se halla en la actualidad en proceso de expansión, con la creación de centros regionales de Ciberdefensa.

Figura 51: Organigrama del Comando Conjunto de Ciberdefensa (Fuerzas Armadas).

Por su parte, cada una de las fuerzas armadas dispone de su propio Departamento de Ciberdefensa, dependientes de las respectivas Direcciones de Comunicaciones e Informática en el caso del Ejército Argentino[120] y de la Armada y del Estado Mayor General en el caso de la Fuerza Aérea.

Aunque el nombre hace referencia a la Ciberdefensa y está contemplado el desarrollo de capacidades ofensivas en el futuro, en la actualidad sólo se realizan actividades propias de seguridad cibernética, con procedimientos y software definido por cada departamento (sin que se halle coordinado o estandarizado por el CCCD)[121].

Los efectivos de los departamentos de la Fuerza Aérea y del Ejército Argentino, no superan los veinte individuos, en tanto que los de la Armada, no alcanzan los 40.

[120] Originalmente fue creado dentro de la Dirección General de Inteligencia, siendo transferido a la Dirección de Comunicaciones e Informática en 2017.

[121] La información consignada, ha sido obtenida a través de una encuesta realizada por el suscripto en cada departamento y en el CCCD).

Asimismo el personal especializado en seguridad cibernética, alcanza un 20 % del efectivo en la Fuerza Aérea, un 40 % en el Ejército y un 60 % en la Armada.

Las acciones de seguridad en la Armada y de la Fuerza Aérea, no sólo alcanzan las redes administrativas o de nivel operacional, sino que se realizan sobre los sistemas tácticos (incluyendo comunicaciones, sistemas de C4I2 tácticos, etc)[122]. En el caso del Ejército, sólo las redes internas administradas desde el Estado Mayor General.

Aunque las cuatro agencias mencionadas mantienen relaciones funcionales, en la práctica no se han coordinado de manera efectiva, las actividades, los procedimientos y los sistemas de seguridad empleados, aunque se encuentra en elaboración un reglamento conjunto de ciberdefensa, con la participación de especialistas de las tres FFAA.

Aunque el panorama podría parecer complicado, se han hecho avances importantes en la actualidad.

En 2016 y en el ámbito del Decreto Nro 434/2016 – Plan de Modernización del Estado, la Nación y las provincias suscribieron acuerdos de cooperación diversos. En base a ellos y promovidos por el Consejo Federal de Modernización e Innovación en la Gestión Pública (COFEMOD), se desarrollaron acciones concretas para ello.

El 09 de marzo de 2017, se llevó a cabo en la casa de la Provincia de Salta, la reunión preparatoria para la constitución de la Comisión de Ciberseguridad del COFEMOD.

Entre los muchos aspectos tratados, se convino en trabajar para la elaboración de un Programa de Ciberestrategia Nacional y en la creación del Comité de Ciberseguridad (básico y ampliado).

“El programa de ciberestrategia, tiene como objetivo principal, diseñar de modo integral y consensuado, políticas y procedimientos a ser normados y aplicados por la Administración Pública Nacional. Asimismo, definir las herramientas que permitan el desarrollo de una Ciberestrategia Nacional acorde a los estándares mundiales. La aplicación del programa permitirá la prevención, detección y mitigación de los ataques cibernéticos, como así también, la investigación y el diseño de nuevas y avanzadas estrategias específicas para cada área de Gobierno” (Gobierno Nacional, 2017).

[122] En función de los efectivos disponibles, del nivel de desarrollo y de las restricciones presupuestarias, el autor aprecia que la capacidad para asegurar los sistemas tácticos sería muy limitada.

El 28 de julio de 2017, por decreto Nro 577/2017, se creó el Comité de Ciberseguridad, cuyo objetivo es la elaboración de la Estrategia Nacional de Ciberseguridad. Está integrado por representantes de los Ministerios de Modernización, de Seguridad y de Defensa. Entre las tareas del Comité, figuran las siguientes (Presidencia de la Nación, 2017):

a) Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.

b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.

c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente.

d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad.

e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.

f) Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional que se le encomienden.

Cabe aclarar que a la fecha, aún no ha sido presentada la mencionada estrategia y que se están desarrollando las reuniones iniciales de relevamiento de las capacidades disponibles. En principio cabrían al Ministerio de Modernización, la dirección del Comité y todos los aspectos relacionados con Ciberseguridad, al Ministerio de Seguridad lo relacionado al Cibercrimen[123] y al de Defensa, lo relacionado a Ciberdefensa, aunque entre sus tareas, no hace referencia a esta actividad y el ciberdelito puede ser incluido en acciones propias de ciberseguridad.

[123] Estas son las funciones asignadas en la organización del Comité. Se aclara que el término Cibercrimen, derivado de la palabra *Cybercrime* en inglés, corresponde a la acepción española de ciberdelito.

D. Fortalezas y vulnerabilidades de la estructura de ciberseguridad y ciberdefensa de Argentina.

En función de lo desarrollado previamente es posible concluir acerca de cuáles son las fortalezas y debilidades que la estructura de Ciberseguridad y Ciberdefensa, presenta en Argentina

Como fortalezas se pueden mencionar las siguientes:

- **Alto grado de conciencia** sobre la importancia de encarar la problemática de la seguridad cibernética de manera integral, tanto a nivel privado como estatal.
- **Disponibilidad del know how y de profesionales informáticos** con gran capacidad para el desarrollo de sistemas y software de seguridad cibernética.

