MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

Tema:

Ciberdefensa

Título:

Análisis de las amenazas a la infraestructura crítica de un teatro de operaciones contemporáneo y maneras de combatirlas

Autor: My. (FAA) Mauricio Hernán Ortiz

Profesora: Lic. María Cristina Alonso

2015

Resumen

La dependencia que las sociedades actuales tienen con respecto a los sistemas informáticos es cada vez mayor, resultando muy difícil el desarrollo de la vida ciudadana sin el apoyo que los mismos prestan en todas las áreas, entre ellas la económica, la sanitaria o la de transportes, siendo esto especialmente evidente en los países más avanzados tecnológicamente. De esta dependencia nace una vulnerabilidad que un virtual adversario podría explotar y de allí la necesidad de brindar un marco que posibilite la protección adecuada y oportuna de estos sistemas.

Esto mismo sucede en un teatro de operaciones donde se ubican elementos bélicos de gran sofisticación tecnológica, que al tiempo que le conceden elevadas capacidades los hace susceptibles de ser atacados a través del ciberespacio, siendo estos ciberataques patrocinados por los Estados. Por lo tanto se advierte la necesidad de contar con un Elemento de Ciberdefensa a Nivel Operacional que brinde al Comandante ciertas capacidades para hacer frente a las amenazas cibernéticas y que colabore con los otros dominios operativos del combate (terrestre, marítimo, aéreo y espacial), en la obtención de los objetivos por éste planteados.

El presente trabajo de investigación propone un criterio de organización de los Elementos de Ciberdefensa a Nivel Operacional y su relación con los niveles Estratégicos y Tácticos; asimismo indica los servicios esenciales que éstos deben brindar, tanto reactivos como proactivos y de gestión de calidad en seguridad, y todas las áreas funcionales que se deben considerar conducentes a manejar un programa robusto de Ciberseguridad, dando por cumplido el objetivo general y la hipótesis planteada de establecer una manera de proceder que permita limitar las acciones nocivas y las amenazas cibernéticas que puedan afectar alguna estructura crítica del estado, y las capacidades del instrumento militar dentro de un teatro de operaciones contemporáneo.

Palabras clave:

Ataque Cibernético - Ciberdefensa - Ciberseguridad – Nivel Operacional.

Tabla de contenido

Resumen i
Palabras clave: i
Introducción 1
Capítulo I: Ciberespacio y su marco legal en los conflictos armados 4
Derecho Internacional respecto a la Ciberdefensa 4
Principio de Distinción en Ciberdefensa 6
Bienes de uso dual en Ciberdefensa 8
Marco Legal en Argentina 9
Capítulo II: Amenazas Cibernéticas 12
Incremento de los Ciber-arsenales 12
Objetivos de los Ciberataques 13
Ciberataques con Objetivos Económicos 14
Ciberataques con Objetivos Psicosociales 15
Ciberataques con Objetivos Políticos 16
Ciberataques con Objetivos Militares 17
Capítulo III: Ciberdefensa en el Nivel Operacional 20
Clasificación de Grupos de Riesgo en Ciberdefensa 21
Elemento de Ciberdefensa a Nivel Operacional 21
Servicio que deben prestar los Equipos de Seguridad en Ciberdefensa 25
Servicios Reactivos 25
Servicios Proactivos 25
Servicios de Gestión de Calidad en Seguridad 25
Áreas funcionales del Elemento de Ciberdefensa 26
Conclusiones 28
Bibliografía 31
Anexo 1: Prácticas de Ciberataques 37
Anexo 2: Amenazas Cibernéticas 40
Anexo 3: Figuras 43
Anexo 4: Niveles de Fiabilidad 45

Introducción

El concepto Ciberespacio se utiliza por vez primera en 1984, año en que William Gibson publica su novela de ciencia ficción *Neuromancer*. Actualmente este espacio virtual no solo ha dejado de ser ciencia ficción, sino que a ganado tanta relevancia que ha sido reconocido por el Departamento de Defensa de Estados Unidos y el Pentágono como *el quinto dominio de la guerra junto a tierra, mar, aire, y espacio*[1] como un área de potencial conflicto.

Entonces esta investigación trata esta problemática de los conflictos presentes y futuros, ya que el Ciberespacio a pasado a ser un lugar donde los estados dirimen sus diferencias debido fundamentalmente a la marcada dependencia que las sociedades modernas tienen de los sistemas de información que posibilitan el normal desarrollo de la vida de sus habitantes, como el sistema bancario, el sanitario, el financiero entre otros, los cuales deberán ser protegidos eficazmente evitando de esta manera una posición de precariedad o inferioridad ante un enemigo real o potencial.

En 1943, durante la Segunda Guerra Mundial, los aliados se centraron en bombardeos sobre diferentes objetivos, refinerías y centrales eléctricas entre ellos, tratando de afectar el sistema energético germano, realizándolos con armamento muy poco preciso y con una tasa de atrición propia que en términos actuales sería inaceptable y con resultados muchas veces decepcionantes, más adelante, en la guerra del Golfo Pérsico de 1991, para degradar el suministro eléctrico a la ciudad de Bagdad se emplearon filamentos de carbono que produjeron el corto circuito de las redes de energía, evitando así el uso de armamento con mayor poder destructivo.

En 2010 Israel, ante la imposibilidad de bombardear una central iraní, ya que la ruta área era demasiado larga, debiendo sobrevolar naciones neutrales y contra instalaciones subterráneas[2], opta por una acción más sigilosa e inteligente pero igualmente efectiva, introduciendo un virus cibernético denominado *Stuxnet* en las computadoras industriales del sistema de control de la central de Natanz, con el que logró retrasar el programa nuclear de un poderoso enemigo.

---

[1] Juan Carlos Batanero. "Ciberdefensa"; *IX CICLO DE CONFERENCIAS UPM TASSI*. Madrid: Indra, 2013. Diap. 3.

[2] Gema Sánchez Medero; "La ciberguerra: los casos de Stuxnet y Anonymous". *Derecom, Nueva Época. No. 11* , Septiembre-Noviembre, 2012; p. 130.

Es decir, se puede observar por medio de estos ejemplos como han evolucionado los métodos empleados en busca de un mismo efecto, en este caso afectar el sistema energético enemigo, y lograr al mismo tiempo evitar o mitigar los efectos no deseados del poder bélico de un estado, como el daño colateral, escalada de conflicto o la atrición propia, con el aporte de la tecnología.

Continuando con este desarrollo se observa como el concepto de distancia geográfica se desdibuja en el entorno cibernético, adquiriendo más importancia los intereses contrapuestos que configuran a potenciales enemigos que las fronteras físicas. Esto queda claramente graficado por diversos especialistas, como Richard A. Clarke*, entre otros, que tratan la batalla que desde hace algunos años libran países como China, Estados Unidos y Rusia en este ámbito virtual. [3]

En la ciberguerra la primera lección es la ocultación ya que nadie desvela las armas informáticas que tiene porque revelarlas concedería al enemigo una ventaja y la posibilidad de diseñar formas de contrarrestarlas. También es muy difícil identificar en ella un *casus belli*, determinando fehacientemente de donde viene la amenaza y por lo tanto es necesario defender todos y cada uno de los puntos vulnerables porque no se sabe cuál de ellos decidirá explotar el enemigo.

Esta investigación pretende contribuir al campo disciplinar nuevos enfoques en relación a la ciberdefensa, ya que aportará una nueva perspectiva a como conceptualizar y definir en el nivel operacional las características de la misma y a su vez se espera que abra nuevas líneas de investigación sobre esta problemática.

La seguridad del ciberespacio es de incumbencia estratégica nacional, pero el alcance de esta investigación está enmarcado en el ámbito militar exclusivamente y en aquellos aspectos que se relacionan al desempeño del IM dentro de un TO, por lo que también se hará necesario analizar algunas cuestiones del Nivel Táctico. Por lo tanto se limitará a la esfera castrense y no abordará la ciberdefensa en sus dimensiones políticas, sociales, económicas y legales.

---

* Asesor Especial del Presidente sobre ciberseguridad en el gobierno de Bush se centró en la seguridad cibernética y la amenaza del terrorismo contra la infraestructura crítica de los Estados Unidos. Autor de Cyber War: The Next Threat to National Security and What to Do About It en 2010 y de How China Steals Our Secrets en 2012.

[3] Diginota; "China, EEUU y Rusia en guerra cibernética, según McAfee"; *Diginota*; Publicado el 11 de abril de 2012; Recuperado el 22 de julio de 2015 de http://www.diginota.com/china-eeuu-y-rusia-en-guerra-cibernetica-segun-mcafee/

Por lo expuesto el problema que se ha formulado para esta investigación es: ¿Cómo se puede combatir las amenazas cibernéticas que afectan a la infraestructura críticas de un teatro de operaciones contemporáneo?

Se planteó como Objetivo General el de establecer una manera de proceder que permita limitar las acciones nocivas y las amenazas cibernéticas que puedan afectar alguna estructura crítica del estado, y las capacidades del Instrumento Militar (IM) dentro de un teatro de operaciones (TO) contemporáneo. Para ello se debe primeramente identificar las amenazas en el entorno cibernético que pueda explotar alguna vulnerabilidad en las estructuras consideradas críticas; y analizar y seleccionar la mejor alternativa para hacerles frente de manera oportuna y eficaz.

Se intentará verifica la Hipótesis siguiente: si se establece una manera de proceder adecuada en el ámbito de la ciberdefensa se podrá limitar las acciones nocivas y las amenazas cibernéticas que puedan afectar alguna estructura crítica del estado, y las capacidades del IM dentro de un TO.

La Metodología a emplear será descriptiva analizando fuentes primarias y secundarias, documentos que se relacionen con el tema, páginas en internet y detallando la problemática tal como la estudiaron las naciones más desarrolladas y las soluciones por estas encontradas.

Este trabajo está estructurado en tres capítulos. En el primero se analizan los aspectos normativos relacionados con la ciberdefensa, tanto en el marco nacional como el mundial. En el segundo capítulo se estudian las diversas amenazas al IM, mediante ejemplos de casos históricos recientemente perpetrados tanto a gobiernos como a grandes compañías que han encontrado formas para combatirlas. El tercer capítulo propone una posible organización del entorno cibernético para que pueda ser utilizado convenientemente en beneficio propio y a su vez sea asegurado de la acción enemiga en el nivel operacional y que de esta manera contribuya al logro de los objetivos perseguidos por el Comandante del TO.

Capítulo I: Ciberespacio y su marco legal en los conflictos armados

Derecho Internacional respecto a la Ciberdefensa

En mayo de 2011, la Casa Blanca emitió la Estrategia Internacional para el Ciberespacio, en la que señaló que *el desarrollo de normas para la conducta del Estado en el ciberespacio no requiere una reinvención del derecho internacional consuetudinario,* ni *hacen obsoletas las normas internacionales existentes*[4]. Esto significa entonces que las *normas internacionales de larga data rectoras* del *comportamiento* de los *estados, tanto para tiempos de paz como de conflicto, también se aplica en el ciberespacio*[5].

Sin embargo, como *no existen disposiciones de tratados que tengan que ver directamente con la guerra cibernética*[6], resulta evidente que se requiere normar específicamente la aplicación de estas políticas y que muchas veces puede resultar necesario complementar las normas existentes. En tal sentido, el Manual de Tallin sobre el Derecho Internacional aplicable a las Ciberguerras, explora el mejor modo de aplicar las normas existentes de derecho internacional al nuevo escenario de la guerra, y presenta reglas que deben regir las prácticas de guerra en el ciberespacio y que se ocupan de los detalles técnicos que permitan traducir la ley al nivel, abordando *temas como la soberanía, la responsabilidad de los estados, el "jus ad bellum", el "jus in bello"*, el derecho humanitario internacional y la ley de neutralidad, entre otros*.[7]

El profesional de armas debe asegurarse de que todos sus actos y los de sus subordinados se encuadren dentro de lo que prescribe el Derecho Internacional de los

---

[4] "The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"; sitio oficial *The White House*; Publicado en mayo de 2011. p.9. Disponible en http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[5] The White House, ibid. p.9.

[6] Michael N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", *Cambridge University Press*; Edición: Reimpreso, 7 de marzo de 2013. p.19

* El *jus ad bellum* es el derecho sobre el empleo de la fuerza y procura limitar el recurso a la fuerza entre Estados, mientras que el *jus in bello* es el derecho en la guerra y sus disposiciones se aplican a las partes beligerantes independientemente de las razones del conflicto o de la justicia o la injusticia de las causas que defiende cada parte. *Comité Internacional de la Cruz Roja*. Publicado el 29 de octubre de 2010. Recuperado el 19 de septiembre de 2015 de https://www.icrc.org/spa/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm

[7] Publicación del Manual de Tallín sobre "Ley Internacional en la Ciberguerra", *Portal de Tecnología e Innovación del Ministerio de Defensa*. Publicado el 22 de marzo de 2013. Recuperado el 9 de septiembre de 2015 de http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59

Conflictos Armados (DICA) y haciendo uso de manual antes mencionado, de los criterios establecidos por los Convenios de Ginebra del 12 de agosto de 1949 y sus Protocolos Adicionales del Comité Internacional de la Cruz Roja (CICR), se procede a analizar algunos puntos principales del confuso escenario legal en el que puede circunscribirse el ciber espacio y los actos de agresión que en él se lleven a cabo.

