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

TRABAJO FINAL INTEGRADOR

<u>Título</u>: "Organización Militar de Inteligencia como elemento de asesoramiento y asistencia a la toma de decisiones antes los ciberataques a nivel componente Ejército".

Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor DANIEL ANIBAL ESCRIBANO.

Director de TFI: Coronel (R) AGUSTO CAYO.

Ciudad Autónoma de Buenos Aires, 01 de noviembre de 2022.

Resumen

Teniendo en cuenta los avances tecnológicos y el incremento de la estructura digital, podríamos considerar que las mismas han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos, demandando mediante el uso de internet y de la conectividad digital una integración cada vez mayor de las tecnologías de la información y la comunicación (TIC).

Estas nuevas tecnologías y el fácil acceso a las mismas, posibilitan a cualquier ciudadano a conectarse y operar en el ciberespacio, en ocasiones de manera maliciosa ejecutando por ejemplo ciberespionaje, ciberataques, etc. Esto trajo aparejado nuevos riesgos y desafíos para la defensa nacional y es por ello que algunos países buscan la mejor forma de combatir estas nuevas amenazas.

Este trabajo de investigación tiene como objetivo ya que los incidentes y los ataques cibernéticos se han convertido en una fuente de amenaza en el mundo globalizado, analizar como BRASIL, CHILE, BOLIVIA, PARAGUAY y URUGUAY han incluido la problemática del ciberespacio a sus agendas de estrategia nacional, para posteriormente enfocarnos sobre las tácticas y procedimiento que se emplean en el ciberespacio destinados a cometer estos actos delictivos, en especial el robo de información, a los efectos de diseñar una organización de inteligencia que permita asesorar y asistir a lo que refiere en medidas de seguridad de contra inteligencia (MSCI), y la manera más eficiente de contrarrestar dichas coacciones con la finalidad de proteger la información digitalizada que administra el Ejército Argentino.

En esta pesquisa para poder arribar a una o varias conclusiones que permitan alcanzar la mejor solución, se estableció como objetivo general, determinar el concepto de empleo

y el equipamiento que debe poseer un elemento de inteligencia que se desempeñe como MSCI ante los ciberataques para operar en el ciberespacio.

Sobre la base del objetivo general se desarrollaron una serie de objetivos particulares que permiten alcanzar el propósito impuesto para esta investigación.

El primer objetivo tiene como objeto analizar las tácticas y procedimientos de empleo que utilizan BRASIL, CHILE, BOLIVIA, PARAGUAY y URUGUAY ante los ciberataques.

A continuación, el segundo objetivo busca determinar que técnicas y procedimientos se utilizan en el ciberespacio para comparar cuales pueden ser utilizados por los elementos de inteligencia teniendo en cuenta las normas legales del país.

Y para finalizar, el tercer objetivo hace referencia al equipamiento que debería emplear el elemento que se desempeñe como MSCI para cumplir con las exigencias que surgen del concepto de empleo que el nuevo conflicto impone dentro del ciberespacio.

Para poder desarrollar esta investigación, y teniendo en cuenta que no se posee doctrina alguna dentro de la fuerza, se procedió a reunir información de diferentes fuentes abiertas como ser: publicaciones, trabajos de investigación, informes periodísticos, informes de estado mayor de cursantes del Centro de Estudios de las Fuerzas Armadas (CEFFAA), actividades recientes y actuales de diferentes países que hacen frente a esta amenaza, y también se profundizo en cómo los ciberatacantes hacen uso de las herramientas tecnológicas para lograr cumplir sus objetivos, además se analizó el marco jurídico y legal determinado en nuestro territorio nacional para poder arribar a conclusiones de interés en la investigación.

Palabras Claves:

CIBERATAQUES –INTELIGENCIA – LEGALIDAD – CIBERESPACIO.

Introducción

Tema

Área de Investigación: Operaciones - Inteligencia Táctica- Conducción Táctica- Metodología para la toma de decisiones.

***Tema de Investigación*:** Apoyo de inteligencia al proceso de toma de decisiones en el marco de un conflicto hibrido.

Tema acotado: Organización Militar de Inteligencia como elemento de asesoramiento y asistencia a la toma de decisiones antes los ciberataques a nivel componente Ejército.

Problema

Antecedentes y Justificación del Problema*:*

El avance tecnológico de los medios que operan en el ciberespacio, convirtió a este en un nuevo escenario táctico, estratégico y operativo para diferentes actores (estatales y no estatales), y ante la aparición de este nuevo espacio emerge el termino conflicto híbrido, refiriéndose a las nuevas guerras del siglo XXI las cuales son muy complejas y dinámicas.

El término de conflicto híbrido es interpretado de diferentes maneras las cuales detallaremos a continuación:

"El conflicto hibrido, es una situación en la cual las partes se abstienen del uso abierto de la fuerza armada y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas" (LISA Institute, 2019, párr. 2).

"Los conflictos se caracterizan cada vez más por ser una híbrida conjunción de tácticas irregulares y tradicionales con planeamiento y ejecución descentralizados, donde estados y actores no estatales combinan tecnologías simples y sofisticadas en formas sumamente innovadoras" (González, 2016, p. 21).

El centro de gravedad de este tipo de guerra, es desestabilizar a otros Estados a través de diferentes tipos de estrategias, y entre las principales podemos citar los ciberataques, donde los objetivos de esta nueva amenaza se materializan en el robo de información y publicaciones cuya finalidad es influir en la sociedad ejecutando sabotajes cibernéticos en infraestructuras críticas.

Esta nueva modalidad de ataques es de preocupación mundial, ya que no hay fronteras claramente establecidas y el entorno de la seguridad cibernética es cada vez más compleja debido a que los avances tecnológicos y la creciente infraestructura digital, han acostumbrado a la población mundial a ser dependientes de esta nueva tecnología, incrementando las vulnerabilidades a los ciberataques teniendo en cuenta que el eslabón más frágil en todo sistema de seguridad es el humano.

Como ejemplo de esta nueva amenaza citaremos algunos antecedentes históricos de ciberataques que han repercutido a nivel mundial en el siglo XXI:

2007 –HACKERS atacaron las páginas de instituciones de Estonia, se acusó al servicio secreto ruso pero expertos estimaron que se realizó a nivel global.

2008 -Malware CONFICKER[1] , fue catalogado una amenaza a nivel militar, logro infectar departamentos de seguridad en todo el mundo como así también fuerzas armadas, hospitales y entidades privadas. Se calcula que infecto más de 10 millones de equipos en 190 países, entre ellos sistemas de buques de la armada y el parlamento de Reino Unido.

2009 –COREA DEL SUR, informó un ataque contra páginas institucionales y bancos del país.

[1] Malware CONFIKER: virus informático que explota una vulnerabilidad en el servidor de Windows. – página web panda segurity.

2010 -Malware STUXNET[2], llamo la atención de los investigadores de seguridad informática del todo el mundo. Se lo utilizó para atacar objetivos esenciales en IRÁN, fue considerado un arma cibernética para ser utilizado en actos de guerra, como una forma de atacar la infraestructura y los sistemas informáticos del enemigo. (esta amenaza informática ataco miles de sistemas informáticos en todo el mundo).

2011 –HACKERS violaron la red informática de RSA[3], obteniendo información sobre la tecnología SecurID que se utiliza para proteger redes de ordenadores en el mundo entero.

2012 –La empresa rusa KASPERSKY y la unión internacional de telecomunicaciones detectaron un programa maligno FLAME destinado a atacar instituciones públicas de IRÁN y otros países de oriente próximo probablemente desarrollado por servicios secretos de ESTADOS UNIDOS e ISRAEL.

2013 -La página oficial del presidente y el jefe del ejecutivo de SINGAPOUR fue vulnerada después de anunciar medidas contra el grupo de HACKERS ANONYMOUS.

2014 –Hackers del grupo CIBERBERKUT (creados después de la resolución de las fuerzas especiales ucranianas), bloquearon con un ataque DDoS por 24hs la página del presidente de UCRANIA.

2017 - ARGENTINA no estuvo exenta de este tipo de amenazas, un claro ejemplo es el ataque que recibió la página del Ejército Argentino.

2020 - FORTINET[4] anunció que se registraron 900 millones de intentos de ciberataques durante el año en el país y que es preocupante el grado de sofisticación y evidencia que están

[2] Malware STUXNET: virus informático que se dirige a los sistemas informáticos que utilizan operativos Windows – página web enigma Soft -

[3] RSA empresa que se dedica a la criptografía y al software de seguridad.

[4] FORTINET es una empresa multinacional de ESTADOS UNIDOS que se dedica al servicio de ciberseguridad. – página web fortinet.globalgate.com

logrando los delincuentes mediante el uso de tecnologías avanzadas e inteligencia artificial para lograr ataques con mayor posibilidades de éxito.

Ejércitos de diversos países han reconocido formalmente el ciberespacio como un nuevo dominio de enfrentamiento, el cual es crítico para el desarrollo de las operaciones militares.

La famosa frase “si utilizas al enemigo para derrotar al enemigo serás poderoso en cualquier lugar donde vayas” (Sun TZU, p.10), es la tendencia que ha ganado valor a lo largo del tiempo y en especial con el empleo del ciberespacio y los ciberataques, donde lo que se busca es poder derrotar al enemigo sin entrar en un conflicto armado, utilizando el engaño en su máximo esplendor.

Debido a la aparición de este nuevo escenario la ciberseguridad y la ciberdefensa son dos áreas que se han convertido para algunos gobiernos, como prioridad en sus agendas de defensa, principalmente debido al incremento del ciberespionaje.

La ciberseguridad es signo de la relevancia en el campo de las relaciones internacionales y es por eso que países en todo el mundo buscan formar alianzas informáticas con empresas privadas para poder combatir estas coacciones en el espacio virtual.

En el marco de la República Argentina, el termino ciberdefensa no es desconocido, pero a su vez es algo nuevo, inédito e inexplorado; el país en relación a este tema se encuentra atravesando un camino de búsqueda e innovación, ya que entiende que no está exento a estas nuevas amenazas, y es por ello que en el año 2019 se inauguró el centro nacional de ciberdefensa cuya tarea es garantizar la confidencialidad, integridad y disponibilidad de la información que circula por internet.