Entre las debilidades más importantes, se pueden inferir las siguientes:

- **Carencia de una Estrategia Nacional de Ciberseguridad**, que establezca objetivos, determine responsabilidades y funciones, coordine esfuerzos y oriente el desarrollo de estrategias para los elementos que dependan del máximo nivel.
- **Recursos limitados** (humanos, materiales y presupuestarios), fundamentalmente por lo expresado en el párrafo anterior y por la existencia de otras prioridades en un marco general de crisis económica.
- **Organismos con funciones superpuestas**, en cantidad, surgidos de iniciativas no coordinadas o reguladas por el máximo nivel, los que pujan entre sí por acceder los escasos recursos disponibles.
- **Marco legal complejo y desintegrado**. La normativa aplicativa a ciberseguridad, es en general adaptada o arreglada a situaciones novedosas, a partir de normas preexistentes, actuando a modo de soluciones de emergencia frente a hechos consumados y no con carácter proactivo o preventivo. No existen leyes o normas que atiendan la problemática de manera integral.
- **Consideraciones de carácter ideológico o político**, relacionadas con problemáticas tales como derechos humanos, libertades individuales, inteligencia interior, etc, las que actuarían como factores limitantes a la hora de lograr un nivel de seguridad aceptable. En tal sentido, la necesidad social d conocer con transparencia, el trabajo de los organismos de seguridad o defensa cibernética, se enfrenta con la necesidad de éstos de mantener un alto grado de reserva para asegurar el cumplimiento de sus funciones con eficiencia.

Esta última debilidad, es particularmente aplicable a las organizaciones que dependan de las Fuerzas Armadas y de Seguridad[124] y en tal sentido, impone limitaciones importantes a la hora de alcanzar un nivel de seguridad cibernética aceptable.

La concientización en materia de seguridad (cibernética o cualquier otra que se considere) deberá estar necesariamente asociada a la recuperación de la confianza entre los distintos grupos de la sociedad y al ejercicio responsable de las funciones sensibles del estado por parte de sus funcionarios (empleado el término en forma genérica).

[124] Es opinión del autor, que el inconsciente colectivo de la sociedad argentina, pretende un nivel de seguridad (física, financiera y eventualmente informática) y bienestar elevado, sin que sea objeto de manera individual y colectiva, de control y supervisión por parte de cualquier organismo del estado, generando una dicotomía imposible de resolver.

CAPÍTULO V

LA ESTRATEGIA MILITAR DE CIBERDEFENSA: HACIA UNA PROPUESTA.

El empleo de sistemas informáticos y su integración a las actividades del ser humano, evoluciona teniendo cinco metas básicas:

- Alcanzar una mayor conectividad.
- Respetar libre flujo e intercambio de contenidos.
- Lograr una mayor integración hombre máquina (*man machine integration*)
- Alcanzar el crecimiento económico con incremento de la productividad.
- Lograr un mayor estándar de vida y salud.

El problema principal es alcanzar dichas metas, en un marco de mayor seguridad sin que esto se traduzca en mayor contención y control de la actividad de los usuarios. Sin lugar a dudas, este es el desafío más importante a enfrentar en un mundo complejo y con importantes desequilibrios.

En relación a las acciones necesarias, la imprescindible a nivel general, es el Desarrollo y protección Ciberespacio Nacional. En ese sentido se hace escencial definir cuál será el alcance de este desarrollo, quiénes serán los responsables y de qué manera lo harán.

En el ámbito específico de la Defensa Nacional, surge la necesidad de emplear y proteger el ciberespacio para el apoyo de operaciones militares y otras tareas y acciones realizadas en tiempos de paz. Deben entenderse a las acciones en este ambiente, como facilitadoras, multiplicadoras de efectos, apoyos y medios de influencia en función de los objetivos perseguidos. Surge entonces como necesidad, elaborar planes de desarrollo y empleo de medios en el ciberespacio, que incluyan la definición de organizaciones, misiones, medios y doctrina relacionada, la cual deberá contemplar la necesaria integración e interactuación con otras agencias nacionales y de otros estados.

Ciertamente los sistemas informáticos de las FFAA, encajan en el concepto de infraestructuras críticas y por ende, merecen igual atención que el resto de las ICIC, con el agregado de que los sistemas militares, requieren tanto en su empleo como en su

protección, un grado de confidencialidad (incluso mayor que las de otras áreas del Estado).

Con la amenaza visible en los monitores, a menos de treinta centímetros del operador, no hay que pensar demasiado en qué hacer.

La inexistencia de una estrategia cibernética propia nacional, constituye una limitación para elaborar una derivada que se aplique al ámbito de la Defensa Nacional.

No obstante, considerando que el Ministerio de Defensa integra el Comité de Ciberseguridad y que dispone de personal, experiencia, organizaciones y procedimientos en uso, su aporte al desarrollo de la Estrategia Nacional y su injerencia en la definición de los objetivos y las misiones que se establezcan, puede ser de trascendencia para el futuro de la defensa cibernética en el país.

Cualquier estrategia militar de ciberdefensa (y en particular una para Argentina), debiera contener como mínimo, los objetivos a alcanzar, las acciones a implementar para reducir las vulnerabilidades actuales, las capacidades militares a desarrollar en este escenario, la estructura de las fuerzas cibernéticas a crear (indicando claramente etapas y plazos), y finalmente los recursos necesarios (humanos, financieros y materiales).

Debido a la necesidad de acotar el desarrollo del presente trabajo y siendo que incluso cada uno de los aspectos contenidos en una eventual estrategia merecerían por sí solos, el desarrollo de estudios de magnitud, sólo se presentará de manera esquemática una propuesta, exclusivamente con fines académicos.

El finalidad general de una estrategia militar de ciberdefensa, aunque sintética en redacción, debiera ser de amplio alcance, y su logro implicaría el desarrollo de capacidades importantes. Podría enunciarse de la siguiente manera:

"Asegurar el dominio del ciberespacio de interés militar y otros contribuyentes al Sistema de Defensa Nacional, para contribuir al cumplimiento de la misión principal y de las misiones subsidiarias de las fuerzas armadas".