Por lo tanto, se inicia este análisis con definición taxativa del término *ataque* ya que es de importancia central para el DICA y las normas internacionales que reglamentan el *jus in bello*. Se entiende por *ataques a los actos de violencia contra el adversario, sean ofensivos o defensivos*[8]. Sin embargo, existen diferentes puntos de vista con referencia específica a las operaciones militares de lo que constituye un *ataque* ejecutado a través del ciberespacio. El Manual de Tallin proporciona una definición de ciberataque en su Regla 30, estableciendo que un ataque cibernético es *una operación cibernética*, ya sea *ofensiva o defensiva*, de la *que razonablemente se espera causar lesiones o muerte a personas; o daños o destrucción de objetos*.[9]

Algunos expertos opinan que dicha definición es deficiente por las particularidades del ámbito cibernético y debería ser actualizada con el agregado del efecto de *neutralización*, en el sentido de deterioro sustancial *de funcionalidad* sin que se produzca el daño permanente[10] ni necesite reparación. Entonces, la definición más adecuada y actualizada de ciberataque expresa que es la suma de *acciones que combinan ataques a la red informática con otras capacidades facilitadoras (como ataque electrónico, ataque físico u otro) para negar o manipular la información y / o infraestructura* o también se puede definir como u*n ataque, a través del ciberespacio,* apuntando *el uso* […] *del ciberespacio con el propósito de interrumpir, deshabilitar, destruir o controlar malintencionadamente un entorno informático / infraestructura o de la destrucción de la integridad de los datos o el robo de información controlada*. [11]

[8] Protocolo Adicional I a los Convenios de Ginebra del 12 de agosto de 1949. artículo 49: Definición de ataques y ámbito de aplicación (1)
[9] Schmitt; *op. cit.*; p.92
[10] Michael J. Norris; "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace". *Student Pulse*. Publicado en 2013. Recuperado el 10 de septiembre de 2015 de http://www.studentpulse.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace
[11] "Cyberattack, Definitions"; *IT Law Wiki*; Publicado el 1 de febrero de 2001; Recuperado el 18 de junio de 2015 de: http://itlaw.wikia.com/wiki/Cyberattack

Dentro del DICA, un ataque se considerará legal solo si cumple con las cuatro condiciones acumulativas siguientes:

a. *El objetivo debe ser un "objetivo militar".*
b. *Los "medios" y "métodos" empleados para atacar el objetivo deben ser legales.*
c. *El atacante debe tomar precauciones específicas.*
d. *El ataque no debe causar daños excesivos a civiles o bienes de carácter civil en relación con el objetivo militar concreto y directo previsto.*[12]

Principio de Distinción en Ciberdefensa

El Principio de Distinción establece que: *A fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las Partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares*[13].

En el Protocolo adicional I (PAI) se estipula explícitamente que es *persona civil cualquiera que no pertenezca a una de las categorías (…)* de combatientes. *En caso de duda acerca de la condición de una persona, se la considerará como civil* [14], mientras que son *bienes de carácter civil todos los bienes que no son objetivos militares*[15].

El PAI también establece que se considera que *los miembros de las fuerzas armadas de una Parte en conflicto (salvo aquellos que formen parte del personal sanitario y religioso a que se refiere el artículo 33 del III Convenio) son combatientes*.[16] Mientras que los objetivos militares se limitan a aquellos *objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida*."[17]

Por lo general no resulta sencillo determinar qué entidades se consideran objetivos militares y muchas veces esto depende de la interpretación de quienes tienen

[12] Michael N. Schmitt, "Essays on Law and War at the Fault Lines"; *Asser Press;* 2012. p.176.
[13] Protocolo adicional I; *op. cit.*; art 48
[14] Protocolo adicional I; *op. cit.*; art. 50 (1)
[15] Protocolo adicional I; *op. cit.*; art. 52 (1).
[16] Protocolo adicional I; *op. cit.*; art. 43 (2)
[17] Protocolo adicional I; *op. cit.*; art. 52 (2)

que decidir si realizar un ataque o no. *El problema reside en establecer el nexo requerido entre el objeto que se proyecta atacar y las operaciones militares.*[18]

La interpretación de la norma presenta un problema que tiene su origen en las frases "*contribuyan eficazmente a la acción militar*" y "u*na ventaja militar definida*" contenidas en la definición de objetivos militares. Para algunos, la primera solo abarca los objetos "directamente utilizados por las fuerzas armadas" (por ejemplo, armas y equipos militares), una ubicación de "importancia particular para las operaciones militares" (por ejemplo puentes), y los objetos concebidos para emplearse o que se emplean para fines militares[19]. En cuanto a la segunda expresión se excluyen los ataques que sólo ofrecen ventajas "indeterminadas o eventuales"[20].

Ciertos actores internacionales, como EEUU, tienen una interpretación bastante amplia de la misma norma por lo que consideran lícito incluir objetivos que en forma indirecta, pero efectivamente, apoyan y sostienen la capacidad de guerra del enemigo[21], por lo tanto, objetivos que para ciertos estados, entre los que se encuentra Argentina, están claramente protegidos por el derecho internacional, para otros se encuentran comprendidos dentro de los objetivos lícitos, ejemplos de ellos serían los elementos del sistema económico, político, tecnológico y psicosocial de un potencial enemigo.

Determinar si el ciberataque causaría o no muertos, heridos o destrucción es importante ya que si solamente provoca inconvenientes sin daños físicos o heridos, ésta no alcanzaría el nivel de un ataque según su connotación tradicional y estaría entonces permitida, *independientemente del nexo, o de la falta de nexo, entre el objetivo y las operaciones militares*[22]. Un hecho histórico que ejemplifica el punto anterior lo constituye el ataque a la estación de la televisión estatal serbia en Belgrado realizado en 1999 por la OTAN con armas cinéticas, ya que es de suponer que si se hubiera ejecutado un ataque de denegación de servicios y prescindido de esta manera daños materiales y personales probablemente las críticas se habrían evitado o minimizado.

---

[18] Schmitt; *op. cit.*.
[19] Yves Sandoz, Christophe Swinarski y Bruno Zimmermann; "Comentario del Protocolo adicional I de los Convenios de Ginebra del 12 de agosto de 1949", *CICR*, Plaza y Janés Editores, Bogotá, tomo II, párr. 2020-23.
[20] Sandoz, Swinarski y Zimmermann; *ibíd*.; tomo II, párr. 2024.
[21] "The Commander's Handbook on the Law of Naval Operations (NWP 1-14M, MCWP 5-2.1, COMDTPUB P5800.7)"; *Marina de EEUU/ Infantería de Marina/ Servicio de Guardacostas;* 1995, párr. 8.1.1.
[22] Schmitt; *op. cit.*.

También existen diferentes criterios para distinguir si el ataque a un civil es lícito o no, ya que el PAI permite esta posibilidad sólo cuando civiles *participan directamente en las hostilidades y mientras dure tal participación*[23]. Hay quienes limitarían aún más la inmunidad de los civiles contra los ataques, considerando a las personas civiles que trabajan, por ejemplo, en una base militar durante las hostilidades como objetivos legítimos, aunque no participen directamente en actos de guerra[24].

En Ciberdefensa el problema de las personas y los bienes de carácter civil es muy complejo. *Algunos países han optado por subcontratar funciones de guerra de la información, sean esas funciones el mantenimiento de bienes o la conducción de operaciones,* [o delegarlas] *a organismos del Gobierno (…) no militares*[25].

Bienes de uso dual en Ciberdefensa

Los bienes de uso dual son los *productos y tecnologías utilizadas normalmente para fines civiles pero que pueden tener aplicaciones militares* [26], entre ellos se encuentran por ejemplo, puertos, aeropuertos, vías férreas, sistemas de producción y suministro eléctricos, sistemas de comunicación, ciertas fábricas, satélites, etc. Si un bien se emplea con fines militares, incluso si estos son secundarios respecto de los fines civiles, se convierte en *un objetivo militar susceptible de sufrir ataques, incluidos los ataques a través de redes informáticas*.[27]

Cabe aclarar que un bien dual puede no ser un objetivo militar por no cumplir función militar alguna en determinado conflicto; también pude pasar a serlo si, aunque se esté usando solamente en su función civil, potencialmente existe una probabilidad razonable e inminente de que se use con fines militares dentro del conflicto en desarrollo.

[23]Protocolo adicional I; *op. cit.*; art. 51 (3)
[24] "Carta de DAJAIA al Consejero para la Investigación y la Ingeniería en Defensa (Economía), Embajada de la República Federal de Alemania (22 de enero de 1988)"; citada en W.H. Parks, "Air War and the Law of War", *Air Force Law Review* , vol. 32, 1992, p. 1.
[25] Schmitt; *op. cit.*, pág. 4.
[26]"Trade Topics, Dual Use"; *European Commission*; Actualizado el 15 de Julio de 2015. Recuperado el 11 de septiembre de 2015 de http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm
[27] Schmitt; *op. Cit.*

Marco Legal en Argentina

Lo primero que se debe tener en cuenta al analizar el ámbito legal en la República Argentina es que la misma estableció una clara diferenciación conceptual entre Defensa Nacional y Seguridad Interior, delimitando el ámbito de incumbencia de cada uno de ellos a través de las leyes 23554 de Defensa Nacional y 24059 de Seguridad Interior y del Decreto 727/2006, que reglamentó la Ley de Defensa Nacional. De estas leyes se desprende que la Defensa Nacional tiene por finalidad la de *conjurar agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro u otros Estados*[28], mientras que la Seguridad Interior es la responsable de *la prevención y persecución de delitos contenidos en el Código Penal y otras leyes especiales*.[29]

Esta diferenciación taxativa se diluye cuando se trata la jurisdicción del espacio cibernético por sus características particulares. *La diferente naturaleza de las esferas de la Seguridad Interior y la Defensa Nacional, no debe desconocer que la mayoría de los Estados reconocen áreas de complementariedad entre ambos sistemas*.[30] También cabe observar que diferentes países, producto de sus propias idiosincrasias han arribado a diversos ordenamientos jurídicos en el ámbito cibernético para incorporar esta complementariedad, sin perder de vista que la misma provoca el empleo del Instrumento Militar (IM) en funciones cuya naturaleza corresponde a la jurisdicción de la Seguridad Interior en mayor o menor medida.

Desde mediados de la primera década de este siglo Argentina ha realizado numerosos esfuerzos para robustecer su seguridad de la información y ciberdefensa; el IM ha acompañado este proceso y como muestra de ello el Ministerio de Defensa ha promulgado una serie de normas legales, siendo la inicial la Resolución N° 364 del año 2006 en la que se crea el Comité de Seguridad de la Información en el ámbito del Ministerio de Defensa, siendo una de las ultimas la Decisión Administrativa 15/2015 de marzo de este mismo año, por la cual se crea la Dirección General de Ciberdefensa.

En vista a lo expresado anteriormente se debe profundizar dicho proceso para adecuarse al contexto de nuevas amenazas, generando una mayor y mejor interrelación

[28] Decreto 727/2006 Reglamentación de la Ley Nº 23554.
[29] Decreto 1273/92 Reglamentación de la Ley Nº 24059.
[30] Sol Gastaldi, Candela Justribó, La seguridad y la defensa en el ámbito ciberespacial. Informe de investigación, Desarrollo Estratégico Nacional en Escuela de Defensa Nacional (EDENA), octubre de 2014. p.6.

entre las distintas Instituciones del Estado, especialmente sus Fuerzas Armadas, y las agencias privadas que por su naturaleza impliquen un riesgo en la seguridad del país, siendo especialmente complejo este aspecto al nivel operacional, pero fundamental para poder estructurar un posible Teatro de Operaciones de manera eficaz y eficiente.

En la aceptación de que el mundo se encuentra crecientemente interrelacionado e interdependiente, con el Decreto 1714 / 2009, Argentina *concibe su defensa en la doble dimensión "autónoma" por un lado, y "cooperativa" por otro, (...) tanto de nivel subregional, regional y también global.*[31]

Un avance en este sentido lo constituye el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), creado en el año 2011, que *tiene como finalidad impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.*[32] Con el mismo propósito la Resolución MD N° 385/2013 conforma la Unidad de Coordinación de Ciberdefensa que busca *generar mecanismos integrados de respuesta para la toma de decisiones*[33].

