ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA:

Ciberdefensa

TÍTULO:

Análisis a nivel operacional del ataque cibernético al desarrollo militar en la República Islámica de Irán en el año 2010 y las medidas y modos de acción adoptados en la República Argentina.

AUTOR: Capitán de Corbeta Pablo Nicolás Miranda.

PROFESORA: María Cristina Alonso.

Año 2016

RESUMEN

Las nacientes amenazas en materia de ciberdefensa y los nuevos escenarios emergentes de características virtuales, generan una preocupación constante en la seguridad de los sistemas de información y comunicaciones en las fuerzas armadas.

El ataque cibernético perpetrado a la central nuclear en Irán en 2010, situada a 17 kilómetros al sureste de la ciudad de Bushehr, para destruir el programa nuclear llevado adelante por dicho país, constituye un claro ejemplo que permite tomar conciencia, sobre este tipo de amenaza y sobre la cual demanda un análisis.

A raíz de lo descripto, Argentina, se encuentra transitando un incipiente camino sobre esta temática y debe elaborar políticas y tomar medidas tendientes a robustecer su sistema de defensa nacional, ante potenciales o posibles ciberataques.

Por lo expuesto, como objetivo general se analizó como se relaciona el ataque cibernético a una central nuclear y cuál fue el impacto en el ambiente de la ciberdefensa y de qué modo influyo en los modos de acción y medidas adoptadas por la República Argentina a nivel operacional.

La hipótesis planteada en la investigación es que el ataque cibernético a una central nuclear en la República de Irán, en 2010 se relacionó con otros factores y a su vez impacto en los modos de acción, adoptados por la República Argentina para el nivel operacional.

Se corroboró al evidenciar que un comandante operacional, debe tomar decisiones sumamente complejas y que exige abordar el análisis desde una manera sistémica en cada ambiente dentro del teatro de operaciones, lo que permitió concebir al ciberespacio como un nuevo ambiente para llevar adelante operaciones.

PALABRAS CLAVE

Ciberdefensa - Defensa y seguridad - Guerra Cibernética - Redes -Teatro de Operaciones.

Tabla de contenidos

Tabla de Figuras

INTRODUCCIÓN

El estudio del ciberespacio como nuevo escenario virtual emergente y las nuevas amenazas en materia de ciberdefensa generan una preocupación constante para la seguridad de los sistemas de información y comunicaciones en las Fuerzas Armadas.

Dicho ambiente creado por el hombre posee la capacidad de adaptarse y sus herramientas empleadas en el mutar continuamente, como se puede ver en la actualidad en las formas de operar de quienes poseen desarrolladas dicha capacidad.

La creación de diferentes virus informáticos, es sólo uno de los ejemplos de cómo los estados o hasta personas con una serie de conocimientos en informática, pueden servirse de ellos para observar o causar desestabilización a otros, con el objetivo principal de perjudicarlos.

En junio de 2010, se conoció al gusano Stuxnet[1]. En ese momento fue identificado como el primer gran virus informático, orientado a la industria y diseñado para atacar al programa nuclear que llevaba adelante la República de Irán, en donde se pretendía sabotear las plantas nucleares iraníes de enriquecimiento de uranio de Natanz.

Se trató del primer *malware*[2] dirigido específicamente a sistemas de infraestructuras consideradas como críticas, como muestras de ser un claro agente o herramienta desestabilizante que se propaga a través de unidades de "memoria flash USB[3]".

Este tipo de ataques, tan sólo fue el inicio de una serie de malware, dirigidos principalmente, a países de Oriente Medio.

---

[1] Stunext es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, pudiendo afectar a infraestructuras críticas como centrales nucleares.
https://es.wikipedia.org/wiki/Stuxnet

[2] Malware es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
https://www.infospyware.com/articulos/que-son-los-malwares

[3] Memoria flash USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB, memoria externa o pendrive.
https://es.wikipedia.org/wiki/Memoria_USB

La presente investigación pretende, por medio del análisis de caso, proporcionar un estudio en materia de ciberdefensa, para entender la complejidad de este nuevo flagelo y generar conciencia sobre la necesidad de doctrina para las Fuerzas Armadas, hoy prácticamente inexistente. La misma busca determinar las medidas y modos de acción, adoptados por la Argentina a nivel operacional, para poder mitigar la falta de protección de "infraestructuras críticas[4]", de algún ciberataque.

Desde el 2010 hasta el presente, las Fuerzas Armadas no son ajenas a la proliferación de ciberataques o ciberoperaciones, a tal punto que hoy en día, se debe actuar efectivamente en un ámbito más, uno de características virtuales denominado "Ciberespacio". Ello se debe a que, si bien Argentina no es considerada un país blanco, se han detectado diferentes ataques, los cuales con muy pocos recursos pueden desarrollar acciones hostiles de gran impacto.

Por lo tanto, existe la necesidad de replantear las medidas de seguridad, a ser implementadas por las Fuerzas Armadas, conducentes a minimizar los efectos que pueden llegar a producir los ciberataques.

En su alcance, la misma busca profundizar en la temática del ambiente de ciberdefensa, para que sean aplicadas dentro de un teatro de operaciones, muchas veces poco definido o fácilmente identificable, teniendo en cuenta que el mismo para esta actividad está dado o constituido por todo el espacio.

Se excluyeron cuáles son las medidas adoptadas por otros países en materia de ciberdefensa, a nivel regional.

El interrogante que surge es ¿Cómo se relaciona el ataque cibernético a una central nuclear en Irán, en 2010 con respecto a las medidas y modos de acción adoptados por la República Argentina, a nivel operacional en materia de ciberdefensa?

Como objetivo general, se plantea analizar con que se relaciona el ataque cibernético a una central nuclear en Irán, en 2010 y cuál es su impacto y modo de acción adoptado por la República Argentina a nivel operacional.

[4]Estructura o infraestructura critica: "Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas". https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad

Los objetivos específicos hacia los cuales se orienta la investigación y de acuerdo a la hipótesis planteada son: describir si el ataque cibernético a una central nuclear en Irán en 2010, produjo una nueva perspectiva en materia de ciberdefensa en Argentina y evaluar con que factores se relaciona, como también describir cuales son desde la doctrina existente en las Fuerzas Armadas a nivel operacional, las medidas adoptadas para enfrentar posibles o potenciales ataques cibernéticos hacia puntos considerados críticos y / o vitales.

La investigación será de tipo exploratoria descriptiva, donde se busca especificar la particularidad de esta temática.

Para este trabajo se empleó el análisis de bibliografía seleccionada y consultada sobre ciberdefensa, en particular artículos de revistas militares e información existente en el sitio de internet, portales digitales, artículos periodísticos y trabajos de investigaciones obrantes en la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. El trabajo está estructurado en dos capítulos, en el primero contiene conceptos generales sobre ciberdefensa y analiza el impacto del ataque cibernético perpetrado a la República de Irán para la Argentina en materia de ciberdefensa. El segundo capítulo describe la importancia de contar con doctrina propia y cuáles son las diferentes medidas y modos de acción que deben ser adoptados por Argentina, a nivel operacional, en el nuevo ambiente: el ciberespacio.

CAPÍTULO I

"Conceptos generales sobre ciberdefensa en relación a los elementos del diseño operacional y análisis del impacto del ataque cibernético perpetrado a la república de Irán para la Argentina"

1.1. Introducción

El presente capítulo desarrolla conceptos generales, los cuales desde un nuevo enfoque, permite entender que el ciberespacio es un nuevo ámbito bélico, con características propias, dinámicas y distintivas muy diferentes a las utilizadas en otros tipos de conflictos y describe específicamente cuales son los diferentes segmentos que pueden llegar a presentarse, en este nuevo escenario de confrontación, teniendo en cuenta al ciberespacio como un nuevo teatro de operaciones militares.

Para iniciar el desarrollo se enunciaran algunas definiciones de elementos del diseño operacional, con los que un comandante operacional está relacionado, entre las que se encuentran el espacio definido como teatro de operaciones, el estado final deseado, el centro de gravedad como así también comenzar a entender a qué se refiere cuando se habla de ciberespacio, ciberdefensa, los tipos de amenazas que se encuentran él y algunas herramientas con las que se debe contar y se deben definir, debido a su especificidad.