De esa finalidad, se derivarán Objetivos Estratégicos, los que podrían ser enunciados de la siguiente manera:

1. **OBJETIVO ESTRATÉGICO 1**: Garantizar el normal funcionamiento de los sistemas y redes de interés de la Defensa nacional, para contribuir a asegurar el cumplimiento de las misiones principal y subsidiarias de las Fuerzas Armadas.

2. **OBJETIVO ESTRATÉGICO 2**: Proteger en forma permanente o a requerimiento, aquellas Infraestructuras Críticas de la Información y Comunicación (ICIC) cuya degradación accidental o intencional, incida negativamente en las capacidades del Sistema de Defensa Nacional.

3. **OBJETIVO ESTRATÉGICO 3**: Alcanzar plena integración, interacción y/o complementación de las organizaciones militares de Seguridad y Defensa cibernéticas, con otras agencias del Estado y organizaciones privadas, para incrementar las capacidades de seguridad y defensa cibernética mutuas, en forma sinérgica.

4. **OBJETIVO ESTRATÉGICO 4**: Asegurar la integración, interacción y/o complementación de las propias organizaciones militares de Seguridad y Defensa cibernéticas, con organizaciones equivalentes de otros Estados, para aumentar las capacidades de seguridad y defensa cibernética, incrementar la confianza mutua y contribuir al cumplimiento de compromisos internacionales.

5. **OBJETIVO ESTRATÉGICO 5**: Proponer y participar en la elaboración y/o actualización de leyes, acuerdos, tratados y/o disposiciones regulatorias referentes a la seguridad y defensa cibernética, para crear y mantener el marco legal imprescindible al cumplimiento de la finalidad.

Cada objetivo estratégico, implica una serie de políticas (líneas de acción estratégicas) a seguir para alcanzar ese objetivo.

A modo de ejemplo, una estrategia militar de defensa cibernética podría tener, a partir de los objetivos mencionados, algunas de las líneas de acción enunciadas para cada caso:

AL OBJETIVO ESTRATÉGICO 1.

“Garantizar el normal funcionamiento de los sistemas y redes de interés de la Defensa nacional, para contribuir a asegurar el cumplimiento de las misiones principal y subsidiarias de las Fuerzas Armadas”.

a. Potenciar las capacidades del Comando Conjunto de Ciberdefensa.
b. Incorporar, capacitar y gestionar los recursos humanos necesarios, incluyendo a los propios de las Fuerzas Armadas, como aquellos provenientes del medio civil.
c. Propender al desarrollo, diseño y producción nacional del software y hardware necesario para asegurar independencia tecnológica, manteniendo un nivel de seguridad aceptable.
d. Promover el desarrollo y empleo de sistemas de C4I2VR[125] que empleen redes y medios de comunicación de uso militar exclusivo.
e. Proponer la elaboración de la doctrina conjunta y eventualmente combinada sobre seguridad y defensa cibernética.
f. Desarrollar programas de capacitación y concientización para los miembros de las Fuerzas Armadas y otras organizaciones afines al sistema de Defensa Nacional.
g. Desarrollar capacidades cibernéticas ofensivas, para su empleo eventual como herramientas de respuesta, ante amenazas del tipo ATP1[126].

AL OBJETIVO ESTRATÉGICO 2.

"Proteger en forma permanente o a requerimiento, aquellas Infraestructuras Críticas de la Información y Comunicación (ICIC) cuya degradación accidental o intencional, incida negativamente en las capacidades del Sistema de Defensa Nacional".

a. Promover convenios de asistencia y cooperación en materia de seguridad y defensa cibernética, con aquellas Infraestructuras Críticas de la Información y Comunicación (ICIC), cuya afectación por ataques cibernéticos, limite o impida el cumplimiento de las misiones asignadas a las Fuerzas Armadas.
b. Desarrollar y organizar equipos de respuesta de emergencias informáticas (CERT)[127]. modulares[128] y de fácil despliegue, con capacidad de neutralizar y recuperar (a orden),

[125] C4I2VR siglas de Comando, Control, Comunicaciones, Computación, Información, Inteligencia, Vigilancia y Reconocimiento.

[126] ATP1: *Advanced Permanent Threat: Amenaza Permanente Avanzada*. Se clasifican así a las amenazas cibernéticas provenientes de estados u organizaciones, cuyo propósito es la anulación de los sistemas informáticos propios o la obtención de información de carácter masivo y que constituyen un serio riesgo a la defensa nacional.

[127] CERT: Computer Emergency Response Team.

[128] El término modular implica que los equipos se conformen (en cantidad y capacidad de personal, medios y sistemas) en función de las características de la amenaza y de la ICIC a proteger.

sistemas y redes pertenecientes a las Infraestructuras Críticas con incidencia en el sistema de Defensa Nacional.

c. Promover la cooperación en materia de investigación, desarrollo y producción de software y hardware de interés, con los organismos responsables de las ICIC integrantes del sistema de Defensa Nacional.

AL OBJETIVO ESTRATÉGICO 3.

"Alcanzar plena integración, interacción y/o complementación de las organizaciones militares de Seguridad y Defensa cibernéticas, con otras agencias del Estado y organizaciones privadas, para incrementar las capacidades de seguridad y defensa cibernética mutuas, en forma sinérgica".

a. Adherir al Programa ICIC integrando a éste, las propias capacidades para contribuir a requerimiento, al incremento de la seguridad y defensa cibernética nacional.
b. Promover convenios de asistencia y cooperación en materia de seguridad y defensa cibernética, con otros organismos del Estado y/o instituciones privadas, relacionados con aspectos que hagan a la problemática de la seguridad y defensa cibernética.

c. Promover la cooperación en materia de investigación, desarrollo y producción de software y hardware de interés.

AL OBJETIVO ESTRATÉGICO 4.