En 2014, con la Resolución N° 350, se instruye al Jefe del Estado Mayor Conjunto de las Fuerzas Armadas *que disponga las medidas necesarias a los efectos de desarrollar capacidades militares para realizar operaciones de ciberdefensa, a los efectos de únicamente garantizar la defensa contra aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal*[34] y contra aquellos ciberataques *que dirigidos a afectar los objetivos de valor estratégico que el Ministerio de Defensa establezca*

[31] Decreto 1714/2009; Ministerio de Defensa; Directiva de Política de Defensa Nacional
[32] "Qué hacemos"; *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*. Actualizado el 15 de Julio de 2015. Recuperado el 11 de septiembre de 2015 de http://www.icic.gob.ar/
[33] Candela Justribó, Ciberdefensa: Una visión desde la UNASUR, VII Congreso del Instituto de Relaciones Internacionales, La Plata, 26, 27 y 28 de noviembre de 2014. p.9.
[34] Resolución MD N° 350/2014

expresamente[35], incorporándose de esta manera al IM como integrante de la estrategia de defensa cibernética nacional.

Resulta evidente que las leyes del país, al tener un enfoque netamente defensivo, restringen el accionar en las actividades de ciberdefensa, en especial si se compara con la misión del Cibercomando de EEUU (USCYBERCOM) que está preparado para *realizar operaciones militares en el espectro que abarca el ciberespacio a fin de posibilitar las acciones en todos los dominios (aire, mar, tierra y espacio) de EE.UU. / Aliados y asegurar la libertad de acción en el ciberespacio y negar la misma a nuestros adversarios*[36].

En 2013, en el ámbito de la Unión de Naciones Suramericanas (UNASUR) y como parte de la Política de Defensa Argentina de avanzar en la conformación de un sistema de defensa subregional integrado dentro del cual está obviamente incluida la defensa cibernética, se suscribió la Declaración de Buenos Aires entre Argentina y Brasil promoviendo la cooperación en ciberdefensa de donde surge el Equipo de Respuesta ante Emergencias Informáticas *(CERT, del inglés Computer Emergency Response Team)* para incrementar la seguridad cibernética de estos países.

Se puede afirmar finalmente que la normativa de la República Argentina está enfocada en preservar su Sistema de Defensa Nacional, protegiendo para ello los sistemas de comando, control, comunicaciones, informática y guerra electrónica, entre otros, de las Fuerzas Armadas, ante cualquier acto disruptivo cibernético originado en una agresión estatal militar externa que pudiera afectar el desarrollo de las operaciones militares.

Es poco realista intentar compartimentar el ciberespacio, ya que no conoce de fronteras terrestres, marinas o aeroespaciales ni discierne entre el ámbito civil del militar, por lo que debe ser tratado como un ente único. También debe notarse que es peligroso ceder la iniciativa al enemigo ya que tener una actitud netamente defensiva se traduce en un esfuerzo colosal al tener que defender todos los puntos vulnerables de ser atacados en todo momento, mientras que el agresor para concentrar sus energías en un punto único en el momento que él lo decida.

---

[35] Resolución MD N° 350/2014

[36] Peter W. Singer y Allan Friedman; "Cybersecurity and Cyberwar, what everyone needs to know"; *Oxford University Press;* New York; 2014; p.133.

Capítulo II: Amenazas Cibernéticas

Incremento de los Ciber-arsenales

Debido a que el control del ciberespacio tiene gran implicancia en el balance de poder relativo entre naciones, las principales potencias a nivel mundial han destinado cuantiosos recursos para lograr obtener posiciones de privilegio en el ámbito cibernético, por ello se afirma que *Washington y Teherán están aumentando sus ciber-arsenales, construidos en el mercado negro de armas digitales, enredando a gigantes de alta tecnología como Microsoft, Google y Apple, con la ayuda de fuentes gubernamentales de alto rango y del sector privado*[37].

Esta nueva manera de hacer la guerra provoca que *países medianamente desarrollados se esfuercen por adquirir las capacidades necesarias en Guerra Cibernética, para lograr un importante reposicionamiento en el contexto global*[38], pero a diferencia de lo que sucediera en la carrera armamentista nuclear, esta carrera se desarrolla de forma subrepticia.

El espectro de las amenazas cibernéticas es ilimitado[39], siendo algunas de ellas más peligrosas y sofisticadas que otras, y no todas ellas son de relevancia en el ámbito militar y es aún más acotada la lista de las que tienen aplicación en el nivel operacional.

En este gran espectro encontramos *malwares* (software utilizado para interrumpir el funcionamiento de un ordenador, recopilar información sensible, o tener acceso a los sistemas informáticos privados [40]), ataques e intrusiones de redes, accesos no autorizados, ingeniería social, distribución ilícita, actividad de agentes internos,

---

[37] Michael Joseph Gross; "Silent War"; *VF News*; Publicado en julio de 2013. Recuperado el 17 de Septiembre de 2015 de *http://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business*

[38] Roberto Uzal; "Guerra Cibernética: ¿un desafío para la Defensa Nacional?"; Revista *Visión Conjunta* Número 7. Año 4 Número 7, 2012 (versión electrónica) p. 40; Recuperado el 17 de Septiembre de 2015 de: *http://esgcffaa.mil.ar/numero7/40.html*

[39] "Amenazas cibernéticas"; *Federal Emergency Management Agency (FEMA)*;s.f.*;* Recuperado el 17 de Septiembre de 2015 de *http://m.fema.gov/es/cyber-attack*

[40] SurfWatch; "Cyber Risk Intelligence"; *SurfWatch, Ciber in Sight*; s.f.*;* Recuperado el 17 de Septiembre de 2015 de *https://www.surfwatchlabs.com/threat-categories#Practice*

* Proviene de la voz inglesa *Hackear* y se refiere a la acción de explorar y buscar las limitantes de un código o de una máquina. El término hackear también significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.Tomado de TECHNICALLY SPEAKING; McFedries, P.; Spectrum, IEEE Volume 41, Issue 2, Feb. 2004 Page(s):80 10.1109/MSPEC.2004.

espionaje, explotación de vulnerabilidades de software, operaciones de hackeo*, intervención e imposición de la ley[41], entre otros (conceptos desarrollados en Anexo 1).

Para entender la complejidad de esta clasificación obsérvese que los *malwares***,** incluyen subcategorías como Virus y Gusanos, Backdoor o Puerta Trasera, Drive-by Downloads, Rootkits, Troyanos, Hijackers, Keyloggers y Stealers, Botnets, Rogue software y los Ransomware, criptovirus o secuestradores.[42] (Conceptos desarrollados en Anexo 2)

Objetivos de los Ciberataques

Durante la aun breve historia de los sistemas de información se pueden encontrar algunos eventos que constituyen puntos de referencia que han servido como casos de estudio para impedir una nueva ocurrencia de dicho suceso. Todos ellos tienen como denominador común que persiguen uno o varios de los siguientes objetivos:

1. *Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo.*
2. *Interrumpir o romper el flujo de la información.*
3. *Destruir físicamente la información del adversario.*
4. *Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información.*
5. *Impedir al adversario acceder y utilizar los sistemas y servicios críticos.*
6. *Engañar a los adversarios.*
7. *Lograr acceder a los sistemas del enemigo y robarles información.*
8. *Proteger sus sistemas y restaurar los sistemas atacados.*
9. *Responder rápidamente a los ataques o invasiones del adversario.*[43]

No todos los ataques cibernéticos son de interés del Instrumento Militar, ya que *una buena parte de los ciberataques registrados en los últimos años han sido obra de piratas informáticos con ánimo de lucro, afán de protagonismo o con motivaciones*

[41] Cyber Risk Intelligence; *op. cit.*
[42] "Tipos de ataques informáticos"; *Core One Information Technology;* s.f.; Recuperado el 17 de Septiembre de 2015 de http://www.coreoneit.com/tipos-de-ataques-informaticos/
[43] Gema Sánchez Medero; "Los Estados y la Ciberguerra"; *Universidad Complutense de Madrid;* 2010; p. 64.

políticas[44], pero también se han producido otros que si resultan de interés para las Fuerzas Armadas, aunque sea en parte, ya que *han sido obra de los servicios de seguridad nacionales*[45] o han afectado la seguridad de un estado.

Los atacantes cibernéticos tienen diferentes perfiles que varian desde profesionales con un nivel de cualificación medio, que puede ocasionar una interrupción temporal de servicios informáticos, hasta actores estatales con capacidad de afectar la infraestructura crítica de un país enemigo, llegando incluso a provocar efectos geopolíticos.[46]

Ciberataques con Objetivos Económicos

El plano económico es en el que más ciber ataques se han producido porque el lucro monetario es un gran motivador, encontrándose muchos ejemplos como el caso de Vladimir Levin, quien en 1995 fue arrestado declarándose culpable de haber ingresado a la red del Citibank desde donde realizó al menos 40 transferencias por un valor superior a los diez millones de dólares.[47]

Más recientemente, en 2013, un grupo de ciber delincuentes robó al menos 300 millones de dólares, aunque Kaspersky Lab, compañía especializada en seguridad de sistemas de información de renombre mundial, admite que esta cifra podría ser tres veces superior, a varios bancos e instituciones financieras de todo el mundo, especialmente de Rusia, Japón, EEUU y Europa Occidental, utilizando software malicioso, en lo que podría ser uno de los mayores robos a bancos de la historia. [48]

Según TICbeat, publicación digital independiente especializada en tecnología e innovación, el 67% de las empresas de Europa experimentó una brecha de seguridad el

[44] Lino González Veiguela, Los ciberataques (conocidos) más importantes, EsGlobal.com. Publicado el 02 de julio de 2013. Recuperado el 17 de Septiembre de 2015 de *http://www.esglobal.org/la-lista-los-ciberataques-conocidos-mas-importantes/*
[45] Veiguela; *ibíd.*
[46] Guillem Colom Piella, José Ramón Coz Fernández, Enrique Fojón Chamorro y Adolfo Hernández Lorente; "Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales"; ARI 26/2013; *Real Instituto Elcano*; 4 de julio de 2013; Tabla de p.3.
[47] Amy Harmon; "Hacking Theft of $10 Million From Citibank Revealed"; *Los Angeles Times*; Publicado el 19 de Agosto de 1995; Recuperado el 23 de septiembre de 2015 de: *http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system*
[48] Juan Miguel Revilla; "Un grupo de hackers robó 300 millones de dólares a varios bancos"; *ITespresso*; Publicado el 16 de febrero de 2015; Recuperado el 20 de Septiembre de 2015 de: *http://www.itespresso.es/hackers-robo-300-millones-dolares-bancos-134021.html*

último año y el 100% ha sido atacada en algún momento del pasado. También afirma que el coste de uno de estos ataques es cada vez más alto, siendo el gasto directo medio para una compañía de 75.000 euros, sin tener en cuenta la pérdida de negocio y reputación, aspectos que *hacen incrementar esta suma de forma exponencial y que en muchos casos es incluso imposible de calcular*.[49]

Ciberataques con Objetivos Psicosociales

Con referencia al manejo de la opinión pública, en 1999, se han producido una serie de ciberataques como el ejecutado durante el conflicto bélico en la provincia serbia de Kosovo, del que se señaló que estaba transformando al ciberespacio en "*una zona etérea de combate donde la batalla por las mentes y los corazones es peleada a través del uso de imágenes, listas de discusión y ataques de hackers*"[50]. Durante el mismo conflicto el slogan "Down with barbarians" fue colocado en chino en la página de la embajada estadounidense en Pekín después que la OTAN accidentalmente bombardeara la embajada de China en Belgrado, mostrando también imágenes de los tres periodistas muertos en dicho ataque, de las protestas en Pekín y una bandera china flameando en el sitio del Departamento del Interior.[51]

En abril de 2001, durante los días de tensión por la retención de la aeronave norteamericana y su tripulación, posteriores a la colisión de un avión estadounidense de reconocimiento y un caza chino en la que falleció el piloto asiático, fueron atacados varios sitios web norteamericanos, donde se publicaron condenas en contra de ese país, su política imperialista y elogios al piloto fallecido. El grupo, "Hackers Union of China" se adjudicó el ataque de por lo menos 10 sitios[52]; como respuesta el grupo de hackers estadounidenses PoizonBOx atacó a por lo menos un centenar de sitios chinos[53].