Según lo establecido en el libro titulado "Arte y diseño operacional", de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, el Teatro de Operaciones, se define como: "*Área geográfica terrestre, marítima o mixta, junto con el aeroespacio asociado, para la conducción, establecida por la máxima autoridad nacional, para la conducción de operaciones militares a cargo de un comandante del teatro de operaciones*"[5].

Entonces, podemos decir que dicho espacio una vez declarado y definido, será el área en donde el comandante operacional, tendrá la responsabilidad absoluta de sus operaciones y de las campañas que lleve adelante.

Pero para delimitarlo aún más, solo se tendrá en cuenta en dicha área geográfica lo circunscripto y concerniente al nivel operacional, teniendo en

[5] Kenny, Alejandro, Locatelli, Omar, Zarza, Leonardo; Arte y diseño operacional; Contribución académica V; Escuela Superior de Guerra Conjunta de las fuerzas armadas, Capítulo 4 "Elementos tradicionales del diseño operacional"; Buenos Aires; 2015; P.58.

cuenta que este es el que traduce lo que pretende el Nivel Estratégico y le ordena al Nivel Táctico [6] llevarlo a la práctica.

En este nivel por lo general se determina que es lo que pretende el nivel estratégico y que luego de haber efectuado esa interpretación por parte del comandante y su estado mayor, el nivel táctico llevará las acciones tendientes a definir cómo llevar adelante las mismas para el logro del estado final deseado que se pretende, en donde en la misma publicación anteriormente descripta queda definido como: *"La situación política y / o militar que debe existir cuando las operaciones se den por finalizadas en términos favorables"*

Dicha definición es considerada en términos generales, pero debido a que existe un estado final para cada nivel de la guerra, tomaremos en cuanta la que corresponde para el nivel operacional la cual está definida como: "*El estado de cosas a alcanzar o mantener al finalizar las acciones militares en un teatro de operaciones"*[7]

Ello implica que una vez finalizada dichas acciones dentro del teatro de operaciones se debe haber alcanzado el estado anteriormente mencionado y fijado por el comandante.

También se debe considerar que significa el término centro de gravedad, el cual permite definir, a un comandante operacional, cual es el ente sustantivo al cual debe proteger tomando en cuenta al propio.

Al centro de gravedad se lo identifica de acuerdo a la siguiente definición como: "*La fuente de poder que provee fortalezas o capacidades esenciales para el cumplimiento de los intereses, objetivos y misiones de un actor"*[8].

Dichos conceptos son importantes y se deben tener presentes a la hora de definir y priorizar cuales serán catalogadas como infraestructuras militares críticas a ser protegidas contra posibles ciberataques.

---

[6] Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; Planeamiento para Acción Militar Conjunta - Nivel Operacional; PC 20-01; Proyecto 2015; Capítulo I; PP. 4 - 5.

[7] Kenny, Alejandro, Locatelli, Omar, Zarza, Leonardo; Arte y diseño operacional; Contribución académica V; Escuela Superior de Guerra Conjunta de las fuerzas armadas, Capítulo 4 "Elementos innovadores del diseño operacional"; Buenos Aires; 2015; P 64.

8 Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; Edición 2015; PC 20-01 "Planeamiento para la Acción Militar Conjunta - Nivel Operacional"; Buenos Aires; capítulo 2; articulo 2.03.2.; P 19.

1.2 Nuevos conceptos dentro de un nuevo ámbito: el ciberespacio

Para desarrollar nuevos conceptos cibernéticos, los cuales contribuyen y clarifican la temática abordada, se debe empezar definiendo al nuevo escenario, el ciberespacio como:*" El dominio operacional cuyo carácter distintivo y único está enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar la información a través de los sistemas basados en las Tecnologías de Información y Comunicaciones (TICS) y también sus infraestructuras asociadas ".*[9]

Se puede decir entonces que el ciberespacio es un entorno artificial el cual se desarrolla a través de diferentes herramientas que posee la informática y suele asociarse a la red global o comúnmente denominada internet, pero es aún más amplio y abarcativo.

En dicho ámbito se llevan a cabo diferentes operaciones las cuales de acuerdo a su naturaleza pueden catalogarse como defensivas u ofensivas y que debido a su especificidad se las denomina ciberoperaciones.

Ellas deben entenderse como una herramienta más para la solución de problemas militares dentro del ciberespacio, teniendo en cuenta que en éste, no hay un límite geográfico definido.

El teatro de operaciones, entonces estará determinado por las redes globales interconectadas.

Si las ciberoperaciones a través de diversos ciberataques, son utilizadas de modo defensivo, las mismas perseguirán detectar, mitigar y neutralizar, el impacto que pueda producir un ataque o bien evitar que cumpla con su efecto para el cual fue dirigido.

En cambio, las que se empleen de modo ofensivo, buscaran actuar sobre centros de gravedad, tratando de afectar a estructuras o infraestructuras consideradas críticas.

Pero para entender mejor lo que ocurre dentro del ciberespacio, se debe considerar, además cuales son los tipos de amenazas presentes, en este nuevo escenario de confrontación.

9 Kuehl, Dan: From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management College-National Defense University, Estados Unidos, 2009.

El concepto para calificar a los ciberataques, es sustancialmente diferente, según el alcance de los objetivos y actuaciones de los mismos.

Bajo este enfoque, se pueden segmentar tres (3) diferentes tipos de ciberoperaciones, pudiendo encuadrarlas de acuerdo a lo establecido en el trabajo del doctor Flores de la siguiente manera:[10]

a. <u>Cibercrimen:</u> *Cuando son individuos o grupos no estaduales, que utilizan el ciberespacio para cometer actos ilícitos en beneficio propio.*

   En general estas acciones son reconocidas como delitos y de incumbencia policial. Un ejemplo es el robo de identidad, para acceder a cuentas en entidades financieras.

b. <u>Ciberterrorismo</u>*: Cuando quienes lo realizan son individuos o grupos no estaduales que, a través del ciberespacio, buscan efectos de naturaleza variable sobre individuos, empresas e incluso Estados. Los medios para hacer frente a estas acciones variarán según sea el marco legal del Estado considerado.*

c. <u>Ciberguerra</u>*: Aquí aparecería la figura de un Estado o grupo de Estados que atacan la estructura funcional y / o decisional de otro u otros Estados, empleando el ciberespacio.*

   En este caso sería de aplicación el concepto de agresión establecido por la ONU (resolución 3314, del 14 de diciembre de 1974)[11], retenida por el Decreto 727 / 2006 que reglamentó la Ley de Defensa Nacional de la Argentina."

La descripción de estos nuevos conceptos que, por sus características particulares, comienzan a ser parte constitutiva de este nuevo ambiente,

10 FLORES, Héctor Rodolfo; Centro Superior de estudios de la Defensa Nacional; Los ámbitos no terrestres en la guerra futura: Ciberespacio; Buenos aires; marzo 2012; P 25.

[11]Definición de la agresión [Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas http://www.dipublico.org/4071/definicion-de-la-agresion-resolucion-3314-xxix-de-la-asamblea-general-de-las-naciones-unidas.

evidencian que no son solo responsabilidad exclusiva de las Fuerzas Armadas.

Por ello contar con metodologías y procedimientos doctrinarios orientados a la protección del ciberespacio frente a las nuevas amenazas a las que se encuentran expuestas las Fuerzas Armadas, son una constante necesidad cada vez más frecuentes y a las que se deberá prestar especial atención para poder fortalecer distintos sistemas e ir generando doctrina.

Para lograrlo se debe estar preparado permanentemente y estar en condiciones de dar en el momento oportuno, rápidas respuestas a este tipo de amenazas, permitiendo el fortalecimiento en las capacidades para actuar ante una amenaza de este tipo.

Sobre este tema, el autor Rodolfo Flores, sostiene que: *"El ciberespacio, ámbito creado por el hombre, no posee límites o barreras físicas definidas, presenta como una característica bien definida la de que es abierto y que permite su utilización en todo momento, y donde el uso de malware (virus) se realiza de manera rápida y en pocos segundos".*

En esta primera parte, permite inferir que el ámbito de aplicación, al no poseer barreras físicas que puedan ser definidas de manera clara, la amenaza en dicho ambiente podrá ser omnidireccional[12] y en todo tiempo aplicable, sin tener un intervalo de tiempo definido, lo que determina la necesidad de estar en permanente estado de alerta.