En el ámbito del Ejército Argentino el tema de ciberdefensa es aún más incierto y desconocido, no existe doctrina fehaciente para enfrentar dicha amenaza, en algunos

reglamentos de comunicaciones hace referencia solamente a la ciberdefensa como un mecanismo de protección de los medios.

En el marco extra regional de nuestro territorio nacional los países van tomando conciencia de dicha amenaza, creando organizaciones o bajando lineamientos referido a la ciberseguridad, algunos de ellos citaremos a continuación:

BRASIL: “Estrategia de Seguridad Cibernética 2020”. (DECRETO Nro 10.222, art 1) de República federativa del Brasil, donde establece la aprobación de la estrategia de seguridad cibernética el 5 de febrero del 2020.

URUGUAY: “Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional (d-csirt) 2015”. (DECRETO Nro 36/015. art 1) de la República Oriental del Uruguay en el cual instaura la creación de un Centro de Respuesta a Incidentes de Seguridad Informática en el Ministerio de Defensa Nacional, el que tendrá por visión ser el centro coordinador de todas las actividades relacionadas con la gestión de incidentes de seguridad informática.

CHILE: “Comité Interministerial Sobre Ciberseguridad 2015”. (DECRETO Nro 579, art 1) de la República de Chile, en el cual instituye la creación del Comité Interministerial sobre Ciberseguridad, de carácter permanente, y con una composición interministerial, cuya misión es proponer una política nacional de ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia.

BOLIVIA: “Centro de Gestión de Incidentes Informáticos 2015”. (DECRETO SUPREMO Nº 2.514, art 1) de la República de Bolivia en el cual establece la creación del Centro de Gestión de Incidentes Informáticos (CGII), cuya misión es proteger la información crítica del Estado y promover la conciencia de la seguridad para prevenir y responder a los incidentes de seguridad.

En el marco de la República Argentina, particularmente en nuestro Ejército Argentino se detalla lo siguiente:

"ROD–05-01 Conocimientos Básicos Sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza". detalla en forma muy general el empleo de la ciberdefensa en el ciberespacio mediante el empleo de acciones pasivas para su protección.

"Manual de Seguridad Informática". Básicamente el manual establece procedimientos, términos y definiciones, evaluaciones de riesgos y política de seguridad para la transición de datos.

"Orden Especial del Subjefe del Estado Mayor General del Ejército Nro 05/g/19". (2019) en donde establece la creación de una red técnica de Oficiales de Ciberdefensa, para instruir, asesorar y brindar apoyo técnico a fin de asegurar el libre acceso al ciberespacio de interés militar y brindar una respuesta adecuada ante incidentes, amenazas o ataques que puedan afectar a los activos e infraestructura crítica de la Fuerza.

"Directiva del Jefe del Estado Mayor General del Ejército Nro 918/18 (Régimen de funcionamiento del Subsistema Informático del Ejército - SUIE) (2018)" donde establece normas de procedimientos, instrucciones, estándares, funciones y políticas de seguridad que regirán el empleo del subsistema informático del Ejército Argentino y que serán de cumplimiento obligatorio para todos los usuarios.

"Directiva del Subjefe del Estado Mayor General del Ejército Nro (2020)" en la cual ofrece procedimientos generales que normen los aspectos de ciberdefensa en el ámbito de la Fuerza.

"Centro Nacional de Ciberdefensa". (Resolución 1380/2019. Art1) boletín oficial de la República Argentina instituye que se entiende por ciberdefensa a las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes

nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional.

Refiriéndonos al marco legal en el territorio argentino podemos mencionar:

“La Ley 25520 de Inteligencia Nacional”. que implanta las limitaciones que poseen los órganos de inteligencia de las fuerzas armadas las cuales quedan en claro, pero a fines de la investigación, no admite restricciones en lo relacionado a actividades de contra inteligencia ante nuevas amenazas.

“La Ley Nro 23554 de Defensa Nacional”. sancionada el 13 de abril de 1988 y promulgada el 26 de abril de 1988, en su título VI determina la organización territorial y movilización ante conflictos armados a los elementos de las fuerzas armadas, determinación así la zona de operaciones.

“Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”. (Resolución 580/2011. Art 1). Ministerio de justicia y derecho Humanos establece la creación del programa nacional de infraestructuras críticas de información y ciberseguridad en el ámbito de la oficina nacional de tecnologías de información de la subsecretaría de tecnologías de gestión de la secretaría de gabinete de la jefatura de gabinete de ministros.

Relacionado con trabajos realizados por personal militar podemos aludir:

“A Estrutura da Defesa Cibernética na República Argentina e na República Federativa do Brasil, Entre os Anos 2014 e 2019” um estudo comparado. ESG de Brasil, donde compara la ciberseguridad de los dos países (Luis Pablo Guimpel, pág. 30)

“Estructura y Capacidades de un Sistema de Inteligencia táctico en un Contexto de Guerra Híbrida”. TFI de la Escuela Superior de Guerra de la República Argentina, donde describe las conclusiones finales sobre la capacidad de adaptarse a los cambios que deben tener

los órganos de inteligencia durante el asesoramiento frente al conflicto hibrido" (Roveda, 2012, p. 49).

"De la Guerra Asimétrica a la Guerra Híbrida". TFI de la Escuela Superior de Guerra de la República Argentina donde detalla en sus conclusiones, que la guerra asimétrica como guerra híbrida son nuevas denominaciones para antiguas formas de conflicto, y que los avances tecnológicos en el campo de batalla son los principales responsables de haber producido el gran salto. (González G. Pág. 24)

Relacionado con documentos y artículos de revistas podemos enumerar:

"Ciberamenazas y Tendencias Sep 2020". donde establece métodos de ataques (Centro cristológico Nacional. Pág. 26)

"Ciberinteligencia Qué Es, Tipos Que Existen y Ejemplos Prácticos de Cómo se Aplica". donde describe que en el uso cotidiano de Internet y las tecnologías digitales las amenazas virtuales están a la orden del día, el peligro no está solamente ahí afuera, sino también en la red con datos e información confidencial que podría acabar en malas manos. (Julián Gutiérrez, párr. 3)

"Principios y Recomendaciones Básicas en Ciberseguridad" en el cual establece políticas de seguridad y manifiesta que el diseño de una estrategia de seguridad dentro de una organización depende en general de: la actividad que esta desarrolle, su dimensión, el ámbito de actuación y la interconexión con usuarios externos. (Centro cristológico Nacional. Pág. 39)

"Ciberseguridad una Estrategia Informático/Militar" en este libro el autor hace mención que la tercera guerra mundial será la ciberguerra y relaciona la operación militar convencional en el ciberespacio. (Alejandro Corletti Estrada. Pág. 58)

"Observatorio de la Seguridad de América Latina y el Caribe" es una página web que permite comparar y relacionar el estado de ciberseguridad de América Central y del SUR

Habiendo analizado y desarrollado los antecedentes para la presente investigación se exterioriza el problema asumiendo: la falta de información en la doctrina vigente, las limitaciones en el marco legal y la experiencia de otros países en este tipo de conflicto.

Formulación del problema

¿Cuál debe ser la organización de un elemento de inteligencia que opere en el ciberespacio para asesorar y asistir en la toma de decisiones ante los ciberataques a nivel componente Ejército?

Objetivo

Objetivo General:

Establecer una organización de inteligencia que pueda operar en el ciberespacio para asesorar y asistir en la toma de decisiones ante los ciberataques a nivel componente Ejército.

Objetivos Particulares:

Objetivo Particular Nro 1.

Analizar las políticas de ciberdefensa que utilizan los países de Brasil, Bolivia, Chile, Paraguay y Uruguay ante los ciberataques para comparar sus procedimientos.

Objetivo Particular Nro 2.

Analizar las tácticas y procedimientos de empleo que se utilizan en el ciberespacio, para comparar cuales pueden ser utilizados por los elementos de inteligencia para ser frente a las nuevas amenazas.

Objetivo Particular Nro 3.

Analizar el empleo de la inteligencia en el ciberespacio teniendo en cuenta las normas legales del país para cumplir con las exigencias que surgen del concepto de empleo que el nuevo conflicto impone.

Metodología a Emplear

Explicación del Método

El método que se empleará para la realización de la investigación será el deductivo. Además, se servirán de ciertos empleos de inferencias inductivas.

Diseño de la Investigación

Para la presente investigación se utilizará el diseño explicativo.

Técnicas de Validación

Las Técnicas de Validación a Emplear Serán.

Análisis bibliográfico.

Análisis lógico.

Capítulo I

Que políticas de ciberdefensa emplean los países de Brasil, Bolivia, Chile, Paraguay y Uruguay para enfrentar los ciberataques.

Las políticas de ciberseguridad son de gran importancia para salvaguardar los derechos de los habitantes en el espacio digital, permitiendo aumentar la confianza de los ciudadanos en el uso de la tecnología en este dominio, hay que tener en cuenta que identificar la amenaza cibernética es tan solo el primer paso, pero tomar medidas contra estas coacciones es un reto aún mayor.

Asumiendo lo anteriormente descripto en este capítulo desarrollaremos como las ciberamenazas afectan a los países que limitan con la Republica Argentina y que mecanismos de defensa utilizan estas naciones para protegerse de los mismos.

Por ultimo buscaremos obtener conclusiones concernientes a este tipo de operaciones y cómo inquieta la misma a los sistemas informáticos del Ejército Argentino.

Sección I

Políticas de ciberdefensa en Bolivia.

Bolivia haces unos años ha focalizado su atención en la plataforma digital y como mejorar su seguridad cibernética estableciendo normas y procedimientos que le permitan cumplir con el objetivo, en el año 2015 con el decreto supremo Nro 2.514, el estado boliviano crea la Agencia de Gobierno Electrónico y Tecnología de la Información y Comunicación (AGETIC), cuyo objetivo era implementar las técnicas de información de las comunicaciones en la gestión pública, y para proteger la información crítica del Estado que circula en el ciberespacio, crea el Centro de Gestión de Incidentes Informáticos (CGII) .