---

[49] Alberto Iglesias Fraga; "El 67% de las empresas europeas sufrió un ciberataque en 2014"; *TICbeat*; Publicado el 23 de septiembre de 2015; Recuperado el 23 de septiembre de 2015 de: *http://www.ticbeat.com/seguridad/el-67-de-las-empresas-europeas-sufrio-ciberataque-en-2014/*

[50] Ashley Dunn; "Crisis in Yugoslavia: Battle Spilling Over Onto the Internet"; *Los Angeles Times*, Publicado el 3 de abril de 1999; Recuperado el 20 de Septiembre de 2015 de: *http://articles.latimes.com/1999/apr/03/news/mn-23851*

[51] Sebastián Masana; "El ciberterrorismo: ¿una amenaza real para la paz mundial?"; Tesis de maestría *Facultad Latinoamericana de Ciencias Sociales*, 8 de julio de 2002; p. 26.

[52] Masana; *ibíd*.; p. 28.

[53] Michelle Delio; "Crackers Expand Private War"; *Wired News*; Publicado el 18 de abril de 2001. Recuperado el 20 de Septiembre de 2015 de: *http://www.wired.com/news/politics/0,1283,43134,00.html*

En 2008 las bases de datos de las campañas presidenciales de los EEUU, tanto republicanos como demócratas fueron hackeadas y descargadas por intrusos extranjeros desconocidos.[54]

En enero de 2010 un grupo llamado Ejército Cibernético Iraní interrumpió el servicio del popular motor de búsqueda chino *Baidu* y los usuarios fueron redirigidos a una página que mostraba un mensaje político iraní. El mismo Ejército Cibernético Iraní había hackeado *Twitter* en diciembre del año anterior, con un mensaje similar. [55]

Ciberataques con Objetivos Políticos

En la primavera de 2007, después de que Rusia presionara a Estonia por la retirada de un monumento de la época soviética de las calles de Tallín, varias páginas oficiales del Gobierno estonio quedaron paralizadas por ataques informáticos provenientes del exterior y los sistemas de algunos bancos y periódicos resultaron bloqueados durante varias horas por una serie de ataques de Denegación de Servicio Distribuidos*. El Kremlin negó toda implicación.[56]

En agosto del 2008, días antes del inicio del breve conflicto bélico entre Georgia y la Federación Rusa por el control de Osetia del Sur, medios de comunicación y páginas webs de instituciones de Georgia y Azerbaiyán sufrieron ataques cibernéticos que impidieron su normal funcionamiento. Una fotografía alterada del presidente, Mikheil Saakashvili, caracterizado como Hitler fue publicada en la página del Ministerio de Asuntos Exteriores georgiano antes de bloquear su funcionamiento. El Kremlin nuevamente negó que los servicios secretos rusos estuviesen implicados en dichos ataques.[57]

En 2007, las primeras versiones de gusanos informáticos muy resistentes, sofisticados, y nocivos, diseñados para el sabotaje físico de maquinaria, comenzaron a infectar ordenadores en varios países, principalmente en Irán. El Virus Stuxnet,

[54] NATO Review; "Cyber - the good, the bad and the bug-free, The history of cyber attacks - a timeline"; *NATO Review;* s.f.; Recuperado el 28 de mayo de 2015, de: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

[55] NATO Review; *ibid*.

* Del inglés "Distributed Denial Of Service" (DDoS) es un intento de hacer inasequible un servicio en línea por abrumadora con el tráfico de múltiples fuentes. Recuperado el 20 de Septiembre de 2015 de: http://www.digitalattackmap.com/understanding-ddos/

[56] Medero; *op. cit.*, p. 73.

[57] Veiguela; *op. cit*.

adjudicado a los EEUU e Israel, fue la primer ciber-arma conocida en causar daño físico significativo a su objetivo al haber destruido las centrifugadoras de enriquecimiento de uranio en las instalaciones nucleares de Irán en Natanz. Jason Healey, quien dirige la Iniciativa Política Cibernética por el Consejo del Atlántico, sostiene que Stuxnet fue "*la primera arma autónoma con un algoritmo, no una mano humana, encargado apretar el gatillo*."[58] Para los EEUU, Stuxnet fue por un lado una victoria, ya que constituye una capacidad temible y eficaz, y por el otro lado una derrota, porque el hecho se hizo público y esto constituye un problema en la Ciberdefensa.

Ciberataques con Objetivos Militares

Investigaciones han establecido que un ataque ahora conocido como *Moonlight Maze* tuvo lugar entre 1998 y 2000 cuando intrusos informáticos tuvieron acceso a miles de documentos clasificados, muchos de ellos relacionados con información del Ejército de EEUU, entre otros mapas de instalaciones militares y planes de despliegue de tropas. En este hecho también fueron afectados los sistemas informáticos del Pentágono, la Administración Nacional de la Aeronáutica y del Espacio, más conocida como *NASA*, el Departamento de Energía estadounidense y universidades privadas de EEUU. Aunque se rastreó la procedencia del sofisticado asalto hasta conexiones ubicadas en Rusia, las autoridades de ese país, como suele suceder en este tipo de actividades, negaron estar implicadas y aun no se ha podido probar quiénes fueron los autores materiales ni los eventuales patrocinadores del ataque, recayendo las sospechas sobre las agencias de espionaje estatales.[59]

El mejor ejemplo del uso del ciberespacio con propósitos militares de materializó en 2007, cuando Israel realizó un ataque aéreo contra instalaciones nucleares de Siria en lo que se conoció como operación Huerto. Para superar las defensas antiaéreas sirias se utilizó un elemento de ciberguerra, el programa informático estadounidense denominado Suter, que permite interceptar y bloquear las comunicaciones enemigas, en este caso específico, las que forman un sistema de radares antiaéreos. *La operación Huerto habría*

[58] Michael N. Schmitt; "La guerra de la información: los ataques por vía informática y el jus in bello"; *Comité Internacional de la Cruz Roja*. Publicado el 30 de junio de 2002. Recuperado el 31 de Agosto de 2015 de http://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business
[59] Veiguela; *op. cit.*

supuesto una combinación entre armas de guerra tradicionales y armas de guerra cibernética que ofrece sinergias aún poco exploradas.[60]

La Operación Huerto de Israel, explicada con anterioridad, ha servido de incentivo para realizar esfuerzos más profundos en el campo de la ciberdefensa. EEUU, por ejemplo, desarrolla el "Plan X", un programa de $ 110 millones diseñado para "*ayudar a los responsables de la planificación de la guerra a montar y lanzar rápidamente asaltos online y hacer de los ataques cibernéticos una parte más rutinaria de las operaciones militares*"[61], esto le permitirá contar con estrategias y herramientas para realizar acciones de ciberguerra dentro de cualquier operación militar que lleve a cabo contra sus enemigos.[62]

En la guerra cibernética es poco probable que las ciber armas sean utilizadas por su cuenta. En su lugar, se prevé que apoyaran ataques convencionales, cegando a un enemigo antes de un inminente ataque aéreo, por ejemplo, o desactivando el sistema de comunicaciones del enemigo durante la batalla.[63] La parte más compleja e importante de la guerra cibernética es el despliegue de las armas digitales propias, incluso antes de que haya comenzado la batalla, infiltrando las redes del enemigo para recopilar información y sentar las bases para una acción potencialmente más agresiva.[64]

A diferencia de espionaje, los ataques cibernéticos militares estarán encaminados a la consecución de un efecto físico y probablemente el Comando Cibernético de Estados Unidos será el responsable de llevarlos a cabo.[65] Con un presupuesto cibernética de 1.540 millones de dólares desde el 2013 al 2017, la agencia Agencia de Proyectos de Investigación Avanzados de Defensa (*DARPA**) se centrará cada vez más en la ofensiva cibernética para satisfacer las necesidades militares.[66]

---

[60] Veiguela; *op. cit.*
[61] Singer; *op. cit.;* p. 128.
[62] Russia Today; "Guerra virtual: EE.UU. dominará el campo de batalla cibernético con su secreto 'Plan X'", *RT Sepa Más*, Publicado el 23 de agosto de 2012. Recuperado el 22 de septiembre de 2015 de: *http://actualidad.rt.com/actualidad/view/52072-guerra-bestia-darpa-dominara-campo-batalla-cibernetica-secreto-plan-x*
[63] Ellen Nakashima; "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace"; *The Washington Post*. Publicado el 30 de Mayo de 2012. Recuperado el 22 de septiembre de 2015 de: *https://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html*
[64] Singer y Friedman; *op. cit.*
[65] Nakashima; *ibíd.*
* Del inglés: Defense Advanced Research Projects Agency

La reconocida compañía de seguridad en sistemas de información Kaspersky Lab ha dado a conocer este año una ciber-arma que supera todo lo conocido en términos de complejidad y sofisticación de las técnicas de ciberespionaje, es un malware denominado *Equation Group*, que lleva activo casi dos décadas, y es único en casi todos sus aspectos. Esta ciber-arma se caracteriza por un extremo nivel de persistencia que lo ayuda a sobrevivir al formateo del disco y la reinstalación del sistema operativo y es imposible de detectar. Además emplea una vasta infraestructura alojada en varios países. Desde 2001, ha infectado a decenas de miles de víctimas de diversos sectores como instituciones gubernamentales, telecomunicaciones, energía, activistas, académicos, medios de comunicación, bancos y empresas que desarrollan tecnologías de cifrado[67]. Este malware es colocado en este apartado porque también ha intervenido en instalaciones militares y *visto la complejidad y potencia de esta ciber-arma, se cree que sólo un Estado puede estar detrás de ella*[68].

Hasta aquí se han puesto de manifiesto algunos tipos de amenazas cibernéticas que afectan los diferentes Factores de Poder de un Estado, en el próximo capítulo se analizará una posible organización del entorno cibernético en el nivel operacional para evitar los actos de agresión del enemigo.

[66] Nakashima; *op. cit.*
[67] Juan Miguel Revilla; "Equation Group, la madre de todas las ciberarmas"; *ITespresso*; Publicado el 17 de febrero de 2015; Recuperado el 23 de Septiembre de 2015 de*: http://www.itespresso.es/equation-group-madre-todas-ciberarmas-134065.html*
[68] Revilla; *ibíd.*.

Capítulo III: Ciberdefensa en el Nivel Operacional

Algunos Estados, como España o Chile, han fomentado modificaciones a su legislación para establecer estrategias y estructuras adecuadas que les permitan dirigir y coordinar las actuaciones de distintos agentes, tanto estatales como no estatales, en materia de protección de infraestructuras críticas, para mejorar la prevención, preparación y respuesta frente a todo tipo de amenazas, incluidas las cibernéticas, que puedan afectarlas. Para ello impulsan la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, con el propósito *de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población*.[69]

Esta adecuación legal se observa como necesaria para poder articular las organizaciones y sus procedimientos operativos que les permitan operar desde sus capacidades previas, encuadradas dentro de los conceptos de seguridad de la información y aseguramiento de la información[70], y al mismo tiempo obtener capacidades complementarias en el ámbito de la ciberseguridad y ciberdefensa, resultando esta última responsabilidad de las Fuerzas Armadas (FFAA) del Estado.

Las FFAA dependen de las Tecnologías de la Información y la Comunicación (TIC) para comunicarse, ejercer el mando y control de las operaciones, obtener y distribuir información e inteligencia, realizar labores de vigilancia, reconocimiento o adquisición de objetivos o coordinar los fuegos, por lo que éstas optimizan la concepción, planificación y ejecución de las operaciones, pudiendo condicionar el desarrollo y resultado de una contienda. Por lo tanto, la posesión de una infraestructura TIC robusta, segura y resiliente*, la sistematización de las dimensiones que componen el ciberespacio y su integración en la planificación operativa o la capacidad para actuar en este dominio son algunos de los asuntos que más atención están recibiendo en el ámbito militar.

---

[69] "Boletín Oficial del Estado; Núm. 102; Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas"; Madrid; Publicado el 29 de abril de 2011 Sec. I. Pág. 43370

[70] Guillem Colom Piella, José Ramón Coz Fernández, Enrique Fojón Chamorro y Adolfo Hernández Lorente; "Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales"; ARI 26/2013; *Real Instituto Elcano*; 4 de julio de 2013; p.4.