Ello exigirá un constante monitoreo de sus sistemas, para que en caso de detectar algún ciberataque en proceso, estar en condiciones de poder repelerlo / mitigarlo lo más rápido posible.

1.3 Medidas a implementar

Algunas de las medidas que pueden llevarse adelante para poder estar en permanente estado de alerta son:

- Revisar en todo tiempo y de manera aleatoria todos los programas de software que se utilizan y emplean en el aérea de la defensa y cuáles son sus niveles de seguridad que poseen.
- Posibilitar por medio de diseños propios de software, evitar una servidumbre en tecnologías particulares y específicas.

[12]Omnidireccional: Que se puede orientar o utilizar en cualquier dirección o sentido. http://servicios.elpais.com/diccionarios/castellano/omnidireccional.

- Emplear diferentes métodos de encriptado y uso de claves de acceso difíciles de romper, como protección para fortalecer y robustecer dichos sistemas.
- Utilizar anti malware y antivirus de última generación.
- Desarrollar herramientas para detectar y evitar rápidamente intrusiones al sistema de defensa o a las capacidades militares.

En otra parte del documento, el mismo autor plantea lo siguiente: *"…Visto los altos costos de los medios militares, más aún los relacionados a tecnologías de punta, debemos señalar que los medios empleados en un ataque cibernético poseen un muy bajo costo y se obtienen en forma libre (sin control) en el mercado".*[13]

En relación a lo anteriormente mencionado, se puede determinar que el daño que puede llegar a producirse, con este tipo de virus malicioso, el cual es almacenado en un pendrive o memoria USB[14]de fácil y libre adquisición, puede ser considerado de gran valor de empleo, en relación al costo que este posee, en comparación con el beneficio que se busca o desea lograr.

Debido a ello, cualquier país, que busque desestabilizar a otro y cuente con las capacidades ya sea por haberla desarrollada o haberla adquirida, podrá llevarla adelante, incluso desde un particular sector; el anonimato, lo que le agrega una mayor letalidad al ciberataque, al no poder determinar claramente, de donde fue generado o quien lo dirige.

1.4 Ley defensa nacional 23.554 y decreto reglamentario Nº 727/2006

Los países de acuerdo y en relación al marco normativo que poseen muchas veces presentan serias dificultades para imponer la legislación motivando muchas veces que los delitos que se cometen o llevan adelante en este ambiente cibernético sean difíciles de juzgar.

En cuanto a la regulación de Argentina, referida al uso del instrumento militar la ley de defensa nacional Nº 23.554, en su decreto reglamentario Nº 727/2006, establece que: "*El sistema de defensa debe ser orientado*

[13] FLORES, Héctor Rodolfo; Centro Superior de estudios de la Defensa Nacional; Los ámbitos no terrestres en la guerra futura: Ciberespacio; Buenos aires; marzo 2012; P.23.

.

[14] La memoria USB (*Universal Serial Bus*) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB, memoria externa, *pen drive* o *pendrive.* https://es.wikipedia.org/wiki/Memoria_USB.

estructural y organizativamente hacia la conjuración de situaciones de agresión externa perpetradas por fuerzas armadas de otro Estado"[15]

Este tipo de tipificación define claramente lo que el instrumento militar está autorizado a intervenir de acuerdo al plexo legal existente, ante esa figura definida.

Ello tiene por objeto poder determinar la naturaleza de los medios a emplear en este nuevo ámbito en estudio, creado por el hombre y en pleno desarrollo, según sea a cuál se enfrenta, que para este caso estará ligado a lo atinente a la ciberguerra o en el caso de ser objeto de una agresión estatal militar externa[16], contra las capacidades cibernéticas militares o hacia estructuras e infraestructuras críticas definidas.

1.5 Visión de diferentes organismos sobre la necesidad de nuevas Políticas / marco normativo en materia de Ciberdefensa

Se debe tener en cuenta cuales son las políticas y marco normativo existentes, para poder determinar cuáles serán los modos de acción a adoptar por la República Argentina, particularmente por las Fuerzas Armadas a nivel operacional, para poder a través de ellas contribuir a la protección y brindar seguridad a todas las infraestructuras críticas de algún ciberataque, que sea perpetrado por un agente estatal militar externo.

A continuación se mencionarán diferentes instituciones que han publicado trabajos referidos al marco legal y a las implicancias que ello tiene en materia de ciberdefensa.

Teniendo en cuenta lo publicado en 2014, en el informe de investigación del Ministerio de Defensa Argentino, titulado: "Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo", de la Escuela de Defensa Nacional, en esta primera parte se extractan diferentes párrafos donde se establece que: *"En la Resolución del*

15 República argentina; Decreto 727/2006; Reglamentación de la Ley Nº 23.554. Principios Básicos. Competencia del Consejo de Defensa Nacional. Atribuciones del Ministerio de Defensa. Estado Mayor Conjunto de las Fuerzas Armadas. Fuerzas Armadas. Disposiciones Complementarias; Título V; artículo 23; P 11.
http://www.ara.mil.ar/archivos/Docs/Decreto%20727.pdf

16 República argentina; Decreto 727/2006; Reglamentación de la Ley Nº 23.554. Principios Básicos. Competencia del Consejo de Defensa Nacional. Atribuciones del Ministerio de Defensa. Estado Mayor Conjunto de las Fuerzas Armadas. Fuerzas Armadas. Disposiciones Complementarias; Título 1; artículo 1º; P 5.
http://www.ara.mil.ar/archivos/Docs/Decreto%20727.pdf

Ministerio de Defensa N° 364 del año 2006, se establece la creación del Comité de Seguridad de la Información en el ámbito del Ministerio de Defensa ,el cual está integrado por los Directores Generales de las distintas agencias pertenecientes a la jurisdicción y es coordinado por la Subsecretaría de Coordinación. El origen del mismo se da a partir de la decisión administrativa N° 669/2004….".

"…..Además, se firma la Resolución del Secretario de Estrategia y Asuntos Militares N° 08 en el año 2010, mediante la cual se creó en el ámbito de esa Secretaria un grupo de trabajo, con el fin de analizar y evaluar la relevancia y la implicancia del ciberespacio en la agenda del Sistema de Defensa Nacional."

En la segunda parte del mismo informe el autor plantea además que: "*…En 2013 se conforma, en el ámbito de la Jefatura de Gabinete de Asesores del Ministerio de Defensa, la: "Unidad de Coordinación de Ciberdefensa", donde establece las funciones e integración de dicha unidad, reuniendo en una sola agencia la coordinación de la política relativa a ciberdefensa en el ámbito de la jurisdicción según la Resolución Nº 385/2013.*

Básicamente en la resolución anteriormente mencionada se establecen las funciones y coordinaciones de políticas generales referidas a ciberdefensa, consolidadas en una sola agencia.

El propósito que busca es poder generar mecanismos que se encuentren integrados para poder determinar que respuestas utilizar, ante posibles amenazas provenientes del ciberespacio.

Esas políticas también entenderán en lo referente a contar con un relevamiento minucioso y detallado de las infraestructuras críticas y estructuras militares, recursos humanos, actividades y protocolos a adoptar.

"*Así mismo dichas políticas buscan la permanente actualización en materia de procedimientos y equipamiento, lo cual observa la importancia del tema y a su vez da origen a un compendio de resoluciones que fueron firmadas en los últimos pasados años, para adoptar en primera instancia una actitud o postura defensiva en dicha materia".* [17]

[17] JUSTRIBÓ Candela, GASTALDI Sol, FERNÁNDEZ Jorge A; Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo; informe

En estos documentos formales promulgados, se evidencia una clara dirección en donde se percibe que existe, por parte de las máximas autoridades, una preocupación por el ciberespacio y la ciberdefensa.

Se busca en particular con ellos, coordinar y tomar todas las medidas vinculadas a la ciberdefensa, como así también impulsar el desarrollo doctrinario, analizando de manera permanente la evolución normativa, en relación con el marco y plexo legal referido a la defensa nacional.

Otro aspecto a considerar, es lo determinado por el Consejo Argentino para las Relaciones Internacionales (CARI); en materia de ciberdefensa del mes de noviembre del año 2013, referente a los riesgos y amenazas, en donde básicamente se centraliza en determinar las implicancias que tiene la ciberdefensa para un estado y da lineamientos generales por donde se debería empezar a transitar referidas a la capacitación, adiestramiento y medidas.