Posteriormente en el año 2016 crea el centro de seguridad y ciberdefensa el cual era operado por el Ejército Boliviano con la finalidad de contrarrestar los ataques cibernéticos de crackers o piratas informáticos hacia el estado y esto fue consecuencia a que entre el año 2015 y 2016 los portales de la armada boliviana, la policía y los ministerios de comunicación recibieron ciberataques de hackers chilenos.

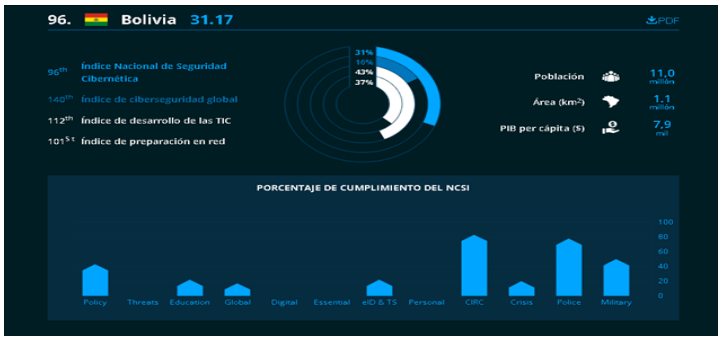
Bolivia para hacer frente estas amenazas, también forma parte del equipo de respuestas a incidentes (CSIRT)[5] Américas desarrollado por la OEA, por el cual intercambia información para poder hacer frente a estas nuevas contingencias.

A pesar de lo anteriormente descripto Bolivia no cuenta con una legislación específica sobre los delitos informáticos, y hace participe al sector privado para contribuir con la ciberseguridad y ciberdefensa aprovechando de los mismos la ciberinteligencia, una de esas compañías que podríamos citar es Data Total Security (DTS) que, en el primer semestre del año 2020 ha detectado para el Estado boliviano abundantes vulnerabilidades en el sistema de ciberseguridad y ciberdefensa derivado por la falta de buenas prácticas. La participación de estas empresas no solo es identificar ciberamenaza, sino que también desarrollar programas que permita alertar de futuros sucesos delictivos.

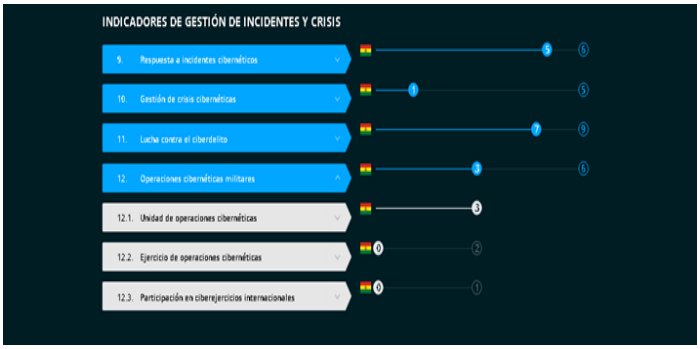
Estudios proporcionados por National Cibersecurity Index (NCSI)[6] establece que Bolivia en lo relacionado a la ciberseguridad y ciberdefensa se ubica en el puesto 96, ocupando uno de los últimos lugares en América Latina.

[5] Centro de Respuesta a Incidentes en Seguridad Informática (CSIRT) Américas es un hub de coordinación de incidentes de ciberseguridad en los países de América Latina y el Caribe.

[6] National cyber security índex (NCSI) es una base de dato un índice global que mide la preparación de los países para prevenir amenazas cibernéticas.



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021

Sección II

Políticas de Ciberdefensa en Brasil.

Ante el incremento de los ciberataques en el mundo, el gobierno de Brasil en el año 2011 creo el Centro de Defensa Cibernética (CDCIBER) con el objetivo de proteger los sistemas informáticos militares y gubernamentales como así también infraestructuras críticas que, de verse comprometidas causarían daños públicos irreparables. Este centro posee laboratorios de simulación y ciberguerra y está dirigido por personal de oficiales del Ejército, la Fuerza Aérea y la Marina.

En el año 2012, el gobierno brasilero en su libro blanco de defensa nacional, en su apartado relacionado con el sector cibernético otorgó la responsabilidad de la seguridad cibernética al Ejército Brasilero, el cual estaría a cargo de la coordinación de todas las

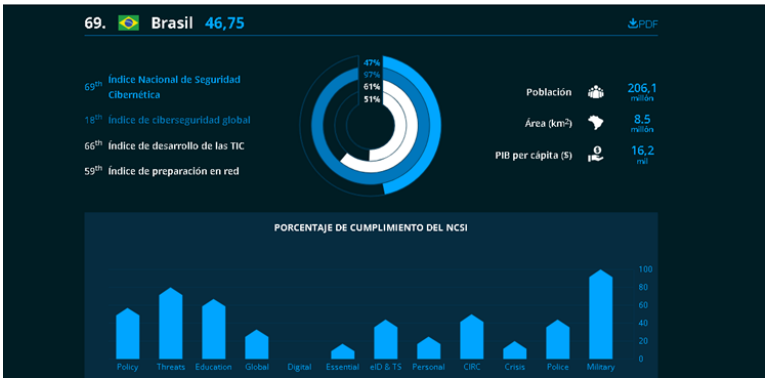
actividades que se desarrollan sobre la materia, como ser capacitación, inteligencia, investigación científica, doctrina, preparación y uso operativo y gestión de personal.

En el año 2019 inauguró la Escuela Nacional de Defensa Cibernética (ENaDCiber), con la misión de fomentar y diseminar las capacidades necesarias para la defensa cibernética en el ámbito de la Defensa Nacional, esta institución entrena y capacita al personal de la fuerza para investigar en inteligencia, seguridad cibernética y criptografía.

El 5 de febrero de 2020, Brasil publicó el decreto federal Nro 10.222 donde se aprueba la estrategia nacional de ciberseguridad con el objetivo de aumentar su resistencia a las amenazas cibernéticas y fortalecerse a nivel internacional, además estableció un consejo nacional de ciberseguridad, donde diferentes actores que se dedican en esta área trabajen en forma coordinada para hacer frente a estas amenazas.

En Brasil todas las instituciones federales deben realizar evaluaciones de riesgo cibernético los cuales se actualizan anualmente, existen políticas y procedimientos bien definidos que deben seguir todas las instituciones públicas en función a la información brindada por el Centro de Estudios, Respuestas y tratamiento de Incidentes de seguridad de Brasil (CERT.br).

La National Cibersecurity Index (NCSI) instaura que Brasil en lo relacionado a ciberdefensa y ciberseguridad se ubica en el puesto 69 en América Latina.



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021

Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021

Sección III

Políticas de ciberdefensa en Chile.

La ciberdefensa para Estado chileno es un problema a nivel nacional y por tal motivo el gobierno chileno crea el comité interministerial de ciberseguridad, el cual tiene la misión de asesorar en la coordinación de acciones, planes y programas en materia de seguridad, conforme a lo establecido en el Decreto Supremo Nro 533, de 27 de abril de 2015.

En el año 2017 CHILE presentó su estrategia nacional de seguridad cibernética que contaba con los siguientes objetivos: tener una infraestructura de información sólida y resilientes, desarrollar una estrategia de seguridad cibernética, establecimiento en relaciones de cooperación de seguridad cibernética con otros actores y promover el desarrollo de una industria de seguridad cibernética a fin de cumplir sus objetivos estratégicos. la idea es alcanzar los objetivos impuestos en el año 2022.

El actual Gobierno del presidente Sebastián Piñera en el año 2019 decidió separar las competencias propias de la ciberdefensa dejándolas en mano del Ministerio de Defensa, la ciberseguridad pasan a ser asumidas por el ministerio del interior y la

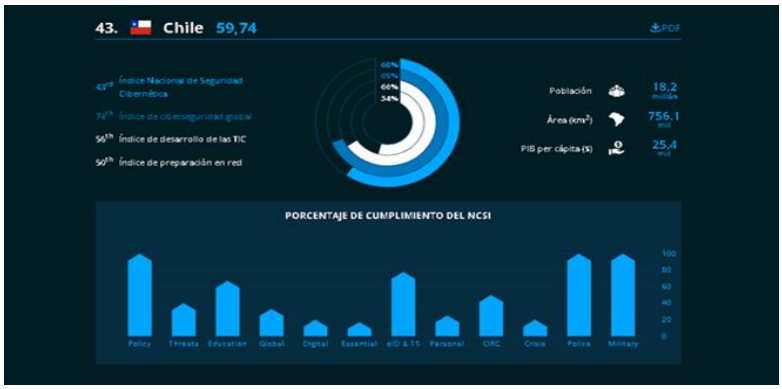
ciberinteligencia desde la óptica de la Agencia Nacional de Inteligencia (ANI), cabe destacar que todas están coordinadas por el comité interministerial de ciberseguridad, el cual menciono como desafíos la atribución de responsabilidades en el ciberespacio y una vinculación más estrecha con el sistema de inteligencia nacional orientada al análisis de riesgos y amenazas.

Algunas de las prioridades estratégicas que posee el actual gobierno con respecto a la ciberdefensa es: la renovación de los equipos de respuesta ante emergencias informáticas, la optimización de los sistemas de autocontrol, la tramitación de leyes alusivas al tratamiento de datos personales, la tipificación de nuevos delitos informáticos e infraestructuras críticas, contar con profesionales entrenados en laboratorios de análisis de códigos maliciosos y hacer análisis de inteligencia sobre la DEEP WE .

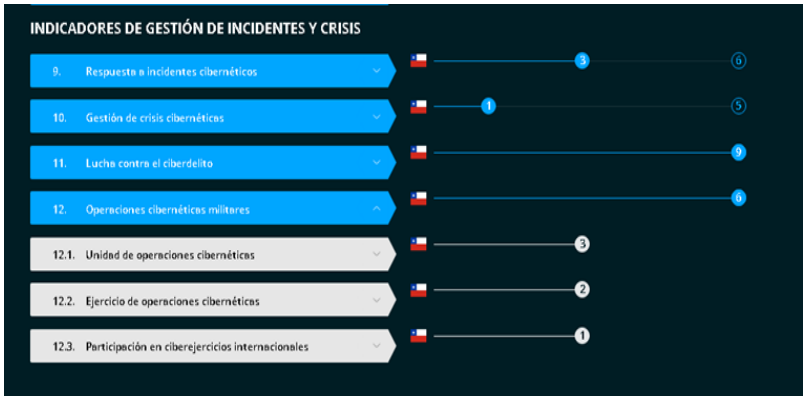
En él años 2020 se buscó fortalecer y modernizar el Sistema de Inteligencia del Estado (SIE).