* La resiliencia; en sistemas tecnológicos, capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones.("Significado de Resiliencia"; *Significados*; Publicado s.f.; Recuperado el 10 de octubre de 2015 de: http://www.significados.com/resiliencia/

Clasificación de Grupos de Riesgo en Ciberdefensa

El estado de riesgo del ciberespacio no es uniforme debido principalmente a las diversas capacidades en materia de ciberseguridad y ciberdefensa de los distintos países. Dependiendo del nivel de organización y funcionalidad de sus sistemas nacionales cibernéticos, los países pueden agruparse en cuatro grandes grupos:

1. Grupo 1, constituido por aquellos países que disponen de un Sistema Nacional de Ciberseguridad y Ciberdefensa operativo, formalmente definido y en continuo proceso de evaluación, revisión y mejora, como EEUU, China e Israel.
2. Grupo 2, formado por países que se encuentran en un proceso formal de construcción de sus sistemas nacionales de ciberseguridad y ciberdefensa, como Australia, Francia e Irán.
3. Grupo 3, integrado por países que se hallan en proceso de definición formal o informal de sus sistemas nacionales de ciberseguridad, en este grupo se encuentran la gran mayoría de países, entre ellos Argentina.
4. Grupo 4, formado por aquellos países que todavía no han emprendido una definición formal ni informal de su sistema nacional de ciberseguridad.[71]

Elemento de Ciberdefensa a Nivel Operacional

Una cuestión de suma relevancia de la Ciberdefensa en el Nivel Operacional es la correcta adopción de un ente o elemento que cumpla los objetivos que ésta persigue en un Teatro de Operaciones (TO). Se observa que algunos países, como España, han resuelto este problema utilizando el concepto de "cibercélula", definiendo a la misma como *una capacidad de alta especialización funcional y naturaleza dual –tanto defensiva como ofensiva– con la función de ejecutar una tarea encomendada con la finalidad de garantizar la seguridad y la defensa de un determinado ámbito cibernético*.[72] Como se observa en esta definición se contempla el rol ofensivo que puede adoptar este elemento para colaborar en la obtención del objetivo, el cual no es aplicable a las FFAA argentinas por su orientación netamente defensiva.

Dependiendo de las particularidades del ambiente operacional en que actúe una cibercélula, ésta podrá ejecutar operaciones cibernéticas específicas, propias del ambiente cibernético, o conjuntas, en forma cooperativa con uno o varios de los

[71] Piella, et al; *op. cit.*, pp. 2-3.
[72] Piella, et al; *op. cit.*, p. 4.

elementos pertenecientes a los restantes dominios operativos del combate (terrestre, marítimo, aéreo y espacial). También, buscando mejorar su nivel de madurez, resiliencia y seguridad y/o *contribuir a la experimentación de nuevos conceptos operativos y capacidades cibernéticas,*[73] podrá colaborar en la evaluación de las capacidades cibernéticas del propio país y del organismo de defensa colectiva del que este forme parte; en tal sentido, al concebir Argentina su defensa en una dimensión "autónoma" y otra "cooperativa" a nivel subregional, regional y global[74], tales actividades podrían realizarse en el marco de la UNASUR.

Otro ejemplo de elemento cibernético en el TO, adoptado por uno de las potencias señeras en ciberdefensa, y que constituyen el componente central del nuevo Comando Cibernético de EEUU son los llamados Equipos de Fuerzas de Ciber Misión, encontrándose éstos en el nivel de unidades tácticas, por lo que colaboran con la obtención de los objetivos operacionales. Los equipos se dividen según sus diferentes especialidades:

1. Equipos de Misión Nacional, preparado para llevar a cabo operaciones en todo el espectro cibernético con el fin de mitigar las amenazas a EEUU y su infraestructura crítica;[75]
2. Equipos Cibernéticos de Protección, que defienden los dominios punto-mil, donde se guardan los secretos militares;
3. Equipos de Misión de Combate que ayudan a las tropas de los comandos combatientes, están ubicados geográficamente con dichos comandos y atacan a sus adversarios en el extranjero.[76]

Los tres tipos de equipos se podrían adaptar a las FFAA argentinas, eliminando del último su capacidad ofensiva, ya que por la actual legislación nacional, no es aplicable al Instrumento Militar del país. Dicha dimensión ofensiva es vital para EEUU debido a que estos equipos cibernéticos deben garantizar la superioridad del ciberespacio, que gira en torno a la idea de prevenir que las fuerzas

[73] Piella, et al; *op. cit.*, p. 4.
[74] Decreto 1714/2009; Ministerio de Defensa; Directiva de Política de Defensa Nacional
[75] Aliya Sternstein; "Pentagon Plans to Deploy More Than 100 Cyber Teams by Late 2015"; *Nextgov*; Publicado el 19 de marzo de 2013; Recuperado el 29 de septiembre de 2015 de: http://www.nextgov.com/defense/2013/03/pentagon-plans-deploy-more-100-cyber-teams-late-2015/61948/
[76] Franz-Stefan Gady; "The US Military Wants to Train More Cyber Warriors"; *The Diplomat*; Publicado el 6 de febrero de 2015; Recuperado el 29 de septiembre de 2015 de: http://thediplomat.com/2015/02/the-us-military-wants-to-train-more-cyber-warriors/

en oposición sean capaces de causar interferencias prohibitivas para que las fuerzas conjuntas propias logren los efectos deseados. [77]

Según los autores que forman parte de *The Cybersecurity Think Tank* (THIBER), grupo de trabajo sobre "Cibercélulas", perteneciente al Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid, en el Nivel Operacional, se deberán traducir los objetivos estratégicos; planificar y supervisar la ejecución de las tareas encomendadas a las cibercélulas, para ello se autorizarán y dirigirán todas las actuaciones concernientes a la tarea delegada por el nivel superior y cada una estará controlada por un Equipo Operativo (EO), cuya composición vendrá determinada por la naturaleza de la tarea. En el Nivel Táctico, los responsables de cada EO definirán los planes y le darán el mayor grado de detalle posible contando con el asesoramiento de los responsables de los equipos tácticos asignados a cada acción y *cada EO estará apoyado por tantos equipos tácticos como acciones formen parte de la actividad*,[78] como se puede observar en el Anexo 3.

Con el propósito de normalizar el funcionamiento en los Niveles Estratégico, Operacional y Táctico, las cibercélulas deberán contar con una metodología de trabajo que proporcione un lenguaje común, fundamentos teóricos y procedimientos tecnológicos homogeneizados.

Además, el THIBER establece que el conocimiento del estado de la ciber-situación ayudará a las cibercélulas a tomar mejores decisiones y a actuar de manera más eficiente si conocen el efecto operativo de estas decisiones sobre el conjunto de la misión. Dicha ciber-situación se obtiene combinando el conocimiento de actividades de inteligencia, las realizadas en el espacio electromagnético y las operativas de todos los dominios de la guerra: tierra, mar, aire, espacio y ciberespacio. Este conocimiento debe incluir el ciberespacio propio, del aliado, de los posibles adversarios y de cualquier otra entidad de interés. [79]

Por las características defensivas de la política de la República Argentina en el plano de la ciberdefensa, es más adecuado adoptar un concepto de Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT o *Computer Security Incident Response Team*), utilizado en el sector académico, comercial entre otros, además del militar. Este equipo, formado por expertos en seguridad de las

[77] Gady; *op. cit.*
[78] Piella, et al; *op. cit.*, pp. 6-7.
[79] Piella, et al; *op. cit.*, p. 8.

Tecnologías de la Información, tiene como principal tarea responder a los incidentes de seguridad informática prestando los servicios necesarios para ocuparse de estos incidentes y ayudar a recuperar el normal funcionamiento del sistema después de sufrir uno de ellos. Para mitigar los riesgos y minimizar el número de respuestas necesarias, realizan tareas preventivas y educativas.[80]

Otra opción que podría adaptarse a la política del país es el elemento conocido como Capacidad de Respuesta a Incidentes Informáticos de la OTAN (NCIRC: *NATO Computer Incident Response Capability*), que es responsable de la defensa cibernética de todos los Puestos Comandos de la OTAN, tanto de los estáticos como los desplegados para operaciones o ejercicios. [81]

Para complementar al anterior, la OTAN formuló el concepto de Equipo de Reacción Rápida (ERR) [82]. Dicho Equipo puede actuar en un plazo muy corto para hacer frente a un ataque que afecta a la capacidad operativa de un sistema de la OTAN durante una crisis o para ayudar a un Estado miembro, a petición del mismo, en el caso de un ataque cibernético importante a nivel nacional[83].

Los ERR están compuestos por un núcleo permanente de seis expertos especializados que pueden coordinar y ejecutar misiones de Reacción Rápida en el ámbito cibernético. También hay expertos nacionales o de la OTAN en áreas específicas. Su número y el perfil se determinan sobre la base de la misión a realizar. Los ERR tienen todo el equipamiento necesario en Tecnologías de la Información y Telecomunicaciones, como teléfonos satelitales y equipos para la recolección digital evidencia, criptografía, análisis forense digital, gestión de vulnerabilidades, seguridad de red, etc.

Como se observa, en el ámbito cooperativo existe una correlación entre el ERR de la OTAN y el Equipo de Respuesta ante Emergencias Informáticas (CERT) en el ámbito de la UNASUR, creado para incrementar la seguridad cibernética de Argentina y Brasil. Pero hay que tener presente que este tipo de entidad está diseñada para complementar las capacidades de los elementos cibernéticos de los respectivos países y de ninguna manera para reemplazarlas o sustituirlas.

---

[80] Agencia Europea de Seguridad de las Redes y de la Información (ENISA); "Cómo crear un CSIRT paso a paso"; 2006; p.6.

[81] NATO; "NATO Rapid Reaction Team to fight cyber attack"; *NATO*; Publicado el 13 de marzo de 2012; Recuperado el 29 de septiembre de 2015 de: http://www.nato.int/cps/en/natolive/news_85161.htm

[82] NATO; *Ibíd.*

[83] NATO; "Men in black: NATO's cybermen"; *NATO;* Publicado el 24 de abril de 2015; Recuperado el 5 de octubre de 2015 de: http://www.nato.int/cps/en/natohq/news_118855.htm

Servicio que deben prestar los Equipos de Seguridad en Ciberdefensa

Los Equipos de Respuesta a Incidentes de Seguridad Informática están diseñados para prestar servicios reactivos, proactivos y de gestión de calidad de la seguridad.

Servicios Reactivos

Son aquellos que se centran en el tratamiento de los incidentes y la mitigación de los daños resultantes de estos. Se clasifican en alertas y advertencias, manejo de incidentes (análisis, respuesta *in situ,* apoyo de respuesta a incidentes y coordinación de respuesta a incidentes); manejo de vulnerabilidad (análisis, respuesta y coordinación de la respuesta de la vulnerabilidad) y manipulación de dispositivos (análisis, respuesta a dispositivos y coordinación de la respuesta a dispositivos)[84]

Servicios Proactivos

Estos servicios proveen de asistencia e información para ayudar a preparar, proteger y asegurar los sistemas constituyentes en previsión de ataques, problemas o eventos. La performance de estos servicios reducirá directamente el número de incidentes en el futuro. Estos servicios son alertas o avisos; tecnologías de vigilancia; auditorías o evaluaciones de seguridad; configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras; desarrollo de herramientas de seguridad; servicios de detección de intrusiones y difusión de información relacionada con la seguridad. [85]

Servicios de Gestión de Calidad en Seguridad

Estos servicios potencian los servicios ya existentes que son independientes de gestión de incidentes y son tradicionalmente realizados por otras áreas de la organización, tales como los departamentos de Tecnologías de la Información, auditoría o formación, ya que su punto de vista y experiencia puede ayudar a mejorar la seguridad general de la organización e identificar los riesgos, amenazas y debilidades del sistema. Estos servicios son generalmente proactivos y contribuyen indirectamente a reducir el número de incidentes. Dentro de estos servicios se encuentran el análisis de riesgo; la planificación de continuidad de función y

[84] CERT; "CSIRT Services"; *CERT, Software Engineering Institute*; Publicado s.f. ; Recuperado el 29 de septiembre de 2015 de: http://www.cert.org/csirts/services.html.
[85] CERT; *Ibíd.*

recuperación de desastres; consultoría de seguridad; generación de conciencia; educación / capacitación y evaluación o certificación de productos. [86]

Áreas funcionales del Elemento de Ciberdefensa

Se han identificado ciertas áreas funcionales que permiten manejar un programa robusto de ciberseguridad en las organizaciones.[87]

Entre estas áreas se encuentra la de Administración de Sistemas, cuyo objetivo es proteger a los canales administrativos de la organización y evitar su uso por parte de un adversario; el área de Seguridad de Redes, para proteger las redes propias contra accesos no autorizados, entre ellas las redes que permiten el Comando y Control en un TO.[88]

Otras áreas importantes son la de Seguridad de Aplicaciones, que tiene por objetivo proteger las aplicaciones y software propios e impedir su uso o la explotación de sus vulnerabilidades por un adversario, el área de Seguridad de Punto final, servidor, y dispositivos, que complementa a la anterior y consiste en resguardar los dispositivos informáticos de punto final (por ejemplo, los ordenadores personales o los que controlan el equipamiento bélico, servidores y dispositivos móviles) de los ataques y detectar cuando las defensas se han vulnerado.[89] Esta área es de vital importancia en los niveles tácticos y operacionales del IM debido a que aquí se encuentra encuadrada la ciberseguridad de los sistemas de armas y los puestos comandos de un TO.