En dicho informe, se determinó que: "*Hay una necesidad de elaborar planes de capacitación y adiestramiento en técnicas y tácticas, con un enfoque sistémico de la ciberdefensa y generar nuevas medidas.*

En el mismo escrito detalla que*, iniciada la colección de información, se seguirá con el registro, la clasificación y el análisis de la misma, de manera tal, que resulte útil al sistema de la Defensa, puesto que el ciberataque, puede vulnerar objetivos de valor estratégico nacional y dejar al país sin capacidad de Comando y control dentro de un teatro de operaciones.* "[18]

En dicho informe se comienza a visualizar que existe una necesidad de comenzar a trabajar de manera conjunta, en forma interdisciplinaria y cooperativa para no solo aunar esfuerzos, sino como una manera de comenzar a transitar un camino que permita formar doctrina conjunta en materia de ciberdefensa.

En concordancia con ello y de acuerdo a las políticas adoptadas por el Ministro de Defensa en el año 2014, se ordenó la creación del Comando Conjunto de Ciberdefensa, dependiente del Estado Mayor Conjunto de las

---

de investigación presentado en la escuela de defensa nacional; Buenos Aires; Octubre2014; P 13.

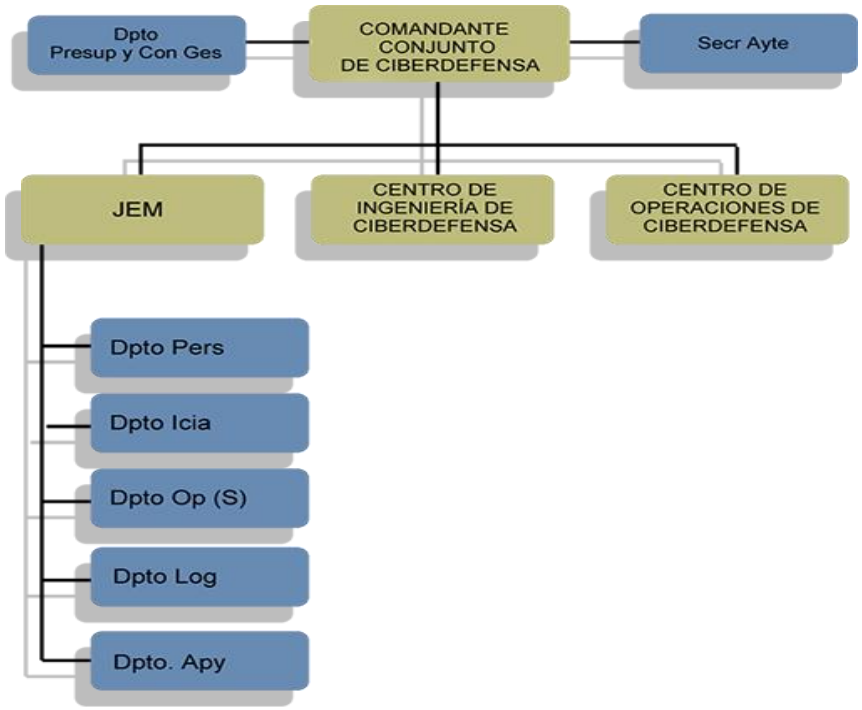
[18] CARI; ciberdefensa-ciberseguridad: Riesgos y Amenazas; Buenos Aires; noviembre 2013; P 31.

Fuerzas Armadas, Organismo que tiene la misión de [19]:"*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"*

A su vez también determina que el mismo Comando Conjunto tiene la función de: *"Coordinar sus acciones con los Centros de Ciberdefensa de las Fuerzas Armadas, entiéndase a los centros del Ejército Argentino, al de la Armada Argentina y al de las Fuerza Aérea Argentina como así también de establecer los criterios rectores, a nivel del instrumento militar, para la determinación de infraestructuras críticas a ser protegidas".*

Teniendo en cuenta que el organismo descripto anteriormente, es el máximo organismo rector actualmente en funciones en materia de ciberdefensa, el mismo se encuentra estructurado de acuerdo al siguiente esquema que a continuación se detalla:

Figura 1: Organización del Comando Conjunto de Ciberdefensa.



Fuente: Recuperado de http://www.fuerzas armadas.mil.ar /imágenes/dependencias/CIBEF/Organigrama CIBDEF.png&imgrefurl

[19] Presidencia de la Nación; Estado Mayor Conjunto de las Fuerzas Armadas; Comando conjunto de ciberdefensa.
http://www.fuerzas-armadas.mil.ar/Dependencias-CIBDEF.aspx

En la figura, se puede observar cómo se encuentra estructurado y organizado el Comando Conjunto de Ciberdefensa, como así también, cuáles son los diferentes departamentos y centros que lo componen.

Cronológicamente y a la luz de lo establecido en el trabajo realizado por la Universidad de Belgrano en materia de ciberdefensa, en diciembre del año 2015, se detallaba que: *"La modernidad introdujo un nuevo espacio y forma de conflicto que, si bien no está plenamente asumido, siempre está activo y nadie puede escapar de él.*

El ciberespacio constituye una nueva dimensión creada por el hombre en la que es difícil atribuir una agresión y que genera una nueva preocupación para los estados.

Cualquier proyecto debería considerar el desarrollo de un marco legal y protocolos, el diseño y aplicación de una estrategia organizacional y, especialmente, la generación de una cultura nacional ciudadana. "[20]*.*

Se ha seleccionado el trabajo anterior debido a que el mismo se centra en la necesidad del desarrollo de nuevos protocolos y modos de acción en ciberdefensa y también marca la necesidad de que los mismos tengan el aval y marco legal necesario.

Todo lo anteriormente mencionado en los diversos trabajos y documentos normativos, se interrelacionan y permiten determinar el inicio, referido a la nueva conciencia que ha generado a nivel global y en particular en las Fuerzas Armadas, los ataques cibernéticos constatados por ejemplo en lo que se refiere al desarrollo militar en la República Islámica de Irán, en el año 2010 y años subsiguientes hasta el presente.

Se describe a continuación lo publicado en diferentes medios de comunicación en relación a dicho ataque.

Podemos aseverar a esta altura con los datos vistos hasta el momento, que quien cuente con un importe desarrollo en materia de ciberdefensa y acompañado de un marco normativo, podrá afrontar de una mejor manera y sentirse más seguro, como así también estar en condiciones de mitigar, evitar o contrarrestar las ciberamenazas a las que puede llegar a estar

[20] Doctor Jaunarena, H; *"*Ciberdefensa y ciberdefensa en la argentina *"*; Revista del centro de estudios para la defensa nacional, CEDEF, universidad de Belgrano Nº13, Buenos aires, diciembre 2015.
http://www.ub.edu.ar/centros_de_estudio/cedef/13_diciembre_2015.pdf

expuesto, pero solo podrá llevarse adelante, si la normativa legal se lo permite.

1.6 Ataque cibernético al desarrollo militar en Irán en 2010

Ahora lo que se pretende es relacionar el ataque cibernético al programa nuclear de Irán, considerado las repercusiones que se replicaron en diferentes medios internacionales.

Referido a ello, se puede constatar que, en varios medios de comunicación durante el año 2010, la República islámica de Irán aseguraba que sus instalaciones nucleares estaban a salvo.

Al mismo tiempo, reconocía que el virus denominado "Stuxnet" al cual se lo consideraba como el primer *gusano* informático capaz de atacar y afectar a plantas industriales, habría afectado al menos 30.000 computadoras dentro de su territorio y continuaría propagándose hacia otras por medio de internet.

Un extracto del artículo del diario: El País de España, en su sección internacional publicaba lo siguiente: *"Los ataques continúan y se están propagando nuevas versiones de ese gusano", informó ayer Hamid Alipour, director adjunto de uno de los principales proveedores de Internet de Irán, citado por la agencia Irna. El malware "Stuxnet" salió a la luz en junio cuando una compañía de seguridad informática de Bielorrusia, Virus BlokAda, lo descubrió en unos ordenadores pertenecientes a un cliente en Irán."*[21]

En esta primera parte se observa que al principio cuando se detectaron los ataques se creía que los mismos se trataban de un programa diseñado para robar información de las computadoras buscando hallar procesos de fabricación, sin embargo, luego de conocerse nuevas especificaciones sobre sus capacidades y estructura de diseño en particular, la probabilidad de que hubiera sido creado para sabotear el programa nuclear iraní, habría extendido el interés de toda la opinión pública internacional sobre este tipo de ciberataque.