Con respecto a las FFAA chilenas se creó el comando conjunto de ciberdefensa bajo el comando del JEMCO responsable del planeamiento y ejecución de las operaciones militares conjuntas de ciberdefensa, cabe subrayar que las FFAA ya han participado de ejercicios cibernéticos en el país, como así también fuera del mismo. Cada componente de las FFAA posee un equipo de respuestas a incidentes informáticos (CSIRT) los cuales operan en forma coordinada con el CSIRT de la defensa nacional.

Para la National Cibersecurity Index (NCSI) instituye que Chile se ubica en el puesto 43 en lo relacionado a ciberdefensa en América Latina.



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021

Sección IV

Políticas de ciberdefensa en Paraguay.

En el año 2017 el Gobierno de Paraguay aprobó su plan nacional de ciberdefensa e íntegro su comisión de ciberseguridad con representantes de distintas instituciones públicas, con el objetivo de garantizar y promover el uso seguro y confiable de las técnicas de comunicación de información (TIC).

Como parte de la Convención de Budapest a la que se adhirió en el año 2017 mediante la Ley Nro 5994/17, el país es beneficiario del programa Acción Global contra

la Ciberdelincuencia Extendida con el objetivo de compartir estrategias legislativas contra el ciberdelito.

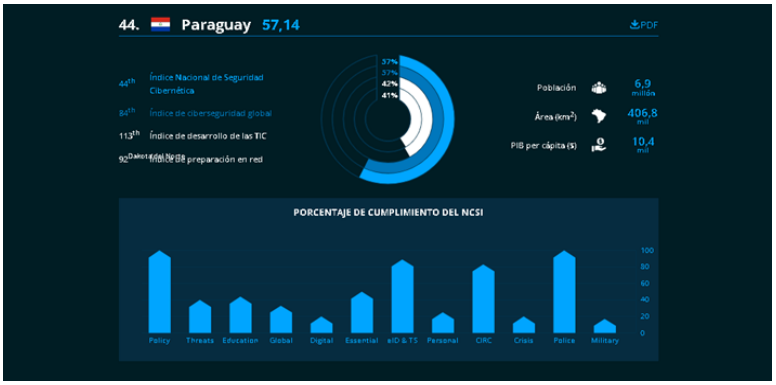
En el año 2018 el Banco Interamericano de Desarrollo (BID), aprobó un programa de apoyo a la agenda digital con el objetivo de incrementar las capacidades cibernéticas de Paraguay y asegurar el fortalecimiento del marco nacional de ciberseguridad, cabe recalcar que CSIRT de Paraguay es miembro de la red CSIRT americanas; y que el sector privado trabaja en cooperación con el sector público en la protección de la infraestructura críticas del país. En el corriente año también se creó el Ministerio de Tecnología de la Información y Comunicación (MITIC) cuyo objetivo es la protección de la información ejerciendo la autoridad en ciberseguridad, prevención, gestión y control de incidentes cibernéticos, ideando planes estratégicos de ciberseguridad a nivel nacional.

Desde el 2019 atendiendo estas problemáticas el Ministerio de Defensa implemento un programa de especialización en ciberdefensa y ciberseguridad estratégica, para capacitar a su personal en la lucha contra las nuevas amenazas que operan en el ciberespacio.

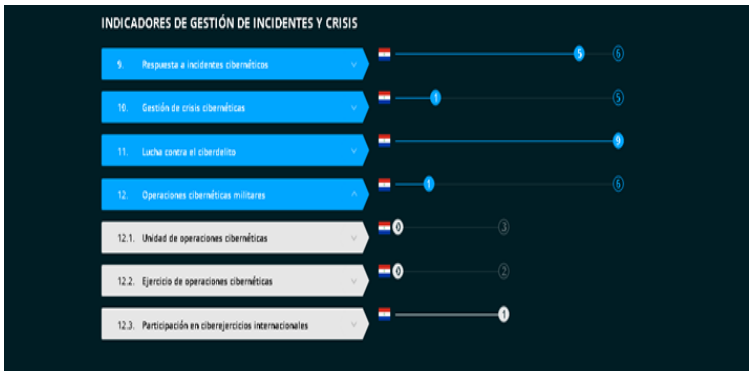
Paraguay posee un Comité de Coordinación e Interoperabilidad para el Gobierno Electrónico (CCIGE) el cual mediante la Secretaria Nacional de Tecnología de la Información y comunicación (SENATICs) se encargan de consumar los principios y fines de la tecnología de la información y comunicación en el sector público.

De acuerdo al análisis de la NCSI las principales debilidades que posee Paraguay es en las operaciones en el ámbito militar y sus mayores fortalezas esta relacionadas con el cibercrimen, este país se apoya en lo que refiere a la ciberinteligencia con organizaciones del sector privado como así también con ciberinteligencia de otros países, pero más orientado al cibercrimen.

Según la National Cibersecurity Index (NCSI) Paraguay se ubica en el puesto 44 en lo relacionado a ciberdefensa y ciberseguridad en América Latina y esto se debe a su gran capacidad de reacción a los cibercrimen informáticos.



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021

Sección V

Políticas de ciberdefensa en Uruguay.

En el año 2017 Uruguay, sobre la base del ciberataque a nivel mundial por el virus Ransower[7], tomo medidas preventivas con respecto a la seguridad informática del país, sobre diversas instituciones incluido el Ministerio de Defensa, y es por ello que este ministerio dispone desde el 2015 un Equipo de Respuestas a Incidentes de Seguridad

[7] Ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado.

Informática de Defensa (D-CSIRT) , siendo el primer centro creado en el ámbito de la Defensa Nacional para dedicarse a la ciberdefensa y a la protección de infraestructuras críticas y servicios esenciales del país, trabajando en forma coordinada con el CERTuy el cual es miembro del CSIRT Américas.

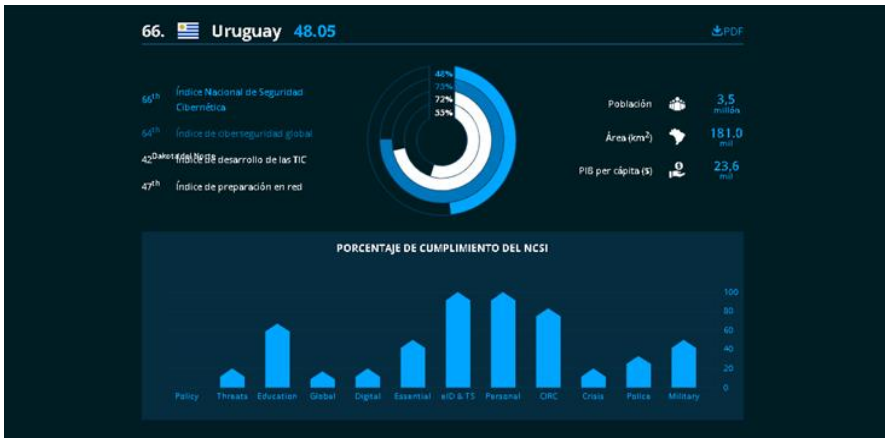
El D-CSIRT también integra otras redes de equipos de respuestas a incidentes como ser, Comité Interamericano Contra el Terrorismo (CICTE), la Organización de Estados Americanos (OEA) y la Unión de Naciones Suramericanas(UNASUR).

A través del proyecto Fortalecimiento de la ciberseguridad en Uruguay, este país fue el primero en la región en acceder con apoyo técnico y financiero por el banco Interamericano de Desarrollo, con el objetivo de robustecer la ciberseguridad a nivel nacional, cabe destacar que el Estado uruguayo también posee algunos proveedores de seguridad cibernética del sector privado los cuales brindan asistencia técnica y ciberinteligencia para detectar nuevas amenazas.

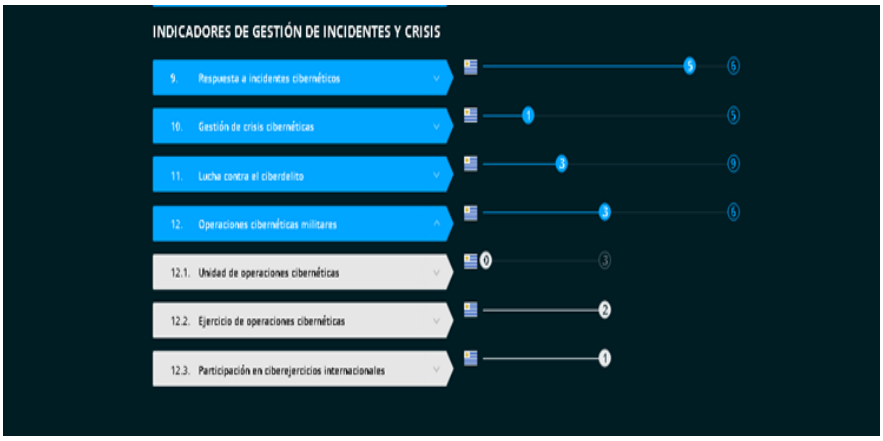
Con respecto a la parte legal Uruguay posee algunos proyectos de ley sobre delitos cibernéticos enfocados en enjuiciar los mismos una vez que son comprobados, también posee normas que protegen datos personales y la privacidad de los ciudadanos de acuerdo a la Ley 18.331, que aplica en el sector privado y público.

Aspecto a resaltar es que, en enero del año 2021, la base de datos del Ejército de Uruguay recibió un ciberataque de Ransoware, el cual bloqueo el acceso al sistema informático de la institución seguido del robo de información sensible.

Al igual que Paraguay el análisis de la NCSI, muestra debilidades en las operaciones en el ámbito militar y sus mayores fortalezas en las operaciones relacionadas con el cibercrimen.