"Asegurar la integración, interacción y/o complementación de las propias organizaciones militares de Seguridad y Defensa cibernéticas, con organizaciones equivalentes de otros Estados, para aumentar las capacidades de seguridad y defensa cibernética, incrementar la confianza mutua y contribuir al cumplimiento de compromisos internacionales".

a. Contribuir con las capacidades propias de las Fuerzas Armadas al cumplimiento de los compromisos internacionales asumidos por el Estado, en materia de seguridad y defensa cibernética.
b. Promover convenios de asistencia y cooperación, con organismos equivalentes de otros estados, tendientes al aumento de la confianza mutua y al incremento de las capacidades de seguridad y defensa cibernética.

c. Promover la cooperación en materia de investigación, desarrollo y producción de software y hardware de aplicación en aquellos sistemas y redes que eventualmente se establezcan y empleen en la acción militar combinada.

AL OBJETIVO ESTRATÉGICO 5.

"Proponer y participar en la elaboración y/o actualización de leyes, acuerdos, tratados y/o disposiciones regulatorias referentes a la seguridad y defensa cibernética, para crear y mantener el marco legal imprescindible al cumplimiento de la finalidad".

a. Contribuir a la generación de un Plan Estratégico Nacional de Seguridad y Defensa Cibernética, aportando aquellos aspectos que hacen a la Defensa Nacional.
b. Participar en la actualización de la Política de Seguridad y Defensa Cibernética, con énfasis en aquellos aspectos que hacen a la Defensa Nacional.
c. Proponer la actualización o formulación de la legislación relacionada con la temática, cuya inexistencia o falta de adecuación a las exigencias presentes o previstas, que impone la operación en el ciberespacio, impida, dificulte o limite, el cumplimiento de los objetivos estratégicos.

Es en base a las líneas de acción estratégicas, que se definen tareas y se establecen plazos para alcanzarlas.

A modo de ejemplo, se fijan en la planilla siguiente, en base a las líneas de acción b y c, del objetivo estratégico número 1, una serie de tareas con un plazo para su cumplimiento.

El paso siguiente, será la imposición de la responsabilidad de la tarea a algún organismo y la asignación de los medios y recursos necesarios para cumplirla en tiempo y forma.

Cabe acotar que los objetivos, líneas de acción y tareas, han sido adaptadas del Taller Integrador realizado en el año 2013, por el Curso Conjunto de Estrategia y Conducción Superior – Nivel II, relacionado a la definición de una Plan Estratégico Militar de Ciberdefensa.

El mencionado trabajo, culminó con la definición de un plan estratégico esquemático completo.

LÍNEA DE ACCIÓN	TAREAS
b. Incorporar, capacitar y gestionar los recursos humanos necesarios, incluyendo a los propios del Instrumento Militar, como aquellos provenientes del medio civil.	1) Definir y actualizar los perfiles del personal necesario.
	2) Asignar el personal militar y civil según los perfiles determinados.
	3) Gestionar el ingreso de personal Especialista.
	4) Definir y actualizar mecanismos de retención del personal militar, civil y especialistas contratados que eviten la deserción a otros ámbitos y la consecuente pérdida de experiencia y conocimientos.
	5) Capacitar al personal en forma continua para mantener su competencia profesional.
	6) Promover becas de estudios y especialización en otras organizaciones y en el extranjero.
c. Propender al desarrollo, diseño y producción nacional de software y hardware necesario.	1) Proponer mecanismos de promoción para el desarrollo de software y hardware en el sector público y privado.
	2) Promover la formación de equipos multidisciplinarios de I+D.
	3) Elaborar y aplicar normas de estandarización según necesidades de desarrollo y diseño de software y hardware.
	4) Incentivar la I+D de nuevos diseños y desarrollo de sistemas en Seguridad y Defensa Cibernética Directa.
	5) Promover becas de investigación y la financiación para el desarrollo del software y hardware de interés.

Figuras 52: Ejemplos de líneas de acción para un OE (del autor).

CAPÍTULO VI

CONCLUSIONES.

En cibernética y por el contrario de lo que se ha sostenido en el país desde 1989, la seguridad es abarcadora, y si se vulnera esa seguridad, debe estar lista la defensa. En Argentina, la actual división entre seguridad interna y defensa externa, no tiene aplicación en el ciberespacio.

La amenaza cibernética a un país no es exclusivamente militar, afecta a empresas, ONG, organizaciones gubernamentales y a privados. Es necesario que la respuesta a agresiones se enfrente desde un solo organismo, por ejemplo, un Consejo de Seguridad Nacional, hoy inexistente. En la Argentina frecuentemente se confunde el Consejo de Defensa Nacional, que se reúne en caso de crisis ante perspectivas de conflicto armado, con el Consejo de Seguridad Nacional presidido por un Asesor de Seguridad Nacional, que en otros países es un organismo permanente que asesora al Presidente de la nación sobre los riesgos a la seguridad del estado.

La dinámica de lo cibernético, hace preciso detener la investigación en algún punto, siendo necesario continuar como parte de otros trabajos profundos y especializados.

La ausencia de una Estrategia Nacional de Ciberseguridad, dificulta el desarrollo de una estrategia militar derivada aplicada a la Defensa Nacional.

Aunque cada Fuerza tiene sus elementos cibernéticos, es de esperar que el futuro cercano, el ciberespacio se constituya en un espacio más de lucha y requiera fuerzas militares de preparación específica. Esto requiere de la instrumentación de un Plan de Carrera para los que lo integren, diferente a los existentes.

Existe un nivel de concientización importante en las Fuerzas Armadas respecto a las amenazas existentes y a los riesgos a los que se está sometidos desde la conformación del Ciberespacio como nuevo ambiente operacional. La inclusión de la Ciberdefensa en planes de desarrollo orgánicos (como capacidad en el PLANCAMIL, como ejemplo) y en reglamentos varios (como operación complementaria en ROB 00-01 “Conducción de las Fuerzas Terrestres Edición 2015), junto a la conformación de organizaciones especializadas, son pruebas irrefutables de ello.