---

[21] ESPINOSA, Ángeles;" Irán sufre un ataque informático contra sus instalaciones nucleares"; Diario el País; Sección internacional; Teherán; 28 de septiembre de 2010.

El Gobierno de la República islámica de Irán por su parte a través de medios oficiales, afirmo que estaría siendo víctima de una "ciberguerra proveniente desde Occidente", en donde consideraba que el virus malicioso seguiría actuando y se encontraría fuera de control.

Dicho ataque en principio estaría dirigido por Estados Unidos. Esta sospecha surge debido a que Irán, su principal enemigo, estaría desarrollando armas nucleares a través de su programa nuclear para enriquecimiento de Uranio.

Irán por su parte negó esas acusaciones enfáticamente, en diversos medios de comunicaciones, a través de sus voceros.

En una segunda parte se afirma que el jefe de la central nuclear de Bushehr, Mahmud Jafarí, admitió que: “Estaban tratando de eliminarlo de varias computadoras pertenecientes a los empleados de la central atómica. Estas computadoras estarían contempladas dentro de las 30.000 contaminadas por dicho gusano, mencionadas anteriormente de acuerdo a lo manifestado y reconocido por el Secretario del Consejo de Tecnología de la Información en el Ministerio de Industria.”

Debido a ello, se comenzó a instalar la idea sobre que la República de Irán se encontraría atravesando, un caso de ciberguerra o guerra de la información[22], la cual afecto temporalmente las actividades de enriquecimiento de uranio de Teherán.

Teniendo en cuenta de que la República islámica de Irán es un país en donde ha sufrido últimamente la mayor cantidad de ciberataques registrados y debido a e la complejidad que presenta dicho malware, ya que el mismo no estaría al alcance de un pirata informático común, ello demuestra que en referencia a la ciberoperaciones estarían en manos de uno o varios estados.

En una tercera parte del mismo artículo y de acuerdo al análisis efectuado por especialistas iraníes que analizaron el tema, determinaron que: *“El virus Stuxnet, está dirigido a un programa concreto de la marca Siemens, que se utiliza principalmente en el control de oleoductos, de plataformas petroleras,*

[22] El concepto de guerra informática, guerra digital o ciberguerra –en inglés: *cyberwar*– hace referencia al desplazamiento de un conflicto, que toma el ciberespacio y las tecnologías de la información como campo de operaciones.
https://es.wikipedia.org/wiki/Guerra_informatica.

en centrales eléctricas, centrifugadoras nucleares y otras instalaciones industriales, con el objetivo de sabotearlas.

Eso ha llevado a especular que una vez dentro de una planta, por ejemplo, la planta nuclear de Natanz, dicho virus estaría en condiciones de comenzar a reprogramar las centrifugadoras con el objetivo de ocasionar fallas aleatorias, sin que las mismas puedan ser fácilmente detectadas".

Desde el año 2010 y como consecuencia de ciberataques registrados, Irán, ha mantenido un constante y permanente control y vigilancia sobre sus estructuras e infraestructuras críticas, buscando contar con una capacidad de resiliencia de sus sistemas informáticos.

El día 26 de diciembre de 2012, en un hipertextual de internet en donde se había publicado lo siguiente: *"Así lo han asegurado las agencias de noticias del país. Al parecer, el gusano Stuxnet , estaba aparentemente destinado a una planta de energía y otros sitios, todos en el sur de Irán. Las autoridades aseguran que fue detenido a tiempo. Mientras, el gobierno acusa a Estados Unidos e Israel del intento de ataque. Se trataba del primer malware dirigido, específicamente a sistemas de infraestructuras críticas. En este caso concreto, dirigido a sabotear plantas iraníes de enriquecimiento de uranio de Natanz……*

…..El nuevo ataque ha sido informado a través de la agencia ISNA[23], quienes han explicado que el virus fue dirigido a una central eléctrica y otras industrias en la provincia de Hormozgan en los últimos meses.

En el mismo artículo hace referencia a que varios ataques fueron detectados en la industria oleosa la cual proporciona aproximadamente el 80% de los ingresos en el país, evidenciando que no solo se focalizo en el desarrollo militar, sino que actuaba en otros sectores.

……Stuxnet se propaga a través de unidades USB y tan sólo fue el comienzo de una serie de malware dirigido a países de Oriente Medio como parte del programa de Estados Unidos e Israel que busca desestabilizar el programa nuclear iraní."

Si se analizan las características del ataque cibernético al desarrollo militar en la República Islámica de Irán, perpetrado a la central nuclear, dicho

[23] La Agencia de Noticias de Irán Estudiantes (en Inglés Agencia de Noticias de Estudiantes Iraníes , ISNA):Es una agencia de noticias con sede en Irán , y mantenida por estudiantes universitarios.
https://pt.wikipedia.org/wiki/Agencia_de_Noticias_Estudantil_Iraniana.

análisis demanda establecer particularmente, cuáles fueron las causas y sus efectos en el teatro de operaciones o escenario de confrontación.

A través del análisis del ataque a las centrifugadoras del centro nuclear iraní de Natanz, se puede visualizar, cuáles fueron las consecuencias que ocasiona este tipo de nueva amenaza.

Expertos iraníes, de los cuales no se conocen sus nombres de forma pública, creen que si se usaran nuevas versiones del virus empleado, contra diferentes sectores como por ejemplo en hospitales o aeropuertos o la industria por citar alguno de ellos, se generaría un caos total asociado a grandes pérdidas económicas.

Se debe tener en cuenta que, al momento, Argentina no es objeto de ataques sistemáticos por no estar contenida dentro de un listado de los denominados como países “blanco”, entendiéndose como tal, a aquel que es elegido para efectuar o dirigir ciberataques, buscando con ello, lograr vulnerar y / o afectar sus infraestructuras críticas[24].

En la actualidad si bien existen, diferentes escenarios con características multidimensionales, que determinan la complejidad dentro del ambiente operacional, el ciberespacio ha cobrado una gran relevancia.

Entonces se debe tener en cuenta que las Fuerzas Armadas se encuentran expuestas a sufrir ataques cada vez más sofisticados y en constante evolución ya que las mismas, son consideradas como factor de poder.

24 Estructura critica: “Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas “. https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad

CAPÍTULO II

“Importancia de contar con doctrina propia y cuáles son las diferentes medidas y modos de acción que deben ser adoptados por la República Argentina, a nivel operacional en el nuevo ambiente: el ciberespacio.”

2.1 Introducción

El presente capítulo busca describir la importancia de contar con doctrina propia y cuáles son las diferentes medidas que deben ser adoptadas por la República Argentina, a nivel operacional en el ciberespacio.

Si se toma en cuenta que la Argentina no es considerada como un país blanco a quien vayan dirigidos gran cantidad de ataques cibernéticos, se ha constatado que se reciben ataques a diario a estructuras o servidores.

Esos ataques buscan encontrar vulnerabilidades o poder penetrar sistemas que se encuentren protegidos, con el objeto de llevar adelante ataques efectivos y exitosos o por el solo hecho de probar cuan robustos son los mismos, en referencia a su seguridad.

Entonces es importante contar con doctrina militar[25] propia pues permite estar en capacidad de contar con diferentes medidas y métodos que posibiliten estar en condiciones de poder hacer frente a la guerra en el ámbito del ciberespacio.

2.2 Doctrina propia

Considerando que hay que destacar que, aunque el país carece de doctrina en relación a este tema, se comenzó a dar señales y reflexionar a partir del año 2006 sobre el nuevo ambiente denominado ciberespacio.

En este sentido cada fuerza posee un centro de repuesta destinado a tareas en esta área los cuales se encuentran bajo el paraguas del Comando Conjunto de Ciberdefensa, siendo éste el órgano máximo de control y comando para las Fuerzas Armadas.

Ello ha permitido contar con doctrina básica para formular estrategias, técnicas y tácticas que llevadas a la práctica permiten operar en dicho ambiente.