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021



Fuente: Gráfico de sitio web del National *Cyber* Security Index (NCSI) 2021

Conclusiones parciales del capítulo I

En el presente capítulo, se ha analizado como los países que limitan con la República Argentina hacen frente a las nuevas amenazas, de ese estudio resulta que estos Estados enfrentan un escenario complejo, dinámico y volátil, donde el grado de incertidumbre es elevado, la ausencia de doctrina sobre este tema en la región hace que estas naciones operen en forma interagencial ya sea con organizaciones privadas o con otros estados, compartiendo información con la finalidad de contrarrestar estas amenazas, un claro ejemplo de esto es que todos los países analizados forman parte del CSIRT Américas.

Otro aspecto relevante es la política de defensa, muy bien marcada donde algunos países se inclinan más hacia la ciberdelincuencia y otros hacia la ciberdefensa mediante el empleo militar, y esto se vio materializado en los informes emitidos por la NCSI, dejando en evidencia las vulnerabilidades y fortaleza que poseen cada país observado.

Por último, es el empleo de la inteligencia en el ciberespacio, sobre este tema se pudo apreciar que todos los estados, se enfocan en prevenir estas ciberamenazas sobre sistemas de alertas que permitan anticiparse a los hechos con el objetivo de proteger la información y sus infraestructuras críticas. Sobre este aspecto se evaluó que hay naciones que buscan independizarse tecnológicamente con la finalidad de establecer su propio sistema de ciberinteligencia, y otros que están sujetos a organizaciones privadas o naciones amigas que le brinden este servicio.

Capítulo II

Tácticas y procedimientos de empleo que se utilizan en el ciberespacio

En este capítulo se buscará estudiar que tácticas y procedimientos utilizan los ciberatacantes en el cibespacio, pero primero debemos conocer las características que posee este nuevo ambiente donde se desenvuelven las ciberguerras, para lo cual y para poder desarrollar una buena pesquisa, este capítulo fue dividido en tres secciones.

La primera sección enfocada en asimilar el termino de ciberespacio, sus características, sus fronteras y todo aspecto de interés que permita a los ciberatacantes poder desenvolverse en este ambiente. Posteriormente en la segunda sección haremos referencia a quienes operan en el ciberespacio y que peculiaridades poseen en función a como se desenvuelven dentro de este nuevo escenario.

En la tercera sección y para finalizar la pesquisa de este capítulo, estudiaremos las tácticas y procedimientos que ejecutan los diferentes entes que despliegan en el ciberespacio, ya sea para obtener información o para la destrucción de infraestructuras críticas.

Sección I

El ciberespacio.

En el año 1984 en una novela de William Gibson[8] llamada Neuramente, aparece por primera vez la palabra ciberespacio que básicamente suponía un espacio virtual creado por las redes informáticas.

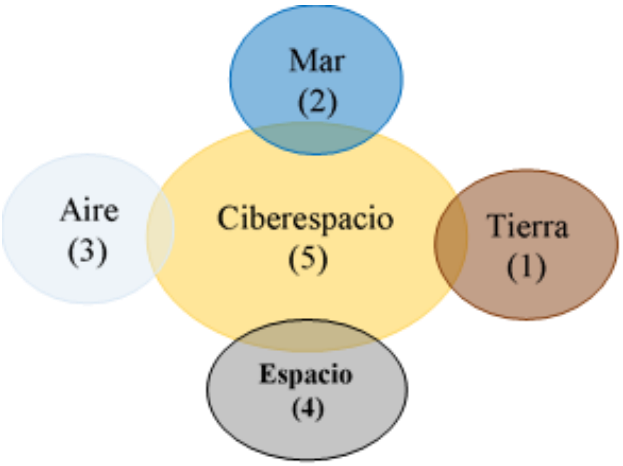
Actualmente hablar del ciberespacio continúa siendo algo relativamente nuevo a

[8] William Ford Gibson es un escritor de ciencia ficción estadounidense precursor del genero cyberpunk.

nivel global, algunos individuos lo denominan como una realidad aumentada de construcción digital desarrollado por computadoras y que no es algo físico que se puede tocar, otros lo asocian directamente con todo aquello que se concibe en internet a través de los sitios web, correos electrónicos, etc., podríamos decir que utilizan este término como sinónimo de internet, o bien que Internet está dentro del ciberespacio.

Como todavía no hay algo claramente establecido sobre este nuevo ambiente, el termino de ciberespacio tiene varias definiciones, por ejemplo, para la real academia española es un espacio virtual creado con medios cibernéticos y para el diccionario informático es el espacio virtual determinado por la conexión de personas a través de redes.

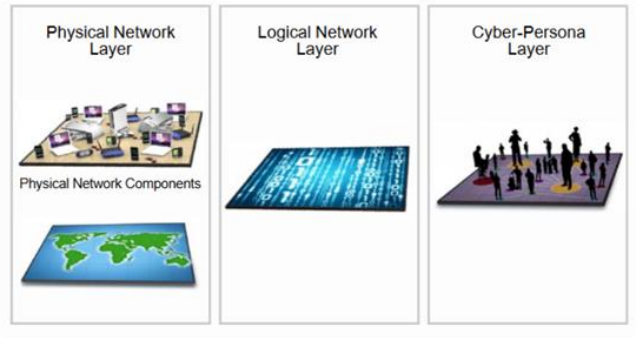
El ciberespacio es también considerado para los países como un nuevo dominio donde se desenvuelven las ciberguerras, definiéndolo como un campo de operaciones militares al igual que la tierra, el aire, el mar y el espacio, pero sujeto a ser un escenario donde se desarrollen operaciones castrenses cibernéticas.



Fuente: Gráfico elaboración propia

Haciendo referencia a las características de este nuevo ambiente, el ejército de los Estados Unidos, divide al ciberespacio en tres capas, red física, red lógica y por ultimo

las ciberpersonas las cuales permiten disociar los datos de las otras capas con el fin de representar un actor.



Fuente: Gráfico de sitio web Pralogy[9] 2018

La primera capa (red física) constituida básicamente por dispositivos e infraestructuras de tecnología de información, es donde los datos binarios de los usuarios son almacenados procesados y transferidos, aspecto a resaltar sobre esta capa es que requiere mucha seguridad física ya que aquel que logra acceder a la misma también tiene acceso a la capa de la red lógica. Si bien esta primera capa permite ubicar geográficamente a un actor en la red, el ciberespacio al no poder definir fácilmente sus fronteras físicas, geográficas y políticas dificulta poder concretar regulaciones y legislaciones estrictas en este ambiente.

La segunda capa (red lógica) materializa todas aquellas interconexiones que se realizan en el ciberespacio pero que no están rectamente asociadas y/o vinculadas en el dominio físico.

La tercera capa (ciberpersonas) permite desarrollar representaciones digitales de la identidad de un actor o entidad en el ciberespacio.

[9] Pralogy es una compañía dedicada a la investigación y desarrollo de productos en el campo de la ciberseguridad.

Habiendo analizado el termino de ciberespacio y sus características, podríamos definirlo como un ambiente artificial, imperceptible, dinámico y que posee fronteras poco definidas, características que dificultan a nivel mundial establecer normas claras que permitan regular todo lo que se desarrolla en él.

Sección II

Entes que manipulan el ciberespacio.

El avance tecnológico y el fácil acceso al mismo, ha permitido que gran variedad de organizaciones e individuos interactúen en este nuevo ambiente, ejerciendo diferentes grados de influencia en cualquier parte del planeta.

Los que maniobran dentro de este nuevo escenario lo hacen con un determinado objetivo, como ser: negocios, interactuar con personas, fines benignos o maliciosos, finalidades militares (ejecutar operaciones militares cibernéticas), fines políticos, etc, podríamos seguir enumerando infinitas actividades que se pueden desarrollar en este nuevo ambiente dado que es multidimensional y no posee fronteras claramente definidas.

Teniendo en cuenta la finalidad de esta investigación a continuación solamente citaremos y desarrollaremos aquellos sujetos que por su desempeño dentro de este contexto pueden afectar y/o proteger información sensible de un país o afectar sus infraestructuras críticas, como ser:

Los Ciberusuarios: aquellos que se conectan al ciberespacio por medio del uso

de internet ya sea, desde sus hogares, lugar de trabajo, institutos educativos o desde otro lugar con el objetivo de obtener información para satisfacer sus propias necesidades o

interactuar con otros usuarios. Estos individuos son los que poseen poco conocimiento de informática y como desenvolverse en este ambiente y es por ello que son los entes más vulnerables del sistema y los más buscados por los ciberatacantes para poder acceder a una infraestructura critica o como enlaces para obtener información.

Los Ciberatacantes: usuarios con mayor conocimiento sobre el uso del ciberespacio cuyo objetivo es el robo de información mediante el acceso no autorizado, destrucción de los sistemas de información y telecomunicaciones o de las infraestructuras que los soportan, cabe destacar que no todos estos individuos realizan ataques maliciosos sino que algunos contribuyen con las fuerzas de seguridad o estatal para detener ciberdelincuentes, para proteger información sensible y/o salvaguardar infraestructuras críticas. Estos ciberatacantes se clasifican en tres tipos los cuales desarrollaremos a continuación:

Los Black Hat: llamados también ciberdelincuentes, su objetivo es acceder a sistemas o redes con la finalidad de infringir daño, obtener información, robar contraseñas e introducir virus; dentro de esta clasificación podemos encontrar una división, los Crackers que se dedican a modificar software, crear malware, colapsar los servidores e infectar las redes, y por otro lado los Phreakers que actúan en el ámbito de las telecomunicaciones.

Los Grey Hat: estos hackers prestan servicio a agencias de inteligencia, a los gobiernos y grandes empresas obteniendo información de utilidad.

Los White Hat: conocidos también como Hacker Éticos, su objetivo es investigar y notificar vulnerabilidades o fallos en los sistemas de seguridad.

Para finalizar esta sección citaremos a los estados que también son entes que maniobran dentro del ciberespacio con la finalidad de proteger sus infraestructuras críticas y la información sensible de su país como la de sus habitantes, esto lo logra mediante el empleo de la seguridad informática, ciberseguridad y la ciberdefensa las cuales están a cargo de las Fuerzas de Seguridad y las Fuerzas Armadas de cada país.

Sección III

Tácticas y procedimientos que se explotan en el ciberespacio.