Fundamentales para la efectividad de las Medidas de Seguridad de Contrainteligencia (MSCI) son el área de Gestión de Identidad, autenticación y acceso, que tiene como meta asegurar que sólo las personas autorizadas puedan acceder a los recursos propios; el área de Protección de Datos y Criptografía, que permite proteger la confidencialidad e integridad de los datos mediante técnicas como el cifrado y firmas digitales*; y el área de Gestión de Monitoreo,

[86] CERT, *op. cit*.
[87] Scott Donaldson, Stan Siegel, Chris Williams y Abdul Aslam; "Enterprice Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats"; *Apress*; Nueva York; 2015; p.47.
* Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad). (Dennis K. Branstad;"Report of the Nist Workshop on Digital Signature Certificate anagement"; *U.S. Department of Commerce;* 1983)
[88] Donaldson, et al; *op.cit.* pp. 48-52.
[89] Donaldson, et al; *op.cit.* pp. 52-56.

vulnerabilidad y revisiones, que aporta la capacidad de monitorear el estado de seguridad de la organización y mantener la misma en el transcurso del tiempo mediante la identificación y eliminación de vulnerabilidades tan pronto como sean descubiertas.[90]

El área de Alta disponibilidad, recuperación de desastres y protección física, cuya meta es procurar la continuidad de las operaciones frente a la adversidad, que pueden ir desde leves fallos informáticos o rutinarios hasta graves catástrofes naturales o de origen humano[91], resulta fundamental en un TO, ya que el oponente intentará degradar las capacidades propias. Se pueden observar los diferentes niveles de fiabilidad de un centro de datos en el Anexo 4.

En apoyo a la anterior, el área de Respuesta a Incidentes proporciona respuesta oportuna cuando se identifican los incidentes de seguridad; como interrupciones operativas, incidentes de seguridad, ataques deliberados, desastres naturales y de origen humano, y errores y accidentes.[92]

Por último, el área de Gestión de Recursos y Cadena de Suministro gestiona los riesgos de dicha cadena, que es especialmente vulnerable, desde la adquisición hasta la eliminación del recurso; y el área de Política, Formación, Auditoría y E-Discovery o Descubrimiento Electrónico, en la que se busca, localiza y asegura información electrónica con el propósito de ser usada como evidencia[93].

Es evidente que estas muchas de estas áreas son básicas para las medidas de seguridad de contra inteligencia, por lo tanto fundamentales para mantener en secreto los propios planes e intenciones, posibilitando así el principio de sorpresa; y otras permiten alcanzar la necesaria libertad de acción. Se observa entonces que el Elemento de Ciberdefensa proporciona una eficaz herramienta para que las Fuerzas Armadas puedan mejorar la defensa y protección en el ámbito cibernético en apoyo a las operaciones en un TO. Estos elementos estarían formados por componentes operacionales y tácticos operando bajo el control de un mando estratégico[94].

[90] Donaldson, et al; *op. cit.* pp. 57-62.
[91] Donaldson, et al; *op. cit.* pp. 57-62.
[92] Donaldson, et al; *op. cit.* pp. 62-64.
[93] Carina Espeche; "Qué es "e-Discovery"?"; *El Auditor Interno*; Publicado s.f.; Recuperado el 10 de octubre de 2015 de: https://www.iaia.org.ar/revistas/elauditorinterno/21/Articulo2.htm
[94] Piella, et al; *op. cit.*, p. 10.

Conclusiones

A lo largo de la investigación se observó la dificultad en relación a la determinación de las infraestructuras que puedan ser objeto de ataques a través del ciberespacio por parte de un oponente, ya que dependerá en gran medida del criterio adoptado por dicho adversario, y esto es debido a que muchos de estos objetivos, como los puertos, aeropuertos, vías férreas, sistemas de producción y suministro eléctricos, sistemas de comunicación, ciertas fábricas dentro del TO, caen dentro de la clasificación de bienes de uso dual cumpliendo éstos tanto con fines civiles como militares.

Por otro lado, si el virtual adversario tiene un marco legal similar al argentino, éste podrá restringirse a atacar solo aquellos objetivos de clara utilidad militar exclusivamente y que estén siendo utilizados en operaciones por las FFAA asignadas al TO. Pero si dicho adversario tiene una política cibernética más amplia, el espectro de objetivos lícitos será mucho mayor y bienes duales que en el presente se esté usando solamente en su función civil, podrán convertirse en blancos de ataques si éste prevé que potencialmente existe una probabilidad razonable e inminente de que se use con fines militares dentro del conflicto en desarrollo.

Por lo tanto deberá existir una adecuada coordinación y colaboración para un accionar eficiente en ciberseguridad entre el Comandante del TO con las organizaciones civiles y del sector privado con incumbencia en un área específica.

Con respecto a la identificación taxativa de las amenazas en el entorno cibernético que puedan explotar alguna vulnerabilidad en las estructuras que se caractericen como críticas es una tarea infructuosa, queda claro que el espectro de amenazas cibernéticas es inmensurable y se encuentra en permanente crecimiento. Cada vez se producen más ataques cibernéticos en el mundo y éstos son cada vez más sofisticados[95].

Se observa que no todas estas amenazas son de incumbencia del Instrumento Militar, y son aún menos las amenazas que entran en la jurisdicción del Nivel Operacional. A pesar de lo anterior, al tener el ciberespacio como características fundamentales la interdependencia e interoperabilidad, hay que considerar las posibles implicancias que tendrán en el desempeño de las FFAA asignadas al TO interferencias realizadas a elementos de uso dual o que estén fuera del TO, como

[95] "NATO Rapid Reaction Team to fight cyber attack", *NATO*; Publicado el 13 de marzo de 2012; Recuperado el 29 de septiembre de 2015 de: http://www.nato.int/cps/en/natolive/news_85161.htm

satélites de comunicación o el sistema ferroviario con el que llevan insumos dentro del teatro. Por esto se hace necesario un sistema de ciberdefensa que pueda integrarse con los sistemas de ciberseguridad desarrollados por los responsables de las infraestructuras básicas del país.

Al analizar las alternativas para hacer frente a las amenazas cibernéticas en un TO de manera oportuna y eficaz, hay que considerar el marco normativo argentino en lo que respecta a la ciberdefensa, el cual se está adecuando al contexto de lo que se conoce como nuevas amenazas o formas de hacer la guerra, observándose que su enfoque es meramente defensivo, dejando de lado la ofensiva por haber sido sesgada en el modo de pensar y actuar del país, lo que queda explicitado en que éste ha dado por concluida toda hipótesis de conflicto.

Aunque muchos de los expertos en el ámbito de la ciberdefensa opinan que la ofensiva es dominante en la guerra cibernética[96], afirmando incluso que *la competencia cibernética será predominantemente ofensiva en el futuro previsible*[97]; una propuesta defensiva que posibilita seleccionar un Elemento de Ciberdefensa a Nivel Operacional que puede adaptarse adecuadamente al proceder nacional es la que propone focalizarse en robustecer lo máximo posible las cualidades defensivas de los sistemas de TIC enfocándose en la resiliencia. *En lugar de construir muros, (hay que) centrarse en cómo recuperar rápidamente los sistemas o, mejor aún, seguir funcionando incluso después de que hayan sido comprometidos*[98].

Pero cabe percatarse que algunos países que, como Argentina, han mantenido una política de ciberdefensa basada en operaciones cibernéticas pasivas y defensivas para contrarrestar los ataques cibernéticos procedentes de sus oponentes, se han visto forzados a cambiar por una conducta mas proactiva y tomar medidas preventivas para defenderse de ciber infiltraciones y evitar de esta forma que el enemigo obtenga una ventaja desde el principio, el mejor ejemplo de esto es el de Corea del Sur con respecto a su vecino homónimo del norte.

Un enfoque bidimensional defensivo-ofensivo se está adoptando en países muy avanzados en el dominio cibernético de la guerra, como es el caso de Israel, y

[96] Zachary Keck; "South Korea Seeks Offensive Cyber Capabilities"; *The Diplomat*; Publicado el 11 de octubre de 2014; Recuperado el 29 de septiembre de 2015 de: http://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/

[97] Peter W. Singer y Allan Friedman; "Cult of the Cyber Offensive: Why belief in first-strike advantage is as misguided today as it was in 1914"; Revista online *Foreign Policy*; Publicado el 15 de enero 2014; Recuperado el 29 de septiembre de 2015 de: http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/

[98] Singer y Friedman*; Ibíd.*

sus autoridades militares señalan que .la conexión entre acción cibernética defensiva y ofensiva es muy importante, y el hecho de que hasta ahora hayan sido vistas como dominios separados era una especie de anomalía, por ello el ejército israelí ha decidido aplicar un enfoque sinérgico a esta nueva dimensión crítica de combate[99].

En el Nivel Operacional aún existe en las FFAA de Argentina un vacío en cuanto al mejor modo de organizar y utilizar los recursos del ciberespacio para contribuir al logro de los objetivos planteados por el nivel superior dentro de un TO. Se estima que una adaptación de las soluciones encontradas por otros países a este respecto, teniendo en cuenta las capacidades actuales y potenciales de la Nación, es el Elemento de Ciberdefensa a Nivel Operacional, el cual vendría a satisfacer necesidades de protección de la capacidad bélica propia brindando fundamentalmente Libertad de Acción.

Como se puede observar, en el ámbito de la ciberseguridad, necesariamente se deben considerar las acciones básicas que desarrollan las FFAA en busca de sus objetivos, para proteger de manera coherente, sistemática y sistémica la información crítica, distribuida en toda su infraestructura de interés, tanto militar, civil o de uso dual, previa evaluación de cómo ella impacta la operación del Instrumento Militar en el TO.

Se puede afirmar que la hipótesis planteada para esta investigación, es decir que si se establece una manera de proceder adecuada en el ámbito de la ciberdefensa se podrá limitar las acciones nocivas y las amenazas cibernéticas que puedan afectar alguna estructura crítica del estado, y las capacidades del instrumento militar dentro de un teatro de operaciones contemporáneo, se ve confirmada por la información de países y alianzas de países que en la práctica han mejorado sus niveles de seguridad a través del robustecimiento de sus sistemas de ciberdefensa.

[99] Barbara Opall-Rome; "Israel to consolidate cyber spending and operations"; *Defense News;* Publicado el 6 de julio de 2015; Recuperado el 29 de septiembre de 2015 de: http://www.c4isrnet.com/story/military-tech/cyber/2015/07/06/israel-cyber-spending-operations/29776041/

Bibliografía

Libros:

- Agencia Europea de Seguridad de las Redes y de la Información (ENISA); "Cómo crear un CSIRT paso a paso"; *ENISA* ; 2006; pp. 6/ 47-69.
- Donaldson, Scott, Stan Siegel, Chris Williams y Abdul Aslam; "Enterprice Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats"; *Apress*; Nueva York; 2015; pp. 47-68.
- Gastaldi, Sol, Candela Justribó; "La seguridad y la defensa en el ámbito ciberespacial. Informe de investigación, Desarrollo Estratégico Nacional en Escuela de Defensa Nacional (EDENA)"; *EDENA*; octubre de 2014. p. 6.
- Masana, Sebastián; "El ciberterrorismo: ¿una amenaza real para la paz mundial?"; Tesis de maestría *Facultad Latinoamericana de Ciencias Sociales*, 8 de julio de 2002; pp. 26, 28.
- Medero, Gema Sánchez; "La ciberguerra: los casos de Stuxnet y Anonymous"; *Derecom, Nueva Época. No. 11* , Septiembre-Noviembre, 2012; pp. 92 / 130.
- Medero, Gema Sánchez; "Los Estados y la Ciberguerra"; *Universidad Complutense de Madrid;* 2010; pp. 64, 73
- Piella, Guillem Colom, José Ramón Coz Fernández, Enrique Fojón Chamorro y Adolfo Hernández Lorente; "Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales"; ARI 26/2013; *Real Instituto Elcano*; 4 de julio de 2013; pp. 2-10 / Tabla de p. 3.
- Sandoz, Yves, Christophe Swinarski y Bruno Zimmermann; "Comentario del Protocolo adicional I de los Convenios de Ginebra del 12 de agosto de 1949", *CICR*, Plaza y Janés Editores, Bogotá, tomo II, párr. 2020-2024.
- Schmitt, Michael N., "Essays on Law and War at the Fault Lines"; *Asser Press;* 2012. p. 176.
- Schmitt, Michael N., "Tallinn Manual on the International Law Applicable to Cyber Warfare", *Cambridge University Press*; Edición: Reimpreso, 7 de marzo de 2013. p. 19
- Singer, Peter W. y Allan Friedman; "Cybersecurity and Cyberwar, what everyone needs to know"; *Oxford University Press;* New York; 2014; pp. 128, 133.