No obstante, el desarrollo y las capacidades concretas, están muy por debajo del

nivel de amenaza, esencialmente por la degradación general sufrida por las FFAA en las dos últimas décadas y por la falta de nivel de conciencia equivalente, tanto en los sucesivos gobiernos como en el conjunto de la sociedad.

Existe en los ámbitos académicos y en organizaciones tanto militares como privadas, el *know how* necesario para incrementar en forma rápida y eficiente, las capacidades tanto para la defensa cibernética directa como para la indirecta (ofensiva).

La existencia de una estrategia militar, que defina finalidades, objetivos, políticas o líneas de acción y tareas concretas, asignadas a individuos u organizaciones responsables de su ejecución, con los recursos necesarios, reducirá significativamente la vulnerabilidad de las Fuerzas Armadas Argentinas frente a las ciberamenazas e incrementaría simultáneamente las capacidades de la Defensa Nacional.

Finalmente, la estrategia militar de ciberdefensa, debiera llevar a una redefinición de la misión, funciones y capacidades del Comando Conjunto de CiberDefensa, ampliando las actuales a efectos de constituirse en el principal organismo de aplicación y desarrollo de dicha estrategia.

Del mismo modo, deberá llevarlo a constituirse en referente obligado a nivel nacional en todo lo relacionado a la temática. Parte de esa redefinición, implicaría un incremento de sus efectivos y el crecimiento de la organización, incluso a expensas de las organizaciones de ciberdefensa de cada fuerza. En ese sentido, la subordinación de los intereses particulares de cada Fuerza a un interés superior y la colaboración permanente, serán dos factores determinantes para el éxito de la estrategia.

Por último, la cooperación e integración con organismos equivalentes en otros Estados, en especial con Brasil, basada en acuerdos de reciprocidad, permitiría un incremento sustancial en la seguridad del sistema de Defensa Nacional y de los sistemas informáticos del Estado, contra todo tipo de amenazas cibernéticas.

BIBLIOGRAFÍA

- AFCEA. (s.f.). (19 de Diciembre de 2012). *AFCEABELVOIR*. Recuperado el 27 de Mayo de 2013, de http://www.afceabelvoir.org/images/uploaded/DEC2012presentation.pdf
- Amir Averbuch, Gabi Siboni. (2013). The Classic Cyber Defense Methods have failed. *Military and Strategic Affairs, 5*(1), 45.
- Arismendi, L. (s.f.). *http://luisarizmendi.blogspot.com.uy*. Obtenido de http://luisarizmendi.blogspot.com.uy/2014/03/ataques-dos-y-ddos-prevencion-deteccion.html
- ARMADAS, E. M. (10 de 08 de 2017). *http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa*. Obtenido de http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Mision.aspx
- ARMY, U. (s.f.). *U.S. ARMY CYBER COMMAND - U.S. 2nd ARMY*. Recuperado el 26 de MAYO de 2013, de http://www.arcyber.army.mil/org-uscc.html
- Arquilla, J; Ronfeldt D. (1993). *CYBERWAR IS COMING!* Pennsylvania: National Security Reaserch Division.
- Baretto, J. F. (2013). *La Guerra Preventiva Y El Ataque Cibernetico. Una forma no sangrienta de combatir.* Trabajo de investigación, ESGCFFAA.
- BID, O. . (2016). *http://observatoriociberseguridad.com*.
- Borghello, L. C. (02 de noviembre de 2015). Nuevas herramientas para estar seguros en la Web. Buenos Aires, Argentina.
- Castillo, U. (2013). *Information Systems Audit and Control Association (ISACA).* Recuperado el 11 de MAYO de 2014, de http://www.isaca.org/Education/Conferences/Documents/Latin-CACS-2013-Presentations/213.pdf
- CCCDOE. (2016). *National Cyber Security Organisation: United States.* Obtenido de https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf
- CCCDOE, N. (s.f.). *Cyber Security Strategy Documents*. Obtenido de https://ccdcoe.org/strategies-policies.html
- CCCDOE, N. (s.f.). *National Cyber Security Organisation*. Obtenido de https://ccdcoe.org/national-cyber-security-organisation.html

- CCDCOE, N. (2017, ABRIL 27). *https://ccdcoe.org*. Retrieved from https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html
- CICTE. (2012). Declaración “Fortalecimiento De La Seguridad Cibernética En Las Américas”. *Declaración “Fortalecimiento De La Seguridad Cibernética En Las Américas”*, (Pág. 8). Nueva York.
- CIO, D. (s.f.). *DoD CIO Priorities for 2014.* Obtenido de https://www.slideshare.net/GTSCoalition/robert-carey-principal-cio?from_action=save
- Civil, P. d.-C. (18 de Diciembre de 2008). Decreto Nro 6703. *Estratégia Nacional de Defesa*. Brasilia. Obtenido de http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm
- Clapper, J. R. (2015). *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community.* Senate Armed Services Committee.
- Cowan, G. (Julio de 2017). USN aims for information warfare "Top Gun". *Jane´s International Defence Review, 50*, 27.
- De Vergara, E. (Enero-Abril de 2013). Hic Svnt Leones. La seguridad informática y de telecomunicaciones de un Estado. (E. S. Guerra, Ed.) *La Revista*(583), 78.
- Defense, D. o. (2015). *Law Of War.* Whashington DC, EEUU.
- Defesa, M. D. (2014). Doutrina Militar Da Defesa Cibernética. En M. D. Defensa.
- *DefesaNet*. (27 de Diciembre de 2012). Recuperado el 29 de Mayo de 2013, de http://www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa
- Excelence, N. C. (s.f.). *NATO Summit Updates Cyber Defence Policy*. Obtenido de https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html
- Excellence, N. C. (s.f.). *Defending The Network - The Nato Policy On Cyberdefense*. Obtenido de https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf
- Exército, C. d. (Noviembre de 2012). Projeto Estratégico de Defesa Cibernética. (G. e. Ltda, Ed.) *Verde Oliva*(217), 30-33.
- Fein, G. (Julio de 2017). Raytheon looks to cyber intrusion detection system for pilots. *Jane´s International Defence Review, 50*, 26.
- Fireeye. (21 de 09 de 2016). *Anatomy of Advanced Persistent Threats.* Obtenido de https://www.fireeye.com/currentthreats/anatomy-of-a-cyber-attack.html