Dentro del ciberespacio existen diferentes procedimientos que ejecutan los ciberataques para modificar las características de un sistema y explotar sus vulnerabilidades, y es por ello que es importante conocer algunas tácticas u operaciones que emplean los ciberdelincuentes para lograr cumplir sus objetivos; para lo cual y siguiendo el lineamiento de esta pesquisa a continuación desarrollaremos las 5 técnicas más utilizadas por los hackers:

Keylogger: es un software que registra la actividad del teclado en un archivo de registro, con este programa se puede obtener información de los ID y contraseña de cualquier aplicación que el operador acceda. Este software puede ser instalado en un ordenador mediante el empleo de acceso virtual o empleando un pendrive con un archivo autoejecutable, que una vez conectado a la computadora ejecuta este programa.

WAP[10] Falso: es uno de los ataques más fáciles de ejecutar y se necesita un simple software y una red inalámbrica, y esto se logra cuando este WAP se

[10] WAP (Wireless Application protocol) es un estándar técnico para acceder a la información a través de una red inalámbrica.

vincula a un lugar público y una vez que la víctima se conecta el ciberatacante accede a sus datos.

Pishing: es una técnica de piratería por la cual el hacker imita sitios más accesibles en la red y atrapa a su víctima enviando enlaces falsos, esto se consigue mediante la ingeniería social[11] y es uno de los ataques más usados y letal.

Virus y Troyanos: son software malicioso, que una vez instalados en el ordenador de la víctima pueden bloquear archivos, desviar tráficos y husmear los datos del equipo, este programa envía continuamente datos al ciberdelincuente

Denegación del Servicio (DDOS): es una técnica para derrumbar un sitio o servidor inundándolo con mucho tráfico, con el objetivo de que no se puedan procesar todas las solicitudes en tiempo real.

Las fuerzas armadas también ejecutan operaciones militares en el ciberespacio dentro del marco de la ciberdefensa, y esas operaciones de dividen en:

Operaciones Defensivas (MDI): que son un conjunto de acciones y medidas defensivas cuyo objetivo es proteger la infraestructura crítica mediante la detección, identificación, interceptación, neutralización y rechazo de todo tipo de ataque y/o penetración en el AOCD.

Operaciones Ofensivas: son acciones destinadas contra posibles adversarios para afectar la integridad y disponibilidad de sus sistemas de información y telecomunicaciones.

[11] Ingeniería Social es una técnica utilizada para obtener información confidencial a través de la manipulación de usuarios legítimos.

Operaciones de Vigilancia y Reconocimiento: son todas aquellas acciones que tienen como objetivo la obtención, análisis y aprovechamiento de la información sobre las capacidades del ciberadversario. Comúnmente este tipo de operación lo desarrollan los elementos de inteligencia cibernética.

Fuente: Gráfico sitio web XIII Jornadas STIC CCN – CERT 2002

Conclusiones parciales del capítulo II

Habiendo analizado las tres secciones de este capítulo, podemos inferir que el ciberespacio es complejo, dinámico y volátil, que evoluciona rápidamente debido al avance tecnológico de las TIC, y que también es el único dominio donde el agresor puede estar en cualquier parte del mundo ejecutando diversos tipos de ataques en diferentes direcciones del planeta, a esto hay que agregarle que no posee fronteras claramente definidas lo que dificulta establecer normas que regulen las actividades que se desarrollan dentro de este ambiente.

La gran cantidad de actores, con intereses claramente definidos, vuelve a este ambiente en un entorno caótico, donde prevalece la incertidumbre fruto a los vacíos de información, ahora podemos comprender la necesidad de formar parte del CSIRT

Américas que tenían los países analizados en el Capítulo I, cuyo objetivo es intercambiar información sobre estas nuevas amenazas, y eso se debe a que para poder sobrevivir en este tipo de hábitat es fundamental mantener gran flujo de información confiable, debido a la codicioso que es este ambiente.

El ciberespacio no es un escenario netamente virtual, ya que como hemos visto en la Sección I, posee tres capas de las cuales dos son tangibles (capa física y capa de las ciberpersonas), que pueden ser atacadas sin penetrar a la capa lógica ocasionando un daño importante al sistema; que se quiere expresar con esto que los ciberataques no solo emplean la capa lógica, sino que también pueden afectar la capa física de manera tangible, como por ejemplo empleando elementos de inteligencia o de fuerzas especiales que puedan sabotear la misma.

Capítulo III

El empleo de los elementos de Inteligencia en el ciberespacio y las limitaciones legales que tienen estos elementos en Argentina.

En los capítulos I y II hemos observado la complejidad que presenta el ciberespacio y la gran ausencia de información que existe en el mismo prevaleciendo la incertidumbre. Este entorno complejo que carece de información nos ha demostrado como afecta negativamente a los países que limitan con la Argentina, y como estas naciones se vieron obligadas a formar alianzas o depender de los elementos de inteligencia de organizaciones privadas y de estados aliados para poder sobrevivir en esta habitad

Por todo lo anteriormente expresado es que en este capítulo estudiaremos la necesidad de poseer un elemento de inteligencia que facilite obtener información de los atacantes dentro del ciberespacio, con la finalidad de poder alertarnos de futuras amenazas o simplemente proteger la información sensible mediante el empleo de medidas de seguridad de contra inteligencia, respetando las normas legales que limitan el empleo de estos elementos.

Es por ello que este Apartado se dividió en dos Secciones, en la primera desarrollaremos la ciberinteligencia y su importancia para desenvolverse en el ciberespacio, y en la segunda sección nos referiremos a las normas legales impuestas en Argentina para determinar que limitaciones poseen los elementos de inteligencia para actuar en este nuevo espacio.

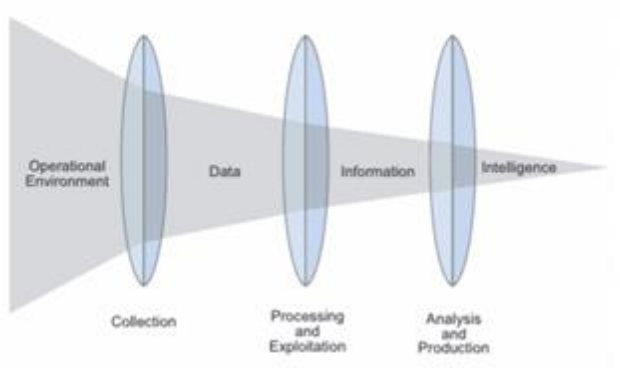
Sección I

La Inteligencia en el ciberespacio.

Como hemos apreciado en capítulos anteriores, el ciberatacante puede encontrarse en cualquier parte del planeta, y ejecutar acciones ofensivas en forma simultánea en varias direcciones del globo; poder localizarlo puede llevar meses, pero si se lo logra identificar hay que tener en cuenta que este ciberatacante puede ser parte de un Estado, de una organización Militar y/o un simple Ciberusuario (hacker).

Ante el incremento de estos ciberatacantes y la escasa información existente, las organizaciones privadas, los Estados y sus las Fuerzas armadas, han optado por implementar el uso de la inteligencia en este nuevo escenario a la cual se la denomino ciberinteligencia, cuyo objetivo es ayudar a gestionar estos riesgos y articular una serie de estrategias que permitan detener, prevenir, defender, analizar e investigar cualquier accionar ofensivo, ejecutado por estos ciberatacante.

Ahora bien, en este nuevo espacio no hay que confundir, datos con información e información con inteligencia, porque normalmente los datos en esta habitad se encuentran en forma desorganizada y en grandes volúmenes de disponibilidad; para que estos se conviertan en información se los debe seleccionar, organizar y analizar. Una vez obtenida la información, esta pasa por otro proceso de análisis e interpretación y es ahí donde se produce la inteligencia.



Fuente: Gráfico de sitio web ciberseguridad. Blog - 2018

Antes de continuar, sería conveniente definir que es la ciberinteligencia, y después de haber analizado diferentes conceptos concluimos que ciberinteligencia es un proceso de obtención y análisis de información dentro del ciberespacio, para localizar y predecir capacidades, intenciones y acciones cibernéticas que ejecuta el ciberatacante, con la finalidad de apoyar la toma de decisiones.

A diferencia con la inteligencia tradicional, este nuevo dominio demanda analistas con conocimientos técnicos sobre la estructura de este nuevo ambiente y el modus operandi de los actores con los que se va a encontrar en el ciberespacio, este nuevo enfoque implica que los analistas de ciberinteligencia además de tener conocimiento de la inteligencia tradicional, sus herramientas y técnicas habituales; también deben conocer el contexto del ciberespacio con especial énfasis en la ciberseguridad.

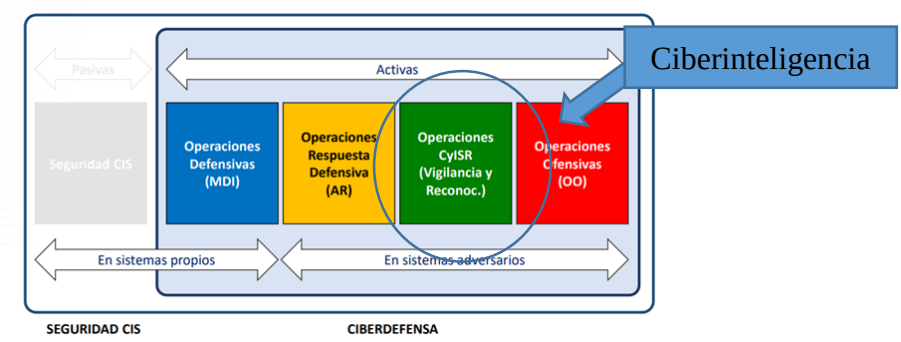
La ciberinteligencia es de gran importancia en el ciberespacio porque permite prevenir futuros ataques y/o daños, gracias al rastro de información suministrada del atacante al momento de realizar la acción, como ser, su infraestructura, sus herramientas o simplemente sus tácticas y procedimientos para desarrollar el ataque. La ciberinteligencia también puede obtener la cantidad de información que fue extraída en la organización a fin de llevar a cabo una evaluación de daño.

La inteligencia empleada en el ciberespacio permite, disponer de un sistema predictivo de alertas ante futuros ataques, monitorear y neutralizar futuras amenazas y mejorar el proceso de la toma de decisiones mediante la reducción de la incertidumbre.