Conferencias:

- Batanero, Juan Carlos; "Ciberdefensa"; *IX CICLO DE CONFERENCIAS UPM TASSI*. Madrid: Indra, 2013. Diap. 3.
- Justribó, Candela; "Ciberdefensa: Una visión desde la UNASUR, VII Congreso del Instituto de Relaciones Internacionales", La Plata, 26, 27 y 28 de noviembre de 2014. p.9.

Leyes, Decretos, Resoluciones y Boletines Oficiales

- "Boletín Oficial del Estado; Núm. 102; Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas"; Madrid; Publicado el 29 de abril de 2011 Sec. I. p. 43370
- Decreto 1714/2009; Ministerio de Defensa; Directiva de Política de Defensa Nacional
- Decreto 727/2006; Ministerio de Defensa; Reglamentación de la Ley Nº 23554.
- Decreto 1273/92; Ministerio de Seguridad Interior; Reglamentación de la Ley Nº 24059.
- Resolución del Ministerio de Defensa N° 350/2014
- Resolución del Ministerio de Defensa N° 350/2014

Manuales:

- "The Commander's Handbook on the Law of Naval Operations (NWP 1-14M, MCWP 5-2.1, COMDTPUB P5800.7)"; *Marina de EEUU/ Infantería de Marina/ Servicio de Guardacostas;* 1995, párr. 8.1.1.

Páginas Web

- "Amenazas cibernéticas"; *Federal Emergency Management Agency (FEMA)*;s.f.*;* Recuperado el 17 de Septiembre de 2015 de *http://m.fema.gov/es/cyber-attack*
- CERT; "CSIRT Services"; *CERT, Software Engineering Institute*; Publicado s.f. ; Recuperado el 29 de septiembre de 2015 de: http://www.cert.org/csirts/services.html.
- Comisión Europea; "Trade Topics, Dual Use"; *European Commission*; Actualizado el 15 de Julio de 2015. Recuperado el 11 de septiembre de 2015 de http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm

- Core One; “Tipos de ataques informáticos”; *Core One Information Technology;* s.f.; Recuperado el 17 de Septiembre de 2015 de http://www.coreoneit.com/tipos-de-ataques-informaticos/
- Delio, Michelle; “Crackers Expand Private War”; *Wired News*; Publicado el 18 de abril de 2001. Recuperado el 20 de Septiembre de 2015 de: *http://www.wired.com/news/politics/0,1283,43134,00.html*
- Diginota; “China, EEUU y Rusia en guerra cibernética, según McAfee”; *Diginota*; Publicado el 11 de abril de 2012; Recuperado el 22 de julio de 2015 de http://www.diginota.com/china-eeuu-y-rusia-en-guerra-cibernetica-segun-mcafee/
- Dunn, Ashley; “Crisis in Yugoslavia: Battle Spilling Over Onto the Internet”; *Los Angeles Times*, Publicado el 3 de abril de 1999; Recuperado el 20 de Septiembre de 2015 de: *http://articles.latimes.com/1999/apr/03/news/mn-23851*
- Espeche, Carina; “Qué es “e-Discovery”?”; *El Auditor Interno*; Publicado s.f.; Recuperado el 10 de octubre de 2015 de: https://www.iaia.org.ar/revistas/elauditorinterno/21/Articulo2.htm
- Fraga, Alberto Iglesias; “El 67% de las empresas europeas sufrió un ciberataque en 2014”; *TICbeat*; Publicado el 23 de septiembre de 2015; Recuperado el 23 de septiembre de 2015 de: *http://www.ticbeat.com/seguridad/el-67-de-las-empresas-europeas-sufrio-ciberataque-en-2014/*
- Gady, Franz-Stefan; “The US Military Wants to Train More Cyber Warriors”; *The Diplomat*; Publicado el 6 de febrero de 2015; Recuperado el 29 de septiembre de 2015 de: http://thediplomat.com/2015/02/the-us-military-wants-to-train-more-cyber-warriors/
- Gross, Michael Joseph; “Silent War”; *VF News*; Publicado en julio de 2013. Recuperado el 17 de Septiembre de 2015 de *http://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business*
- Guilarte, María; “¿Qué es un Tier?”; *MC Pro*; Publicado el 14 de marzo de 2013; Recuperado el 23 de septiembre de 2015 de: http://www.muycomputerpro.com/
- Harmon, Amy; “Hacking Theft of $10 Million From Citibank Revealed”; *Los Angeles Times*; Publicado el 19 de Agosto de 1995; Recuperado el 23 de

septiembre de 2015 de: *http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system*

- ICIC; "Qué hacemos"; *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*. Actualizado el 15 de Julio de 2015. Recuperado el 11 de septiembre de 2015 de http://www.icic.gob.ar/
- IT Law Wiki; "Cyberattack, Definitions"; *IT Law Wiki*; Publicado el 1 de febrero de 2001; Recuperado el 18 de junio de 2015 de: http://itlaw.wikia.com/wiki/Cyberattack
- Keck, Zachary; "South Korea Seeks Offensive Cyber Capabilities"; *The Diplomat*; Publicado el 11 de octubre de 2014; Recuperado el 29 de septiembre de 2015 de: http://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/
- Ministerio de Defensa de España; Publicación del Manual de Tallín sobre "Ley Internacional en la Ciberguerra", *Portal de Tecnología e Innovación del Ministerio de Defensa*. Publicado el 22 de marzo de 2013. Recuperado el 9 de septiembre de 2015 de http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59
- Nakashima, Ellen; "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace"; *The Washington Post*. Publicado el 30 de Mayo de 2012. Recuperado el 22 de septiembre de 2015 de: *https://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html*
- NATO; "Cyber - the good, the bad and the bug-free, The history of cyber attacks - a timeline"; *NATO Review;* s.f.; Recuperado el 28 de mayo de 2015, de: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
- NATO; "Men in black: NATO's cybermen"; *NATO;* Publicado el 24 de abril de 2015; Recuperado el 5 de octubre de 2015 de: http://www.nato.int/cps/en/natohq/news_118855.htm
- NATO; "NATO Rapid Reaction Team to fight cyber attack"; *NATO*; Publicado el 13 de marzo de 2012; Recuperado el 29 de septiembre de 2015 de: http://www.nato.int/cps/en/natolive/news_85161.htm
- Norris, Michael J.; "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace". *Student Pulse*.

Publicado en 2013. Recuperado el 10 de septiembre de 2015 de http://www.studentpulse.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace

- Opall-Rome, Barbara; "Israel to consolidate cyber spending and operations"; *Defense News;* Publicado el 6 de julio de 2015; Recuperado el 29 de septiembre de 2015 de: http://www.c4isrnet.com/story/military-tech/cyber/2015/07/06/israel-cyber-spending-operations/29776041/
- OVH; "Niveles Tier"; *OVH.es*; Recuperado el 24 de septiembre de 2015 de: https://www.ovh.es/servidores_dedicados/niveles-tier-3-4.xml
- Revilla, Juan Miguel; "Un grupo de hackers robó 300 millones de dólares a varios bancos"; *ITespresso*; Publicado el 16 de febrero de 2015; Recuperado el 20 de Septiembre de 2015 de: *http://www.itespresso.es/hackers-robo-300-millones-dolares-bancos-134021.html*
- Revilla, Juan Miguel; "Equation Group, la madre de todas las ciberarmas"; *ITespresso*; Publicado el 17 de febrero de 2015; Recuperado el 23 de Septiembre de 2015 de*: http://www.itespresso.es/equation-group-madre-todas-ciberarmas-134065.html*
- Russia Today; "Guerra virtual: EE.UU. dominará el campo de batalla cibernético con su secreto 'Plan X'", *Russia Today*, Publicado el 23 de agosto de 2012. Recuperado el 22 de septiembre de 2015 de: *http://actualidad.rt.com/actualidad/view/52072-guerra-bestia-darpa-dominara-campo-batalla-cibernetica-secreto-plan-x*
- Schmitt, Michael N.; "La guerra de la información: los ataques por vía informática y el jus in bello" Comité Internacional de la Cruz Roja. Publicado el 30 de junio de 2002. Recuperado el 31 de Agosto de 2015 de http://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business
- Singer, Peter W. y Allan Friedman; "Cult of the Cyber Offensive: Why belief in first-strike advantage is as misguided today as it was in 1914"; Revista online *Foreign Policy*; Publicado el 15 de enero 2014; Recuperado el 29 de septiembre de 2015 de: http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/
- Sternstein, Aliya; "Pentagon Plans to Deploy More Than 100 Cyber Teams by Late 2015"; *Nextgov*; Publicado el 19 de marzo de 2013; Recuperado el 29 de

septiembre de 2015 de: http://www.nextgov.com/defense/2013/03/pentagon-plans-deploy-more-100-cyber-teams-late-2015/61948/

- SurfWatch; "Cyber Risk Intelligence"; *SurfWatch, Ciber in Sight*; s.f.*;* Recuperado el 17 de Septiembre de 2015 de *https://www.surfwatchlabs.com/threat-categories#Practice*
- The White House; "The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"; sitio oficial *The White House*; Publicado en mayo de 2011. p.9. Disponible en http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- Veiguela, Lino González; "Los ciberataques (conocidos) más importantes"; *EsGlobal.com*. Publicado el 02 de julio de 2013. Recuperado el 17 de Septiembre de 2015 de *http://www.esglobal.org/la-lista-los-ciberataques-conocidos-mas-importantes/*

Protocolos:

- Protocolo Adicional I a los Convenios de Ginebra del 12 de agosto de 1949; art 48, art. 49 (1), art. 50 (1), 52 (1), art. 43 (2), art. 51 (3), art. 52 (2)

Revistas:

- Air Force Law Review; "Carta de DAJAIA al Consejero para la Investigación y la Ingeniería en Defensa (Economía), Embajada de la República Federal de Alemania (22 de enero de 1988)"; citada en W.H. Parks, "Air War and the Law of War", *Air Force Law Review* , vol. 32, 1992, p. 1.
- Uzal, Roberto; "Guerra Cibernética: ¿un desafío para la Defensa Nacional?"; Revista *Visión Conjunta* Número 7. Año 4 Número 7, 2012; p. 40.

Anexo 1: Prácticas de Ciberataques

Cuadro Nº 1: Metodología de los ciberataques[100]

Categoría	Descripción	Ejemplos
Malware	Software utilizado para interrumpir el funcionamiento del ordenador, recopilar información sensible, o tener acceso a los sistemas informáticos privados	Virus, troyanos, etc.
Ataque de Red	Interactuar con las comunicaciones informáticas para causar un ataque.	DDoS, sniffers, paquetes imitan, etc.
Intrusiones de Red	El acceso a una red informática prohibido.	
Acceso no Autorizado	Obtener datos más allá de lo que está permitido.	En cuanto a información de la cuenta amazónica de su amigo. Adivinar una contraseña para robar los registros de recursos humanos de una empresa - el secuestro de códigos de verificación, cifrado de derivación - ataque de fuerza bruta
Ingeniería Social	La manipulación de la gente para sacarles información de manera fraudulenta.	Llamar a alguien y pasar por mesa de ayuda para obtener información sensible. Phishing técnicas para obtener datos sensibles - phishing, spear phishing.
Distribución Ilícita	El comercio o la difusión de los datos, la información o tecnología ilegal o indeseable.	Doxxing, cardado y fugas
Actividad de Personal Interno	Una persona empleada por una empresa provoca daños cibernéticos a través de sus accesos.	Un administrador del sistema descontentos trae deliberadamente la red en su último día, o un empleado médico utiliza su posición para obtener información de registro del paciente para su uso individual - Violación BYOD.

[100] SurfWatch; "Cyber Risk Intelligence"; SurfWatch, Ciber in Sight; s.f.; Recuperado el 17 de Septiembre de 2015 de https://www.surfwatchlabs.com/threat-categories#Practice

Espionaje	(Espionaje) Implica obtener una información del gobierno o individuo considerada secreta o confidencial sin la autorización del titular de la información	Operaciones de inteligencia de señales (SIGINT), Operación Flatliquid, espionaje corporativo
Explotar la Vulnerabilidad Software	Cuando un hacker utiliza un agujero de seguridad de software que todavía no ha sido parcheado por los desarrolladores de software para llevar a cabo un ataque cibernético.	Vulnerabilidades del protocolo AIS, CVE-2013-3613, la vulnerabilidad Touch ID
Operación de Hacking	Campaña, Operación o acción de hackers (s) que normalmente se dirige a un grupo / industria específica	Anonymous se dirige al gobierno italiano y anuncia la piratería como una operación. #OpUSA, #OpItaly, Operación Troya
Aplicación de la Ley de Intervención	Esta categoría se puede utilizar para una variedad de acciones de aplicación de la ley, tales como hacer un arresto, llevar a cabo una redada, confiscar equipos relacionados con un delito informático, o cualquier otra intervención policial.	Un ejemplo de esto sería si un mercado criminal en línea fue descubierto por la policía y se apoderó de cualquier equipo o bitcoins de las operaciones en el sitio o arrestado individuos etc.
Investigación sobre Seguridad	Hay muchas empresas que llevan a cabo la investigación en seguridad y publican sus hallazgos esta etiqueta se debe utilizar cuando se lleva a cabo la investigación con el fin de encontrar vulnerabilidades en sistemas operativos, programas o cualquier software.	Los investigadores de seguridad de Microsoft encuentran una vulnerabilidad y publican sus hallazgos en unos documentos.
Ataque Mitigada	Esta etiqueta se puede utilizar en cualquier momento una empresa / entidad / organización detecta un ataque inminente en sus redes o sistemas y evita el ataque se produzca.	