- Fryer-Bigss, Z. (3 de MAYO de 2017). The Digital Front Line. (IHS, Ed.) *Jane´S Defence Weekly, 54*(18), 22.
- Gobierno. (2017). *https://www.argentina.gob.ar.* Obtenido de https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf
- Gómez de Agreda, Á. (21 de Febrero de 2012). *El Ciberespacio como entorno social y de conflicto.* (I. E. Estratégicos, Ed.) Recuperado el Mayo de 18 de 2013, de http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO17_CiberespacioConflicto_Agreda.pdf
- *Govtech*. (19 de Abril de 2013). Recuperado el 29 de Mayo de 2013, de http://www.govtech.com/security/Cyber-Intelligence-Sharing-and-Protection-Act-Passes-House.html
- *Govtech*. (30 de Abril de 2013). Recuperado el 29 de Mayo de 2013, de http://www.govtech.com/policy-management/Senate-Wont-Look-at-CISPA.html
- House, T. W. (s.f.). *International Strategy for Cyberspace 2011.* Obtenido de https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- Igarape-Institute. (Junio de 2012). *A fine balance: Mapping cyber (in)security in Latin America.* Informe Estratégico.
- Instituto Nacional de Ciberseguridad (INCIBE). (Noviembre de 2016). *Servicio antiransomware*. Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware
- Kaspersky. (s.f.). *kaspersky-lab*. Recuperado el octubre de 2016
- Lab, Kapersky. (18 de noviembre de 2014). *http://latam.kaspersky.com/*. Obtenido de http://latam.kaspersky.com/co/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2014/stuxnet-paciente-cero-revelan-las-primeras-vi
- Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* Pittsburgh: RAND Corporation.
- *Mandiant*. (2013). Recuperado el 11 de abril de 2013, de http://intelreport.mandiant.com/
- Marke, J. (7 de septiembre de 2011). *“We Have Crossed Into Syrian Airspace” Operation Orchard.* Recuperado el 26 de mayo de 2013, de Prologue: https://www.box.com/shared/gs2o4yr0hroxgz51r867
- McAfee. (2011). *Ciberataques contra la energía mundial: Night Dragon (Dragón*

Nocturno). White Paper. Recuperado el 17 de Junio de 2014, de https://www.mcafee.com/in/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

- Milanes , V., & Uciferri, L. (Mayo de 2016). *Ciberseguridad En La Era De La Vigilancia Masiva - Descubriendo la agenda de ciberseguridad en América Latina: El caso de Argentina.* Obtenido de https://adcdigital.org.ar/wp-content/uploads/2016/06/ciberseguridad-argentina-ADC.pdf
- *Military Today*. (2016). Obtenido de Http://www.military-today.com.
- Nación, P. d. (s.f.). *http://servicios.infoleg.gob.ar.* Obtenido de http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm
- NATO. (s.f.). Obtenido de NATO Rapid Reaction Team To Fight Cyber Attacks: http://www.nato.int/cps/en/natolive/news_85161.htm
- NATO. (s.f.). *NATO Rapid Reaction Team to fight cyber attack*. Obtenido de http://www.nato.int/cps/en/natolive/news_85161.htm
- NATO. (s.f.). *New threats: the cyber-dimension.* Obtenido de http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm
- NATO. (s.f.). *Wales Summit Declaration*. Obtenido de http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en
- NATO. (s.f.). *Wales Summit Declaration*. Obtenido de http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber
- NATO, C. (s.f.). *NATO Cybersecurity Policy - 2011*. Obtenido de https://ccdcoe.org/cyber-security-strategy-documents.html
- Nuclear Threat Initiative. (2016). *The 2016 Nti Nuclear Security - Theft And Sabotage: Building a Framework for Assurance, Accountability, and Action. 3rd edition.* Recuperado el enero de 2017, de http://www.ntiindex.org/wp-content/uploads/2016/03/NTI_2016-Index-Report_MAR-25-2.pdf
- OEA. (2004). Adopción De Una Estrategia Interamericana Integral De Seguridad Cibernética. *Adopción De Una Estrategia Interamericana Integral De Seguridad Cibernética: Un Enfoque Multidimensional Y Multidisciplinario Para La Creación De Una Cultura De Seguridad Cibernética.*
- ONU, A. G. (s.f.). Resolucion De La Asamblea General NRO 55/63 Lucha contra la utilización de la tecnología de la. Obtenido de http://www.iri.edu.ar/publicaciones_iri/anuario/A01/Dep-