---

[25] La doctrina militar se trata del conjunto de estrategias, tácticas, técnicas y prácticas que constituyen el accionar de los militares. La doctrina compartida por los militares delimita todo el comportamiento de los mismos, y establece los pasos a seguir en caso de guerra. http://www.definicion.co/doctrina/

Pero también se debe considerar que debido a la reciente creación del Comando Conjunto anteriormente mencionado existe a la fecha muy poca doctrina militar conjunta y que el mismo según lo ordenado por el Estado Mayor Conjunto de las Fuerzas Armadas, debe intervenir en la elaboración, revisión y experimentación de doctrina en materia de ciberdefensa.

Ello implica que dicho organismo debe elaborar y difundir a las diferentes fuerzas, doctrina unificada, revisando la doctrina existente en cada una de las fuerzas para determinar si debe ser modificada o dejada sin efecto como producto del reemplazo por una nueva.

En cuanto a la experimentación, se refiere a que deberá poner en práctica en el campo del ciberespacio, a través de por ejemplo ejercicios o simulaciones de ataques para ver cuáles son los resultados obtenidos como así también las modificaciones o mejoras que puedan surgir luego de realizar dichos eventos.

El hecho de contar con doctrina propia, permite afianzar diferentes conocimientos y poder contar con expertise, para determinar distintos modos de acciones a emprender ante un evento o situación determinada, para proteger infraestructuras críticas o evitar que se vulneren sus sistemas.

2.3 Otros ciber ataques a estructuras petroleras y militares en Irán

En relación al ataque perpetrado a la central nuclear de Irán en 2010 se pensaba en un primer momento que sería un ataque que tendría un inicio y un final, más aún luego de haber sido detectado y comunicado a la comunidad internacional, por diferentes medios de comunicación, ya que muchos países comenzaron a estar más alerta en cuanto a los niveles de seguridad que adoptan a los efectos de poder ser alcanzado por distintos ciberataques.

Si bien se conoce que tuvo un inicio, se puede decir que el mismo no finalizo, debido a que después del virus Stuxnet llegaron otros virus que, si bien eran diferentes, tenían el mismo patrón, dando una idea de que eran la continuación o provenían del mismo creador que el Stuxnet.

Para poder ejemplificar más aun lo que se pretende demostrar y considerando lo publicado por el diario New York Times el día 01 de junio de 2012, dos años después del incidente, publicaba un artículo en donde señalaba enfáticamente que: *“El origen del virus o malware denominado Stuxnet, provenía*

de los Estados Unidos de América. La ola de ataques contra la planta nuclear de Irán habría sido ordenada por el presidente de dicho país."[26]

Luego de diferentes investigaciones llevadas a cabo por expertos en Irán, pudieron llegar a la conclusión sobre quien estaría detrás de los diversos ataques a el desarrollo militar en Irán.

Si bien Estados Unidos lo negó en diferentes medios de comunicación, la Republica de Irán, asegura que posee pruebas de dicho país estuvo detrás de esos ataques.

Otro diario, el Washington Post, en su versión digital del 19 de junio del mismo año, también coincidía en informar sobre nuevos ataques sufridos o direccionados hacia Irán, confirmando que otro tipo de malware o gusano, conocido con el nombre de Flame, tenía como objetivo atacar el programa nuclear de Irán. Este software malicioso de vigilancia es el más complejo hasta el presente y también habría sido desarrollado por Estados Unidos e Israel.

Básicamente dicho virus, recopilaba datos privados incluso de los que poseen alta seguridad y esa información era procesada y utilizada por parte del país que había efectuado el ciberataque.

La firma de seguridad Kaspersky,[27] quien lo detecto, afirmo lo siguiente: *"Una vez que el sistema está infectado, Flame comienza un complejo conjunto de operaciones, incluyendo la sustracción del tráfico de la red, realiza capturas de pantalla, graba conversaciones de audio, intercepta el teclado y así sucesivamente.*

Hasta el momento se estima que dicho malware seria la continuación del Stuxnet y en el que estarían involucrados varias agencias incluyendo la Agencia de Seguridad Nacional (NSA) estadounidense, la Agencia Central de Inteligencia (CIA) o los militares israelíes"[28].

---

[26] Sanger, David; Obama Order Sped Up Wave of Cyberattacks Against Iran; new york time; June 01 de 2012 recuperado de: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&hp

[27] Kaspersky: Es un grupo internacional activo en, aproximadamente, 200 países del mundo. Su sede central se encuentra en Moscú, Rusia, mientras que el holding está registrado en Reino Unido. Actualmente. Sus productos y tecnologías garantizan protección informática a más de 300 millones de usuarios. https://es.wikipedia.org/wiki/Kaspersky_Lab

[28] Ellen Nakashima, Greg Miller and Julie Tate; U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say ; Washington post; National security; June 19 de

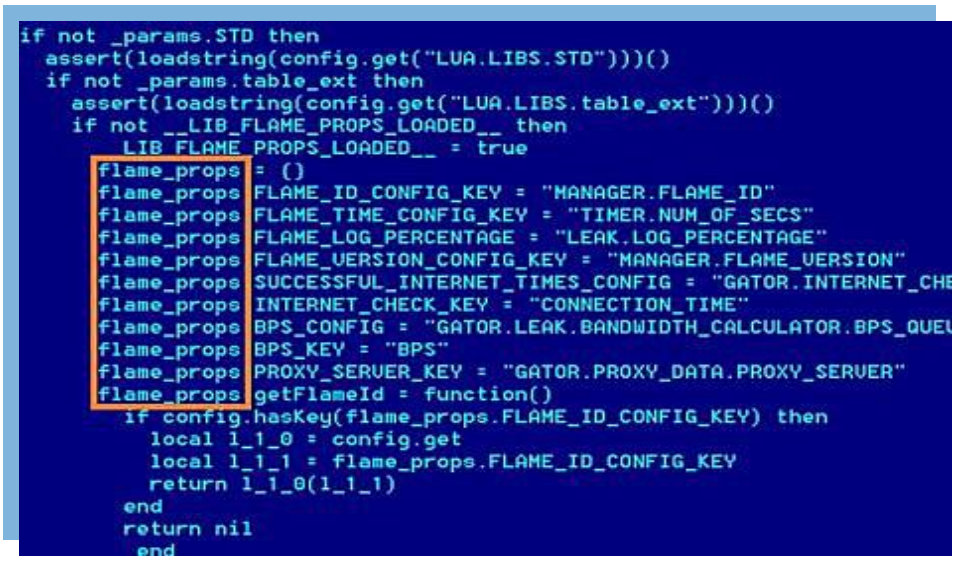
A raíz de los diferentes estudios de forencia efectuados a ambos virus se logró detectar que tanto el código del virus Flame con el del virus Stuxnet poseían patrones comunes entre sí, lo que hacen pensar que el gusano Flame habría sido desarrollado por los mismos que desarrollaron al Stuxnet".

Ello evidencia que el interés de países como Estados Unidos y la Republica de Israel, sobre Irán se mantenía y que a través del ciberespacio buscaban afectarlo principalmente en el desarrollo militar y en otros sectores económicos.

Así mismo no se limitó a usar un solo virus, sino que, por el contrario, luego de utilizarse al Stuxnet, le siguieron otros a lo largo del tiempo, pero todos ellos con un objetivo en común, el cual básicamente era el de afectar y vulnerar los desarrollos militares que Irán estaba llevando adelante.

Para poder ejemplificar dichos ataques se toma como ejemplo al virus Flame, en donde de acuerdo a una captura de pantalla obtenida se puede observar en la figura Nº2 como el virus se encuentra instalado dentro de los diferentes procesos, buscando información de utilidad la cual será duplicada, extraída y enviada a un ordenador bajo control del país que efectúo o realizo el ataque.

Figura N° 2: Captura de pantalla donde se insertó el virus Flame.



Fuente: Capturado de

http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html

2012, 2012 recuperado de : https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?hpid=z

La figura anterior demuestra como el gusano pudo penetrar en el software y comenzar a atacar y alterar los sistemas informáticos a los que se deseaba afectar ya que puede propagarse hacia otros sistemas por medio de la red o en memorias USB.

El mismo está constituido por varios módulos, ubicados en bibliotecas comprimidas, una base de datos y una computadora virtual y puede realizar capturas de pantallas, grabar audios y conversaciones de teleconferencias realizadas.

La particularidad que posee este tipo de virus es que puede quedar en estado latente o sin actividad dentro del sistema, a la espera de que por ejemplo un programador o experto, que conoce su codificación, le envíe nuevas instrucciones dirigidas a reactivarlo y a que comience con las tareas que fueron programadas anteriormente.