Soluciones de Seguridad	Esta etiqueta es para productos de hardware, software o servicios utilizados para la prevención de amenazas o de mitigación de ataques.	Ejemplos: Frontier Communications anuncia Computer Security Pro & Mobile Security Pro para las pymes. IBM lanza amenaza Sistema de Protección suite de productos y el Programa de Protección de Datos Críticos.

Anexo 2: Amenazas Cibernéticas

Los siguientes conceptos han sido recuperados de la página web de Core One[101].

Tipos de ataques informáticos

Existen diferentes tipos de softwares maliciosos que son utilizados como ataques a la información de las organizaciones. Éstos se clasifican en Malwares y Grayware.

Es un tipo de software que tiene como propósito infiltrarse y dañar una computadora o sistema de información sin el consentimiento de los propietarios.

Los malwares son considerados en función de los efectos que provoquen, incluyendo diferentes tipos como son:

- **Virus y Gusanos:** Éstos, son los tipos más conocidos de software maligno que existen y se distinguen por la manera en que se propagan. El término de virus informático se usa para designar un programa que al ejecutarse se propaga infectando otro software ejecutable de la misma computadora. Pueden tener un playload que realice otras acciones maliciosas en donde se borran archivos. Los gusanos son programas que se transmiten así mismos, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. Su principal objetivo, es infectar a la mayor cantidad posible de usuarios y también puede contener instrucciones dañinas al igual que los virus. A diferencia que los gusanos, un virus necesita la intervención del usuario para propagarse, mientras que los gusanos se propagan automáticamente.

- **Backdoor o Puerta Trasera:** Es un método para eludir los procedimientos habituales de autenticación al conectarse en una computadora. Una vez que el sistema ha sido comprometido, puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro de los atacantes. Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, permaneciendo ocultos ante posibles inspecciones, utilizando troyanos, gusanos u otros métodos.

- **Drive-by Downloads:** Son sitios que instalan spyware o códigos que dan información de los equipos. Generalmente se presentan como descargas que de algún tipo, se efectúan sin consentimiento del usuario, lo cual ocurre al visitar un sitio web, al revisar un mensaje de correo o al entrar a una ventana pop-up. El proceso de ataque Drive-by Downloads se realiza de manera automática mediante herramientas que buscan en los sitios web alguna vulnerabilidad e insertan un script malicioso dentro del código HTML.

- **Rootkits: E**s un software que modifica el sistema operativo de la computadora, para permitir que el malware permanezca oculto al usuario, evitando que el proceso malicioso sea visible en el sistema.

[101] Tipos de ataques informáticos, Core One Information Technology. Recuperado el 17 de Septiembre de 2015 de http://www.coreoneit.com/tipos-de-ataques-informaticos/

- **Troyanos:** Es un software malicioso que permite la administración remota de una computadora de forma oculta y sin el consentimiento del propietario. Generalmente están disfrazados como algo atractivo o inocuo que invitan al usuario a ejecutarlo. Pueden tener un efecto inmediato y tener consecuencias como el borrado de archivos del usuario e instalar más programas maliciosos. Son usados para empezar la propagación de un gusano, inyectándolo de forma local dentro del usuario.

- **Hijackers:** Son programas que realizan cambios en la configuración del navegador web, cambiando la página de inicio por páginas con publicidad, pornográficas u otros re direccionamientos con anuncios de pago o páginas de phishing bancario. Ésta es una técnica que suplanta al DNS, modificando archivos hosts, para redirigir el dominio de una o varias páginas a otras, muchas veces una web falsa que imita a la verdadera. Comúnmente es utilizada para obtener credenciales y datos personales mediante el secuestro de una sesión.

- **Keyloggers y Stealers:** Estos programas están encaminados al aspecto financiero, la suplantación de personalidad y el espionaje. Los Keyloggers monitorizan todas las pulsaciones del teclado y las almacenan para realizar operaciones fraudulentas como son pagos desde cuentas de banco o tarjetas de crédito. La mayoría de estos sistemas son usados para recopilar contraseñas de acceso, espiar conversaciones de chat u otros fines. Los Stealers también roban información privada pero solo la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados y si tienen contraseñas recordadas, por ejemplo en los navegadores web la descifran.

- **Botnets:** Son redes de computadoras infectadas, también llamadas "zombies", que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de spam o para lanzar ataques contra organizaciones. En una Botnet cada computadora infectada por el malware se loguea en un canal de IRC u otro sistema de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente. Las botnets también pueden ser usadas para actualizar el malware en los sistemas infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad.

- **Rogue software:** Hacen creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.

- **Los Ransomware:** También llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un "rescate" para poder recibir la contraseña que permite recuperar los archivos.

Grayware o greynet

Los Grayware o greynet son software maliciosos que no son tan peligrosos como los malwares. Suelen utilizarse para clasificar las aplicaciones o programas de cómputo y se instalan sin la autorización de los usuarios.

Los tipos de Grayware que existen son:

- **Adware:** Son programas que automáticamente se ejecutan y muestran publicidad web, después de instalar el programa o mientras se está utilizando la aplicación "Ad", que se refiere a "advertisement" (anuncios) en idioma inglés.

- **Dialers:** Son programas maliciosos que toman el control del módem, realizan una llamada a un número de teléfono de tarificación especial, muchas veces internacional, y dejan la línea abierta cargando el costo de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos, salva pantallas, pornografía u otro tipo de material. Actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem, lo cual hace que los Dialers ya no sean tan populares como en el pasado.

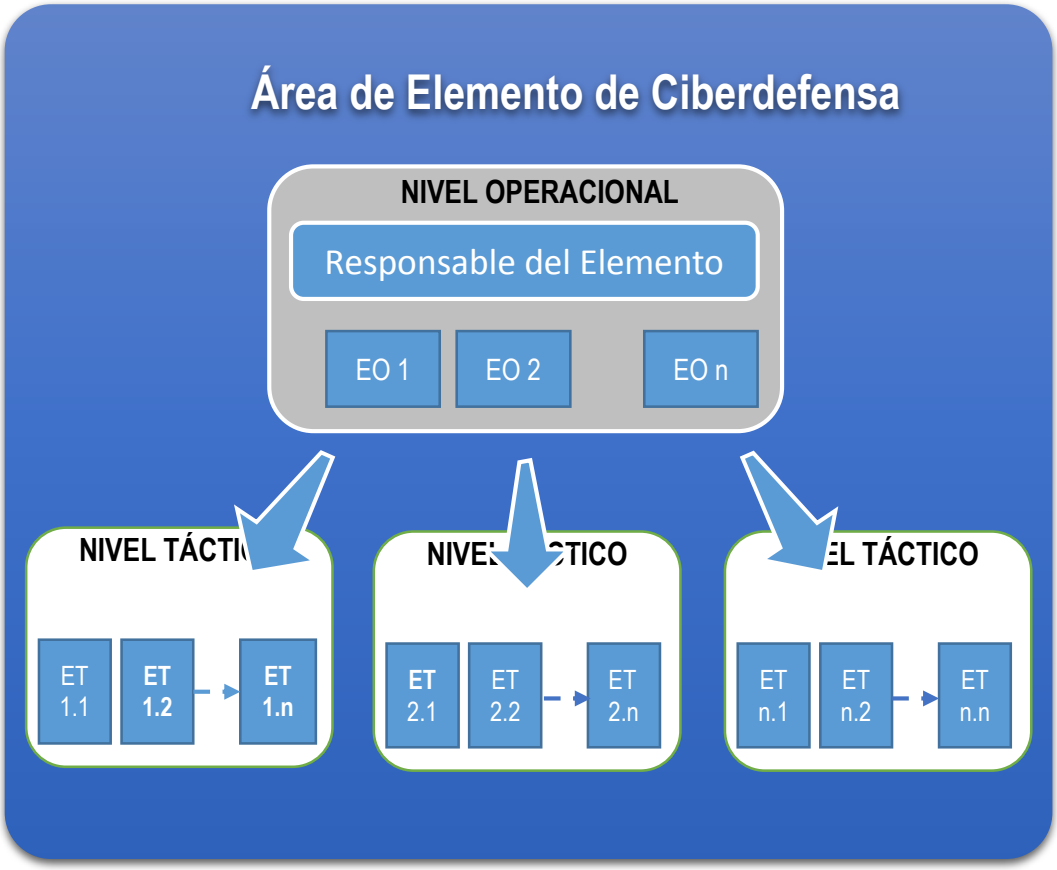
- **Spyware:** Son creados para recopilar información sobre las actividades realizadas por un usuario, obteniendo datos sobre los sitios web que visita, direcciones de email a las que después se envía spam. La mayoría de los programas son instalados como troyanos. Otros programas spyware recogen la información mediante cookies de terceros o barras de herramientas instaladas en navegadores web. Generalmente se presentan como programas que muestran publicidad o ventanas emergentes (pop-up) que son aceptadas de forma involuntaria, afectando los sistemas del usuario.

Anexo 3: Figuras

Fig 1: Modificación de Figura "Contextos externo e interno de las cibercélulas"[102]

[102] Guillem Colom Piella, José Ramón Coz Fernández, Enrique Fojón Chamorro y Adolfo Hernández Lorente; Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales; ARI 26/2013; Real Instituto Elcano; 4 de julio de 2013; p.4.

Fig. 2: Modificación de Figura "Organización de una cibercélula"[103]



[103] Guillem Colom Piella, José Ramón Coz Fernández, Enrique Fojón Chamorro y Adolfo Hernández Lorente; Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales; ARI 26/2013; Real Instituto Elcano; 4 de julio de 2013; p.9.

Anexo 4: Niveles de Fiabilidad

Niveles de Fiabilidad en Ciberdefensa

Se emplea el concepto de *Tier*[104] para indicar el nivel de fiabilidad de un centro de datos, existiendo cuatro niveles definidos:[105]

El Tier I, correspondiente a un Centro de datos Básico, tiene una disponibilidad del 99.671%, no cuenta con componentes redundantes en la distribución eléctrica y de refrigeración, su infraestructura estará fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparación.[106]

El Tier II se corresponde con un Centro de datos Redundante, su disponibilidad es del 99.741%, es menos susceptible que el anterior a interrupciones por actividades planeadas o no, tiene componentes redundantes, suelos elevados, generadores auxiliares, pero están conectados a una única línea de distribución eléctrica y de refrigeración y el mantenimiento de esta línea de distribución o de otras partes de la infraestructura requiere una interrupción del servicio.[107]

El Tier III, nivel para un Centro de datos Concurrentemente Mantenible, tiene una disponibilidad del 99.982%, permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas, tiene componentes redundantes, está conectado a múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa y hay suficiente capacidad y distribución para poder llevar a cabo tareas de mantenimiento en una línea mientras se da servicio por otras.[108]

El Tier IV, para un Centro de datos Tolerante a fallos, posee una disponibilidad del 99.995%, permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento dañino grave no planificado sin impacto crítico, también están conectados a múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes y duplica la

[104] Tier: su significado más próximo en español es grado o nivel.
[105] María Guilarte; "¿Qué es un Tier?"; *MC Pro*; Publicado el 14 de marzo de 2013; Recuperado el 23 de septiembre de 2015 de: http://www.muycomputerpro.com/
[106] Guilarte; *Ibíd*.
[107] Guilarte; *Ibíd*.
[108] OVH; "Niveles Tier"; *OVH.es*; Recuperado el 24 de septiembre de 2015 de: https://www.ovh.es/servidores_dedicados/niveles-tier-3-4.xml

redundancia de los anteriores[109], tienen dos procesadores que trabajan en simultaneo y permiten cambiar los discos sin interrumpir la operación.[110]

Hay que tener en cuenta que como se ha descripto anteriormente, a mayor número en el *Tier*, mayor disponibilidad y seguridad del sistema, teniendo como contrapartida los mayores costes asociados en su construcción y tiempo más prolongado para su construcción y puesta en funcionamiento. [111]

[109] Guilarte; *op.cit.*
[110] OVH; *op.cit.*
[111] Guilarte; *op.cit.*