Anexo/Naciones%20Unidas/a55r063s.pdf
- ONU, A. G. (s.f.). Resolucion De La Asamblea General NRO 56/121 Lucha contra la utilización de la tecnología de la. Obtenido de http://www.unodc.org/pdf/crime/a_res_56/121s.pdf
- Ortiz, J. U. (Septiembre - Diciembre de 2012). Estrategias de defensa cibernética en la era de la información. (E. S. Guerra, Ed.) *La Revista*(582), 95.
- Pablo Edgardo Camps Laserre. (2016). Ciberdefensa Y Ciberseguridad: Nuevas Amenazas A La Seguridad Nacional, Estructuras Nacionales De Ciber Defensa, Estrategias De Ciberseguridad Y Cooperacion Interagencias En Este Ámbito. En C. D. Iberoamericanos, *Ciberdefesa E Cbersecuranca: Novas Amenazas A Seguranca Nacional* (Pág. 265). Rio De Janeiro: Escola Superior De Guerra.
- *Portaltic*. (26 de Abril de 2013). Recuperado el 29 de Mayo de 2013, de http://www.europapress.es/portaltic/sector/noticia-ley-cispa-podria-quedarse-estancada-senado-eeuu-20130426141536.html
- PRESIDENCIA. (s.f.). *INFOLEG - Resolución 81/99.* Obtenido de Secretaría de la Función Pública
- Ramos, Cobb, Gutierrez Amaya. (2016). *Tendencias 2016 (In) Security everywhere.* ESET , Madrid.
- (s.f.). *Report Of The Chairman Of Hleg To Itu - Secretary General .* Informe Final , HLEG. Obtenido de http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf
- Sampaio, F. (2001). *Ciberguerra. Guerra Eletrônica e Informacional – Um Novo desafio Estratégico.* Informe para debate, Escola Superior de Geopolítica e Estratégia, Brasilia.
- Sánchez Medero, G. (2010). Los Estados y la Ciberguerra. *Boletín Informativo Nro 317 - Ministerio de Defensa Español*, 64.
- Shmuel Even, D. S.-T. (2012). *Cyber Warfare:Concepts and Strategic Trends.* Tel Aviv: INSS.
- Shmuel Even, David Siman-Tov. (2012). CyberWarfare: Concepts and Strategic Trends. The Institute for National Security Studies.
- Stel, E. (2005). *Guerra Cibernética.* Buenos Aires: Círculo Militar.
- Tabansky, L. (2011). *Basics concepts in Cyber Warfare.* Military and Strategic Affairs, Tel Aviv. Recuperado el diciembre de 2013
- Thomas, T. (Julio - Agosto 2001). Las estrategias electrónicas de China. *Military*

Review, 72-79.

- Union Internacional De Las Comunicaciones. (2011). *La Busqueda De La Paz En El Ciberespacio.* ITU.
- USGovernment. (14 de Julio de 2011). *Defense.Gov*. Recuperado el 29 de Mayo de 2013, de http://www.defense.gov/news/d20110714cyber.pdf
- Veracode. (s.f.). *Veracode*. Obtenido de https://www.veracode.com/security/spoofing-attack
- Willett, D. L. (03 de mayo de 2017). Addressin Russia´s hybrid warfare threat. (I. jane´s, Ed.) *Jane´s Defense Weekly*, 20. Recuperado el 11 de mayo de 2017
- Zetter, Kim (julio de 2011). Countdown to Zero Day. Crown Publishers, New York

ANEXO 1: GLOSARIO

A

ACCIÓN (D. AMC)
Conjunto de medidas, previsiones y actividades destinadas al logro de un objetivo.

ACCIÓN MILITAR (D. AMC)
Este concepto puede ser abordado en una doble acepción:
1. Actividad necesaria para desarrollar una función militar, en virtud de las facultades profesionales atribuidas.
2. Empleo de fuerzas militares para cumplir una misión.

ACCIÓN CONTRIBUYENTE (D. AMC)
Esfuerzo que una organización militar realiza tendiente a incrementar la capacidad de otra.

ACCIÓN MILITAR CONJUNTA (D. AMC)
Elaboración, diseño, empleo y ejecución coherente, coordinada y sistemática de medidas, previsiones y actividades de medios y recursos puestos a disposición por dos o más Fuerzas Armadas de un país, bajo un solo comando y con la misma finalidad, durante las etapas de planeamiento, preparación, empleo y ejecución de los medios y recursos militares disponibles, en el ámbito del “Sistema Militar”.

AGENCIA
Organización especializada a la que se confía la gestión de un servicio.

AGRESIÓN EXTERNA (D. AMC)
Uso de una Fuerza Armada por parte de uno o más Estados contra los intereses vitales de la Nación, o de cualquier forma de acción que sea incompatible con la Carta de las Naciones Unidas.

AMBIENTE OPERACIONAL (D. AMC)
Conjunto de condiciones y características que existen en forma estable y semiestable en

una región. Forman parte del ambiente operacional: la influencia de la política nacional, el ambiente geográfico, la composición y capacidades de las fuerzas enemigas, las características de la lucha, los sistemas de armas que puedan emplearse y el marco de la conducción militar.

AMENAZA (D. AMC)

Acción consciente y deliberada de un actor que, teniendo capacidad, muestra la intención o da indicio de probable concreción de un perjuicio en contra de los propios intereses.

AMENAZA CIBERNÉTICA

Acción consciente y deliberada de un actor que, teniendo capacidad y mediante el empleo del espacio cibernético, ocasione un perjuicio al cumplimiento de la propia misión.

ANALISIS FODA

Es una metodología de estudio de la situación de una organización o un proyecto analizando sus características internas (DEBILIDADES y FORTALEZAS) y su situación externa (AMENAZAS y OPORTUNIDADES).

DEBILIDADES: se refieren a todos aquellos elementos, recursos, habilidades y actitudes que la organización ya tiene, que constituyen barreras para lograr su buen desarrollo.

FORTALEZAS: son todos aquellos elementos internos y positivos que diferencian a la organización o proyecto de otros de igual tipo o clase.

OPORTUNIDADES: son aquellos factores positivos que se generan en el entorno de la organización y que, una vez identificados, pueden ser aprovechados para el desarrollo de la misma.

AMENAZAS: son situaciones negativas y externas al programa, proyecto y organización que pueden atentar contra esta, por lo que llegado el caso, puede ser necesario diseñar una estrategia adecuada para neutralizarla o sortearla.

C

CIBERNETICA

Es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y las maquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes.

CIBERATAQUE / ATAQUE CIBERNÉTICO (MINIDEF COLOMBIA)

Acción, a través del espacio cibernético, organizada y/o premeditada de un actor para perturbar, negar, neutralizar o destruir información y/o sistemas informáticos y otros asociados.