Las diferencias que tienen ambos virus radican en las funciones que ejecutaban cada uno, más allá de que el fin fuera el mismo, demorar el proceso de enriquecimiento de Uranio.

Como se pudo constatar a través de diferentes estudios de expertos iraníes, el virus Stuxnet fue diseñado para dañar procesos industriales, y como muestra de ello podemos observar el caso analizado en cuestión.

En cambio, el virus Flame es utilizado con fines de robo de información o como se conoce comúnmente en tareas de ciber espionaje industrial y militar.

Otra diferencia destacable referida a este virus es que le permite a los que lo manejan, eliminar todo rastro del sistema infectado, posibilitando que, si el mismo no hubiera sido detectado, luego de cumplir con la tarea encomendada, sea eliminado de dicho sistema.

Todo esto es un claro ejemplo de cómo los diferentes tipos de amenazas van mutando, actualizándose y mejorando.

Ello persigue que el enemigo u oponente esté siempre un paso adelante, de los diferentes sistemas de seguridad o medidas que debe tomar un estado para la protección de diferentes sectores y del instrumento militar en relación a sus puntos a proteger.

2.4 Ciber resiliencia

La resiliencia es una herramienta y un instrumento útil y necesario para afrontar este tipo de posibles o potenciales ciber ataques, a través de los diferentes virus descriptos anteriormente, a los que se encuentran expuestas las Fuerzas Armadas.

"*La ciber resiliencia se trata de la administración de riesgos, no de su eliminación. La eliminación no solo es imposible, sino que impide la agilidad; un entorno con un nivel aceptable de riesgo y admite innovación*."[29]

Dicha herramienta permite que, una vez detectado algún tipo de ataque efectuado a sistemas militares, poder controlarlo, entendiéndose que no se busca eliminarlo sino confundirlo, por ejemplo, si el malware empleado es utilizado para el robo de información, lo que se hace es confinarlo en alguna computadora y colocar allí datos falsos con algunos datos ciertos, creíbles y rápidamente comprobables por parte del oponente o enemigo que efectuara el ataque.

Ello permite poder engañar al agresor y además crearle una sensación de que está consiguiendo lo que se propone.

2.5 Indicadores

A su vez existe una necesidad de contar con indicadores que permitan mensurar la capacidad que poseen los diferentes centros de respuesta de las Fuerzas Armadas, ante distintos ciberataques, amenazas o incidentes que puedan detectarse.

Esos indicadores deberán ser los mismos en cada fuerza, para permitir y poder dimensionar, en relación a la capacidad de Resiliencia que se tiene, un rápido conocimiento sobre incidentes o eventos detectados y estado en que se encuentran los mismos.

Actualmente si bien los temas que se tratan en cada centro de respuestas pertenecientes a cada fuerza son similares, muchas veces la misma información es representada de formas y maneras diferentes y ello muchas veces genera demoras en la interpretación o divulgación de diferentes informes.

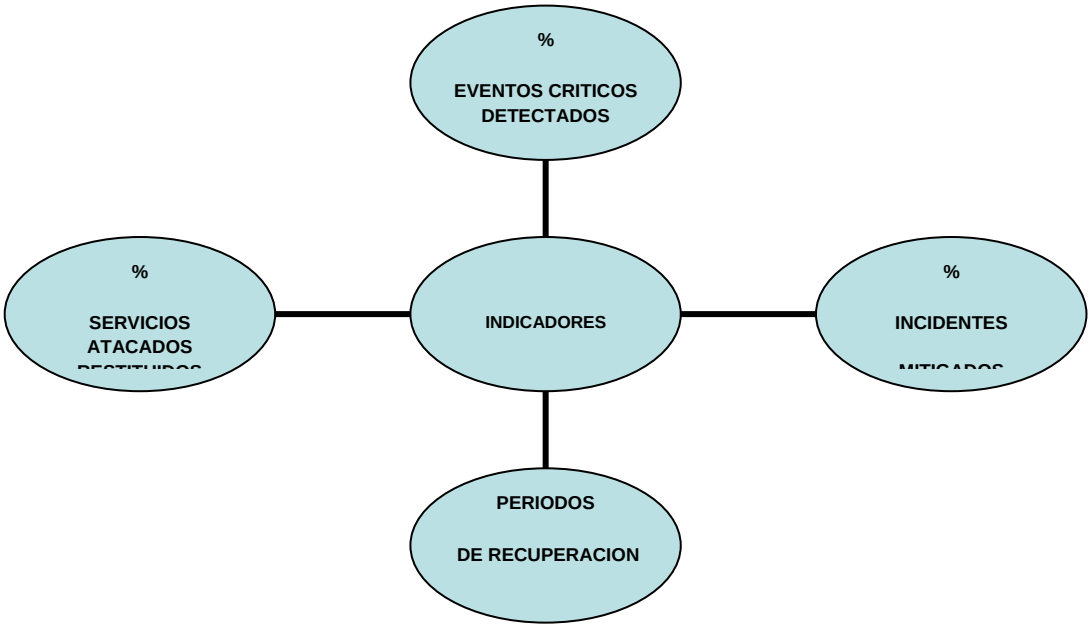
---

[29] Recuperado de:https://www.symantec.com/es/mx/page.jsp?id=cyber-resilience

Al poder contar con algunos indicadores de uso común, ello posibilitara, contribuir con la agilidad en el manejo y en la forma de representar los distintos tipos de datos con los que se cuentan y con los que se van generando en cada centro de ciberdefensa de cada fuerza.

Para ello el siguiente esquema, proporciona una idea de cómo podría estar constituida dicha información en cada centro de respuesta inmediata dentro de cada fuerza y en su zona de responsabilidad:

FIGURA Nº3: Indicadores en la capacidad de resiliencia.



Fuente: Elaboración propia.

2.6 Recursos materiales y humanos

Si bien el contar con modernas tecnologías y políticas orientadas a la ciberdefensa favorecen el dominio o superioridad en un ambiente en un teatro de operaciones, todas ellas deberán encontrarse sustentadas a través de diversas estructuras que contengan personal idóneo y capacitado.

Ello demanda la necesidad de contar con personal militar y civil dentro de cada fuerza armada y que este orientado a tareas vinculadas con el ciberespacio, en materia de medidas de seguridad, resguardo y protección de información y el manejo de nuevas tecnologías.

2.7 Normas y medidas en un teatro de operaciones

Para poder determinar cuáles son las normas y medidas a tener en cuenta en un teatro de operaciones se ha tenido en cuenta lo expresado en el trabajo de investigación del año 2013 del Capitán de Corbeta Giudici,D quien establece que se deberán cumplir con los siguientes principios como primera medida:[30]

- *Las fuerzas deben estar interconectadas a fin de mejorar el intercambio de información, la percepción de la situación, permitiendo la colaboración, sincronización y mejora de la velocidad en la toma de decisiones.*
- *Todo usuario tendrá un perfil de derechos de acceso a la información, dondequiera que se conecte a las redes de telecomunicaciones.*
- *Es vital la total interconexión con otros sistemas, incluso con organizaciones no gubernamentales (ONG's).*
- *Todos los usuarios precisarán recibir la formación y adiestramiento adecuados para utilizar adecuadamente cada uno de los sistemas que integran la red de la defensa.*
- *Necesitarán emplear todas las herramientas disponibles del sistema para extraer la información.*
- *Consideración de alianzas ya que habrá algunos estados y organizaciones que no estarán dispuestos a compartir cierta información sensible.*

Estos principios responden claramente a varias necesidades algunas de ellas insatisfechas hoy en día y que deben abordarse rápidamente para poder operar de la mejor manera posible y segura.

En cuanto a las organizaciones no gubernamentales se refiere a que en el teatro de operaciones actúan e intervienen cada vez con mayor frecuencia.

A su vez también abarca el tema del conocer con que herramientas informáticas se cuentan y están disponibles para su empleo.

[30] Giudici, D; " *Lineamientos para la seguridad cibernética en un teatro de operaciones*"; Trabajo Final Integrador de la especialización en Estrategia Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta, Buenos Aires, 2013; P 15.