Dependiendo de su alcance o nivel de acción puede ser estratégica, operacional o táctica, cuando nos referimos a la inteligencia estratégica por lo general es la que examina las tendencias de las amenazas actuales y emergentes y analiza oportunidades para contenerlas; cuando hacemos referencia a la ciberinteligancia operacional consiste en el conocimiento de amenazas inminentes o directas hacia la organización; y la ciberinteligencia táctica, es la que analiza lo que sucede en la red, examina fortalezas y debilidades, como así también las tácticas y procedimientos empleados por los ciberatacantes.

Relacionado con las operaciones castrenses, la ciberinteligencia ejecutaría operaciones de vigilancia y reconocimiento, ya que su función principal es la obtención de información para producir inteligencia a fin de poder asesorar en la toma de decisiones.

Así como la inteligencia tradicional es empleada para apoyar a elementos del componente ejército en el espacio terrestre, la ciberinteligencia debería apoyar a los elementos de ciberdefensa del componente ejército que ejecutan actividades en el ciberespacio.



Fuente: Gráfico elaboración propia

Sección II

Marco legal para el empleo de la Inteligencia militar en el la Argentina.

Antes de desarrollar esta sección, debemos apreciar que las normas legales establecidas a nivel mundial para controlar las actividades en el ciberespacio, son escasas y de difícil implementación, dadas las características de este nuevo escenario.

En la presente sección citaremos y desarrollaremos algunas normas legales que regulan el espacio digital y delimitan la ciberseguridad y la ciberdefensa en el ámbito de la Defensa Nacional, como ser:

Decreto Nro 624/03 y sus modificaciones (Estructura Organizativa de la Jefatura de Gabinetes de Ministerios), establece que la Secretaria de Gestión Pública (SGP) es el organismo responsable del diseño, implementación y seguimiento de la política de modernización del Estado y también de definir las estrategias sobre tecnologías de la información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información en la administración Pública Nacional.

El Decreto Nro 1028/03, establece que la Oficina Nacional de Tecnologías de Información (ONTI), (la cual depende de la SGP) es la encargada de proponer una estrategia de optimización relacionado con los recursos aplicados y niveles de prestación de las subredes que componen La Red Nacional de Información, sobre la base de normas para el control técnico y administrativo, mantener actualizada la información sobre los bienes informáticos de la Administración Nacional entre otros.

Resolución Nro 580/11 de la Jefatura de Gabinete de Ministro, establece el Programa Nacional de Infraestructuras Criticas de Información, cuyo objetivo es administrar toda la información sobre reportes de incidentes de seguridad en el sector

Público Nacional que hubieren adherido al Programa y encauzar sus posibles soluciones de forma organizada y unificada, como así también establecer planes estratégicos y prioridades para liderar el abordaje de la ciberseguridad, certificando la implementación de los últimos avances tecnológicos para la protección de infraestructuras críticas. El artículo Nro 5 de esta resolución invita a todas las entidades y jurisdicciones, entre ellos el Ministerio de Defensa y sus Fuerzas Armadas a adherir a este programa, por otro lado, el articulo Nro 6 de esta resolución haciendo referencia a lo establecido en la Ley Nro 25.326 (protección de Datos Personales) y su Decreto reglamentario Nro 1558 de fecha 29 de noviembre de 2001, instaura que la implementación del programa no supondrá la intercepción ni la intervención en conexiones o redes de acceso privado.

Habiendo analizado las normas que regulan la ciberseguridad desarrollaremos a continuación aquellas normativas que reglamentan el empleo del instrumento militar.

Ley Nro 23554 (Ley de Defensa Nacional), sancionada el 13 de abril de 1988 y promulgada el 26 de abril de ese mismo año, en su artículo 2 que expresa que la Defensa Nacional "es la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo" , y en su artículo 4 expresa que para "dilucidar las cuestiones atinentes a la Defensa Nacional, se deberá tener permanentemente en cuenta la diferencia fundamental que separa a la Defensa Nacional de la Seguridad Interior" (p.1).

El Decreto Nro 727/06 (Poder Ejecutivo Nacional, 2006), en su artículo 1, especifica que" las Fuerzas Armadas, instrumento militar de la defensa nacional, serán empleadas ante agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro/s Estado/s, sin perjuicio de lo dispuesto en la Ley Nº 24.059 y en la

Ley Nº 24.948 en lo concerniente a los escenarios en los que se prevé el empleo del instrumento militar y a las disposiciones que definen el alcance de dicha intervención en operaciones de apoyo a la seguridad interior. Se entenderá como "agresión de origen externo" el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas". (PEN, 2006, p.1)

Directiva de política de Defensa Nacional (DPDN), plasmada en el Decreto Nro 457 (Poder Ejecutivo Nacional, 2021), en el Capítulo II "Política de Defensa Nacional: Concepción y posicionamiento estratégico de la República Argentina en materia de defensa", presenta al Sistema de Defensa Nacional que "se orienta estructural y organizativamente hacia la disuasión de potenciales agresiones externas por parte de fuerzas armadas de otros estados, siguiendo lo dispuesto por la Resolución 3314 (1974) de la Asamblea General de las NACIONES UNIDAS y el consenso político interpartidario plasmado en el plexo normativo construido para el sector de la Defensa en democracia (compuesto, entre otras normas, por la Ley N° 23.554 de Defensa Nacional, la Ley Nº 24.059 de Seguridad Interior, la Ley N° 25.520 de Inteligencia Nacional, sus respectivas modificatorias y el Decreto Reglamentario Nro 727/06)"(p.18).

Queda bien establecido que las fuerzas militares pueden ser empleadas solamente ante agresiones externas y con ellos sus elementos de inteligencia, ahora bien, también existen excepciones donde las fuerzas armadas pueden actuar en el interior del país, los cuales desarrollaremos posteriormente.

En la Ley 24059 (Ley de Seguridad Interior), sancionada el 8 de diciembre de 1991 y promulgada el 6 de enero de 1992, referido a las agresiones y/o atentados, establece:

Articulo Nro 27 “Las Fuerzas Armadas podrán apoyar las operaciones de seguridad interior mediante la afectación de sus servicios de arsenales intendencia, sanidad, veterinaria, construcciones y transporte, así como de elementos de ingenieros y comunicaciones, para lo cual se contará en forma permanente con un representante del Estado Mayor Conjunto en el Centro de Planeamiento y Control de la Subsecretaria de la Seguridad Interior” (p.8)

Artículo Nro 28” Todo atentado en tiempo de paz a la jurisdicción militar, independientemente de poner en forma primordial en peligro la aptitud defensiva de la Nación, constituye asimismo una vulneración a la seguridad interior” (p.8)

Artículo Nro 29 “constituye una obligación primaria de la autoridad militar la preservación de la fuerza armada y el restablecimiento del orden dentro de la aludida jurisdicción, de conformidad con las disposiciones legales vigentes en la materia” (p.8).

Artículo Nro 31” las Fuerzas Armadas serán empleadas en el restablecimiento de la seguridad interior dentro del territorio nacional, en aquellos casos excepcionales en que el sistema de seguridad interior resulte insuficiente a criterio del Presidente de la Nación para el cumplimiento de los objetivos establecidos en el artículo 2º”.

Articulo Nro 32” a los efectos del artículo anterior, el Presidente de la Nación, en uso de las atribuciones contenidas en el artículo 86, inciso 17 de la Constitución Nacional, dispondrá el empleo de elementos de combate de las Fuerzas Armadas para el restablecimiento de la normal situación de seguridad interior, previa declaración del estado de sitio.”

Cuando hablamos de jurisdicción militar en la Ley del Seguridad del Interior, expresa en la Resolución 1020 (Ministerio de Defensa, 2009) “como el ámbito territorial donde la autoridad militar ejerce competencias propias derivadas de las leyes Nro 23.554 y Nro 24.948” (p.6).

Ley Nro 24.948 (Restructuración de las fuerzas armadas) reconoce otros supuestos empleos del Instrumento Militar, definidos como subsidiarios por el Decretos Nro 1691/06, como ser operaciones en el marco de Naciones Unidas, operaciones en apoyo a la seguridad interior, enmarcados en la Ley Nro 24.059, operaciones de apoyo a la comunidad nacional o de países amigos y participación de las Fuerzas Armadas en la construcción de un sistema de Defensa Subregional.

Ley Nro 25520, Ley de Inteligencia Nacional, expresa claramente las limitaciones de la producción de inteligencia dividiendo la misma en inteligencia criminal y la inteligencia militar, prohibiendo a esta última ejecutar inteligencia interna, pero no delimita claramente la responsabilidad de la obtención de información en el ciberespacio.

Cabe destacar que esta ley sufrió modificaciones pertinentes al tema donde se expresa en la Ley 27126, (Agencia Federal de Inteligencia) sancionada el 25 de febrero de 2015 y promulgada el 3 de marzo de ese año. autoridad máxima del Sistema de Inteligencia Nacional, donde establece el manejo de la información sensible sobre datos de las personas y/o organizaciones, donde ella presenta en su artículo 13 que “Los organismos de inteligencia enmarcarán sus actividades inexcusablemente dentro de las prescripciones generales de la Ley de Protección de los Datos Personales 25.326. El cumplimiento de estas disposiciones será materia de directivas y controles por parte del titular de cada organismo integrante del Sistema de Inteligencia Nacional en el ámbito de su respectiva Jurisdicción. La revelación o divulgación de información respecto de

habitantes o personas jurídicas, públicas o privadas, adquirida por los organismos de inteligencia con motivo del ejercicio de sus funciones, requerirá sin excepción de una orden o dispensa judicial "(p.4). Cabe destacar que la protección de datos y archivos de inteligencia son centralizados en una base de datos a cargo de un responsable del sistema con el objetivo de garantizar las condiciones y procedimientos respecto a la recolección, almacenamiento, producción y difusión de la información obtenida.