CIBERAMBIENTE / AMBIENTE CIBERNETICO (DIRECTIVA 02/13 JEMCFFAA)

Incluye actores, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas, firmware de dispositivos que están conectados directa o indirectamente a las redes asociadas a los sistemas de capacidades del Instrumento Militar.

CIBERDEFENSA / DEFENSA CIBERNETICA (DIRECTIVA 02/13 JEMCFFAA)

Conjunto de acciones desarrolladas en el ambiente Cibernético para prevenir y contrarrestar toda amenaza o agresión cibernética. Utilizado normalmente en el ámbito militar.

CIBERSEGURIDAD / SEGURIDAD CIBERNETICA

Sinónimo del término Defensa Cibernética. Utilizado normalmente en el ámbito público y privado.

CIBERESPACIO / ESPACIO CIBERNETICO (DIRECTIVA 02/13 JEMCFFAA)

Ámbito virtual en el que se desarrollan actividades de procesamiento, almacenamiento y explotación relacionadas con los datos e información digital, a través de redes interdependientes e interconectadas, software, firmware de dispositivos, cuyo carácter distintivo está dado por el empleo de las tecnologías de información y comunicaciones.

CIBERDEFENSA MILITAR / DEFENSA CIBERNETICA MILITAR:

Es el conjunto de operaciones desarrolladas a los fines de garantizar:

1. La protección de las redes informáticas y activos de la jurisdicción del Ministerio de Defensa y del Instrumento Militar.

2. La defensa contra aquellas amenazas cibernéticas que pretendan ocasionar un perjuicio al Instrumento Militar, en cumplimiento de su misión principal, misiones subsidiarias y otras responsabilidades.

3. Las operaciones cibernéticas de defensa indirecta en el ciberespacio, en el marco estricto de la misión principal asignada al instrumento militar.

CIBERDEFENSA MILITAR DIRECTA (CDMD) / DEFENSA CIBERNETICA MILITAR DIRECTA:

Operaciones permanentes del Instrumento Militar (IM) que garantizan la confidencialidad, autenticidad, no repudio, integridad y disponibilidad de la información digital del ambiente cibernético de la jurisdicción del ministerio de defensa y del IM, dirigidas a asegurar el empleo en todo momento de las tecnologías de la información, las comunicaciones y los sistemas de control inherentes a las capacidades del IM frente a potenciales agresiones cibernéticas.

CIBERDEFENSA MILITAR INDIRECTA (CDMI) / DEFENSA CIBERNETICA MILITAR INDIRECTA:

Conjunto de operaciones del IM dirigidas a afectar la superioridad de un agresor en el ambiente cibernético de interés de la defensa nacional, siempre en el marco del cumplimiento de su misión principal.

CIBERINTELIGENCIA / INTELIGENCIA CIBERNÉTICA

Incluye todas las acciones, a través del espacio cibernético, destinadas a la recolección o reunión, procesamiento y uso de la información.

COMANDO (D. AMC)

La estructura compuesta por el Comandante, su Estado Mayor y todo otro elemento considerado necesario para facilitar el ejercicio de sus funciones en la conducción de las fuerzas puestas a su disposición.

D

DEBILIDADES (D. AMC)

Aquellas deficiencias de diferente naturaleza que se detectan en las propias fuerzas, en el enemigo u oponente o en algunos de los factores que conforman un ambiente operacional de interés.

DIRECCIÓN GENERAL

Organismo superior que dirige los diferentes sectores en que se divide la administración pública.

E

EFICACIA (D. AMC)

Es el resultado o acción que se obtiene como producto de la correcta selección de la metodología (actividades y procedimientos) y de la forma en que ésta se emplee en el marco del proceso del desarrollo de las misiones, funciones y actividades asignadas.

Implica el logro de la tarea de la misión sin considerar la aceptabilidad de la misma en cuanto a la relación costo – beneficio.

EFICIENCIA (D. AMC)

Empleo racional de los medios disponibles a efectos del logro de la meta propuesta del modo más óptimo posible. Implica el logro de la tarea de la misión, considerando la aceptabilidad de la misma en cuanto a obtener el mayor beneficio al menor costo.

ENTENDER (D. AMC)

Ocuparse directamente de un asunto con responsabilidad primaria

F

FUNCIÓN (D. AMC)

Actividad diferenciada dentro de un conjunto orgánico. Deber, responsabilidad o tareas propias o asignadas a un individuo, cargo u organización.

I

INTERVENIR (D. AMC)

Tomar parte de un asunto, interponiendo autoridad pero sin tener responsabilidad primaria.

INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN (JEFATURA DE GABINETE DE MINISTROS)

Son las instalaciones, redes, servicios, equipos físicos y de tecnología de la información cuyo funcionamiento es indispensable para brindar servicios a los ciudadanos y las instituciones.

P

PARTICIPAR (D. AMC)

Tener parte en un asunto determinado sin interponer autoridad.

R

RIESGO

La probabilidad que una vulnerabilidad sea explotada con éxito por una amenaza, comprometiendo la confidencialidad, integridad y/o disponibilidad y daño de los propios sistemas.

S

SEGURIDAD (D. AMC)

Desde una dimensión funcional, refiere al conjunto de recaudos para limitar o anular los riesgos y efectos de una amenaza. Se concreta en la adopción de medidas y mecanismos destinados a evitar, en lo posible, la materialización de dichos riesgos o amenazas, como, en su defecto, los efectos que de ellos puedan derivarse.

T

TAREA (D. AMC)

Este concepto puede ser abordado desde una doble acepción:

1. Acciones que implican la consecución de un resultado.

2. Cualquier acción o trabajo que se realiza como parte del cumplimiento de una actividad.

TRATADO (D. AMC)

Instrumento jurídico internacional celebrado entre dos o más Estados o entre estos y organizaciones internacionales, con objeto de crear, modificar o extinguir derechos u obligaciones.

V

VULNERABILIDAD

Una debilidad que puede ser aprovechada por una amenaza.