Por ultimo define la necesidad de formar alianzas regionales, a mi entender en principio dentro de un marco regional para poder lograr confianza mutua, transferir conocimiento y experiencias y posibilitar capacitar al personal especializado para que el mismo se encuentre actualizado y pueda poner en práctica sus conocimientos adquiridos.

En otra parte del mismo documento el autor plantea lo siguiente:

"Independientemente *del tipo de amenaza cibernética, las acciones que se pueden llevar a cabo dentro de dicho teatro sin importar donde se encuentre ubicado, pueden ser defensivas u ofensivas.*

Sin embargo, y de acuerdo al marco legal vigente para el instrumento militar argentino, la ausencia de hipótesis de conflicto y el nivel de seguridad cooperativa alcanzado en la región, se pondrá atención en las acciones defensivas, ensayando una suerte de ordenamiento por fases:

- *Alistarse para un ataque a los sistemas y a las redes de la información para estar en condiciones de.*
- *Replicar el ataque.*
- *Recobrar las capacidades operativas de los sistemas y de las redes de información. "*[31]

El plexo legal al que están sujetas las Fuerzas Armadas y al que hace referencia fue explicado en forma parcial en el capítulo 1, pero básicamente responde a lo detallado en el párrafo anterior, lo que determina que las Fuerzas Armadas adoptaran en relación a dicho marco legal una actitud defensiva en materia de ciberdefensa.

Las tres fases comprenden con la necesidad en todo momento de realizar tareas de alistamiento y ante un ataque estar en condiciones de replicar o sea de responder en contra de lo que el virus pretendió hacer o estar en capacidad de engañarlo y al mismo tiempo estar en condiciones de poder recuperar y restituir en el menor tiempo posible el sistema atacado o afectado.

[31] Giudici, D; " *Lineamientos para la seguridad cibernética en un teatro de operaciones*"; Trabajo Final Integrador de la especialización en Estrategia Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta, Buenos Aires, 2013; P 18.

En relación a todo lo expresado, se debe considerar que la Argentina necesita poner en práctica nuevas medidas y modos de acción en relación a la interopetividad que se necesitan entre las Fuerzas Armadas para trabajar y operar de manera conjunta y aunar esfuerzos en este nuevo escenario creado por el hombre y tomar conciencia de que este tipo de guerra asimétrica es hoy en día un flagelo al que todo país se encuentra expuesto, no solo las Fuerzas Armadas.

Ello demanda una interrelación entre el poder político y las Fuerzas Armadas hacia un mismo objetivo.

El primero de ellos será el encargado de dictaminar las políticas y lineamientos a seguir en materia de ciberdefensa, no solo para la Argentina, sino también congruentes dentro de un ambiente de cooperación a nivel regional. Puede ser tomado en consideración y como ejemplo las llevadas adelante con la República Federativa de Brasil.

Si bien todavía es un gran desafío en el que las Fuerzas Armadas deben comenzar a transitar, los primeros pasos y señales que pudimos observar en el presente trabajo marcan un gran interés y preocupación por este tipo de amenazas presentes en todo el ciberespacio.

Entonces todo ello deberá constituir un plan director que permita a la argentina ser un referente en materia de ciberdefensa y con proyección a nivel regional marcando una clara visión sobre la problemática enunciada.

CONCLUSIONES

Sobre la base del análisis efectuado del ataque cibernético al desarrollo militar en la República Islámica de Irán en el año 2010, y a la luz de los resultados obtenidos en los capítulos anteriores, se puede arribar a las siguientes conclusiones:

- En respuesta al interrogante planteado por este trabajo, se puede afirmar que es posible, a partir del ataque hacia Irán, crear una clara necesidad de conciencia en las Fuerzas Armadas respecto a las amenazas que se emplean en el ciberespacio y cuáles son los impactos que producen.
- Luego del desarrollo de nuevos conceptos, se puede arribar a la conclusión de que el nuevo ambiente, al que nos enfrentamos, demanda nuevas medidas y métodos para poder estar protegidos ante futuros posibles ciberataques.
- El plexo legal existente, permite el uso del instrumento militar ante un conflicto contra un agresor estatal militar externo, dentro de un teatro de operaciones declarado.
- El tiempo transcurrido desde el ataque a Irán en 2010 y las medidas y políticas adoptadas por las autoridades nacionales hasta el presente año, permiten visualizar que se ha tomado conciencia de los riesgos presentes en el ciberespacio y la necesidad de priorizar todo desarrollo o modo de acción a llevar a cabo a fin de evitar que un posible agresor pueda afectar a la República Argentina.
- Implementar políticas adecuadas y trabajos conjuntos entre las tres Fuerzas Armadas y el Estado Mayor Conjunto de las Fuerzas Armadas, permitirá generar y contar con doctrina en el corto plazo.
- Se puede afirmar la hipótesis planteada ya que a pesar de que los ciberataques fueron hacia Irán, los mismos causaron impacto en Argentina y llevo a tomar diferentes medidas a partir del hecho descripto.

Las nuevas líneas de investigación, pueden enfocarse con respecto a cómo Argentina está posicionada a nivel regional y cuáles son los convenios bilaterales con otros países buscando la interacción, compartir experiencias, transferencia de conocimientos y adiestramiento para poder hacer frente a este flagelo cada vez más creciente.

BIBLIOGRAFÍA

1- Libros

- Borghello, C; Seguridad informática, sus implicancias e implementación; Universidad Tecnológica Nacional; Buenos Aires; 2001.
- Consejo Argentino para las Relaciones Internacionales, CARI; Ciberdefensa, Ciberseguridad; Riesgos y Amenazas; Noviembre 2013.
- Justribó, C; Gastaldi, S; Fernández, J; " Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo"; EDENA; Buenos Aires; 2014.

2- Revistas, Boletines, Fascículos

- Jaunarena, H; “Ciberdefensa y ciberdefensa en la argentina“; Revista del centro de estudios para la defensa nacional, CEDEF, universidad de Belgrano; Nº13, Buenos Aires, diciembre 2015.
- Lucero, G "La dimensión desconocida”, Revista Visión conjunta; Escuela superior de guerra conjunta de las fuerzas armadas; Nº12- Buenos Aires ,2015; pp. 36 – 42.
- Uzal, R "Guerra Cibernética: ¿un desafío para la Defensa Nacional?" Revista Visión conjunta; Escuela superior de guerra conjunta de las fuerzas armadas; Nº7- Buenos Aires, 2012, pp.40 – 47.

3- Manuales y Reglamentos

- Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; República Argentina; Planeamiento para la Acción Militar Conjunta. Nivel Operacional; PC 20-01; Revisión 2015.

4- Recursos de Internet

- Espinosa, Á; Irán sufre un ataque informático contra sus instalaciones nucleares- Teherán 28 de septiembre 2010; recuperado de:http://elpais.com/diario/2010/09/28/internacional/1285624808_850215.html.
- Estados Unidos e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán; EFE, Washington; 26 de junio 2012; recuperado de: http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html

➢ Flores, P; Planta nuclear en Irán sufre ataque de gusano; 27 de septiembre de 2010; recuperado de: https://hipertextual.com /2010/09/planta-nuclear-en-Irán-sufre-ataque-de-gusano.

➢ Miguel, J; Stuxnet ataca a Irán de nuevo; 26 de diciembre de 2012; recuperado de: https://hipertextual.com/2012/12/stuxnet-ataca-a-iran-de-nuevo.

➢ Nakashima Ellen, Miller Greg and Tate Julie: U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say ; Washington post; National security; June 19 de 2012, 2012 recuperado de: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?hpid=z1

➢ Sanger, D; Obama Order Sped Up Wave of Cyberattacks Against Iran; new york time; June 01 de 2012 recuperado de: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&hp

➢ Stephens, Bret; Los límites de Stuxnet; 2011; recuperado de: http://soysionista.blogspot.com.ar/2011/01/los-limites-de-stuxnet.html

➢ Umphress, D; el ciberespacio: ¿un aire y un espacio nuevo?; Air & Space Power Journal - Español Tercer Trimestre 2007; recuperadode:http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2007/3tri07/umphress.html

5- <u>Trabajos no publicados</u>

➢ Giudici, D; " Lineamientos para la seguridad cibernética en un teatro de operaciones"; Trabajo Final Integrador de la especialización en Estrategia Operacional y Planeamiento Militar Conjunto; Escuela Superior de Guerra Conjunta Fuerzas Armadas; Buenos Aires; 2013.