Conclusiones parciales del capítulo III

Después de haber analizado como es empleo de la inteligencia en el ciberespacio y el marco legal que poseen las Fuerzas Armadas para ser empleadas ante agresiones externas prohibiendo su intervención en el marco interno, salvo algunas excepciones se llega a la conclusión que a pesar de citar un listado de artículos constitucionales, leyes y decretos en torno al ámbito de la Defensa Nacional especialmente para el empleo del Instrumento Militar con sus respectivos elementos de inteligencia, resulta difícil de visualizar los límites y/o radio de acción para la realización de las actividades propias de la inteligencia militar en el ciberespacio, ya que el mismo no posee limites claramente definidos, lo que dificultaría establecer con claridad si las acciones que se ejecutan están o no violando las normas legales.

Las características del ciberespacio y la gran cantidad de incertidumbre en el mismo, demandan que ante una agresión a cualquier infraestructura critica la respuesta defensiva debe ser inmediata, prevaleciendo la integridad estructural sobre la identidad de la amenaza, ahora bien para que esto funcione debe existir un trabajo interagencial en lo relacionado a la ciberinteligencia donde las FFSS y las FFAA compartan información actualizada sobre los ciberataques que se desarrollan en el ciberespacio.

Con respecto al empleo de los elementos de inteligencia militar en el ciberespacio y las normativas legales que prohíben el que estos actúen en el marco interno del país, la única manera de que esto no ocurra es identificando al agresor, para lo cual una vez que el agresor es identificado por los elementos de inteligencia militar y se toma conocimiento que es de origen interno, el caso se lo debe pasar automáticamente a la inteligencia criminal para que continúe con las investigaciones correspondientes.

Conclusiones finales

El presente trabajo tiene como objetivo establecer una organización de Inteligencia Militar que pueda operar en el ciberespacio y ejecutar actividades de MSCI para contribuir con el asesoramiento y asistencia a la ciberdefensa en el componente militar.

Durante el desarrollo de la presente investigación, se buscó analizar las políticas de ciberdefensa de otros países, entender el ciberespacio como un nuevo dominio para las ciberguerras, indagar sobre los posibles actores que se desenvuelven en este tipo de ambiente estudiando sus tácticas y procedimientos a fin de poder comprender como logran cumplir con sus objetivos, y para finalizar se asimiló el empleo de la ciberinteligencia teniendo en cuenta las normas legales que posee nuestro país para la consumación de la misma.

En primer lugar, hemos observado lo importante que es la obtención de información en este tipo de ambiente, la cual permite alertar de nuevas amenazas y minimizar riesgo, claramente los elementos de ciberinteligencia utilizados por los países analizados tuvieron un rol muy importante en esta actividad, ya que los mismo dependían de esa información para optimizar sus políticas de defensa.

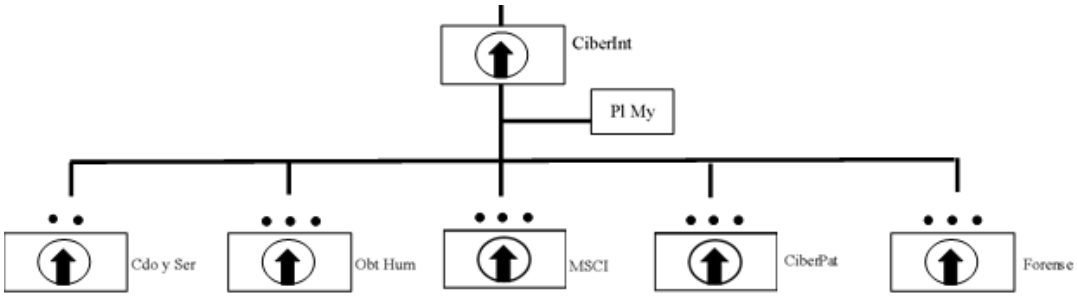
Con respecto al ciberespacio, los aspectos relevantes fueron las diferentes capas en que se divide este nuevo ambiente operacional y como se desenvuelven los actores en el mismo, estos factores de contingencia y de configuración hay que tenerlos en cuenta al momento diseñar un elemento de inteligencia que opere en este ambiente.

Por último y relacionado a la doctrina de esta nueva organización debe estar enfocada a las tácticas y procedimiento de empleo utilizados por los ciberatacantes, a la información obtenida sobre los diferentes tipos de ciberinteligencia que se ejecutan en el ciberespacio y al marco legal en nuestro país.

Después de haber estudiado y analizados los puntos anteriormente expresados se concluye que la organización más adecuada para operar en el ciberespacio y brindar asesoramiento y asistencia a la ciberdefensa en el componente militar, es una compañía de ciberinteligencia cuyo objetivo es la obtención de información y engañar la localización de las infraestructuras criticas TI y TO.

Aspectos organizacionales del elemento propuesto:

Organización



Fuente: Gráfico elaboración propia

Zona de responsabilidad de los diferentes elementos que componen la compañía de inteligencia para operar en el ciberespacio:

Capa Física: Sección Forense y Sección Obtención Humana

Capa lógica: Sección de Ciberpatrullaje y Sección MSCI

Capa Ciberpersona: Sección Obtención Humana y Sección MSCI

Actividades a desarrollar por cada elemento que integra la compañía

Sección forense: recuperar información digital en dispositivos informáticos para identificar táctica utilizada por el ciberatacante.

Sección Obtención Humana: contribuir con la obtención de información y producción de inteligencia de la Sección Ciberpatrullaje que no pueda ser obtenida en la capa lógica.

Sección Ciberpatrullaje: obtener información y producir inteligencia dentro de la capa lógica.

Sección MSCI: engañar al ciberatacante sobre la ubicación de las infraestructuras critica de TI y TO.

Por último, es importante que el personal que integre esta organización tenga conocimiento específico de cómo operar en el ciberespacio es aconsejable que el grupo de analistas este conformado por ingenieros informáticos y por hackers.

Aporte profesional

Además de lo desarrollado en el presente trabajo, considero importante continuar la investigación sobre las capacidades y competencias que debe tener esta organización, teniendo en cuenta el equipamiento necesario para poder afrontar las exigencias.

BIBLIOGRAFIA

Marco jurídico y legal de la República Argentina

Ley Nro 23554 de Defensa Nacional (1988). Boletín Oficial de la República Argentina.

Ley Nro 25520 de Inteligencia Nacional (2001). Boletín Oficial de la República Argentina.

Ley Nro 27126 de la Agencia Federal de Inteligencia (2015). Boletín Oficial de la República Argentina.

Ley Nro 24059 de Seguridad del Interior (1991). Boletín Oficial de la República Argentina.

Decreto 457/21. Directiva de política de Defensa Nacional. Ministerio de Defensa.

Decreto 381/06. Regulación Ley 23554/88 y Ley 25520/01. Ministerio de Defensa.

Decreto 727/06. Reglamentación Ley 23554/88. Ministerio de Defensa.

Decreto 950/02. Reglamentación Ley 25520/01. Ministerio de Defensa

Decreto 1291/91. Reglamentación Ley 24059/92. Ministerio de Seguridad.

Publicaciones oficiales nacionales

EMCOFFAA (2007). Inteligencia para la Acción Militar Conjunta. República Argentina.

EMCOFFAA (2007). Medidas de Seguridad de Contrainteligencia para la Acción Militar Conjunta. República Argentina.

EMCOFFAA (2019). Glosario para la Acción Militar Conjunta. p. 139. República Argentina.

Ejército Argentino (2021), DIRECTIVA DEL SUBJEFE DEL ESTADO MAYOR GENERAL DEL EJÉRCITO NRO 01/21. República Argentina.

Ejército Argentino (2019). ORDEN ESPECIAL DEL SUBJEFE DEL ESTADO MAYOR GENERAL DEL EJERCITO NRO 05/G/19. República Argentina.

Publicaciones oficiales extranjeras

DECRETO Nº 10.222. Atos do Poder Executivo (2020) Diário Oficial da União

DECRETO N° 36/015. (2015). Ministerios de defensa nacional. República Oriental del Uruguay

DECRETO Nº 579 (2020). de la Republica de chile

Centro de Estudios e Investigaciones del Ejército de CHILE (2020). Escenarios Actuales.

Biblioteca del Congreso Nacional de CHILE (2018). Política Nacional de Ciberseguridad 2017-222

Publicaciones y artículos varios

Alejandro Carletti Estrada (2017), Ciberseguridad una estrategia informática/militar. España

Casey, George W (2008). America's Army In an Era of Persistent Conflict, Army Magazine. EEUU.

Centro Cristológico Nacional 13/20. (2020). Ciberamenazas y tendencias. España

Centro Cristológico Nacional. (2021). Principio y recomendaciones básicas en ciberseguridad 01/21. España

GONZALEZ, G (2017). De la guerra asimétrica a la guerra hibrida. Tesis ESG. República Argentina.

Instituto Español de Estudios Estratégicos. (2010) Ciberseguridad. retos y amenazas a la seguridad nacional en el ciberespacio 149/10.

Julián Gutiérrez. (2020) Ciberinteligencia Qué es, tipos que existen y ejemplos prácticos de cómo se aplica. Diario web Ciberpatrullaje.

LISA Institute. (2019). Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas. Documento Web. España.

Luis Alberto Álvarez. (2020). Ciberataques, antesala de la guerra híbrida. Diario web Expansión.

Luis Pablo Guimpel (2020). A estrutura da defesa cibernética na República Argentina e na República Federativa do Brasil, entre os anos 2014 e 2019: um estudo comparado. Monografía ESG República Federativa del Brasil.

Roveda, G. (2012). Estructura y capacidades de un Sistema de Inteligencia Táctico en un contexto de Guerra Híbrida. TFI ESG. República Argentina

Sun Tzu (2003). El arte de la guerra. Longseller. República Argentina

Verónica Barrios Achavar (2018), Política Nacional de Ciberseguridad: 2017-2022. Documento de la Biblioteca del congreso Nacional de Chile.

Baqués Quesad, J (2015). Las guerras híbridas: un balance provisional, Documento de Trabajo del Instituto Español de Estudios Estratégicos. España

Otras fuentes

https://ncsi.ega.ee/country/

https://cert.br/stats/incidentes/

https://www.lisainstitute.com

https://bidlab.org/es/publications

https://www.esgcffaa.edu.ar/esp/

https://www.ejercito.cl/

http://www.eceme.eb.mil.br//

https://definicion.de/

https://www.campusciberseguridad.com/

https://www.redeszone.net/