Parte 1: **INTRODUCCION**

"Nadie lo sabe todo, pero todo el mundo sabe algo."

Adagio Español.

1. Tema

a. Área de Investigación: Inteligencia.
b. Tema de Investigación: Medidas de Seguridad de Contrainteligencia en redes sociales.
c. Tema acotado: Protección a la propia fuerza contra las operaciones de información a través de las redes sociales.

2. Problema

a. Antecedentes y justificación del problema:

El problema, en parte, ha sido estudiado pero haciendo referencia a medidas de seguridad de contrainteligencia y por otro lo que se refiere a seguridad en redes sociales del punto de vista técnico para evitar delitos informáticos del tipo robo de identidad o la intrusión en la privacidad de las personas.

El Ejército de EEUU, ha desarrollado "Army Social Media Handbook", en donde hace recomendaciones acerca de la correcta utilización de las redes sociales para evitar la fuga de información con clasificación de seguridad y dificultar la obtención a través de las redes sociales.

En la doctrina vigente en el Ejército Argentino no se desarrollan las denominadas operaciones de información, excepto en su definición, pero en los países vecinos, por ejemplo los países integrantes del Consejo de Defensa Sudamericano, dentro de sus correspondientes doctrinas definen cuales son las operaciones de información y su respectiva caracterización y cada día son más importantes en el entorno complejo en que se desarrollan las operaciones militares en la actualidad y la tecnología abre más lugares y espacios proclives a las mismas.

En el "Manual de Seguridad Informática – EA Ed 2013", se han desarrollado las medidas tendientes a proteger las redes informáticas y de comunicaciones sobre los denominados malware (programas mal intencionados), pero sin hacer referencia a su uso como parte de una operación de información.

Cada día es mayor la cantidad de información que se reúne a través de la denominada "Open Source Intelligence (inteligencia de fuentes abiertas)", que es la inteligencia que se realiza sobre información que se obtiene desde fuentes tales como internet, radios, dispositivos multimedia, televisión, comunicados de prensa, correos involuntarios etc., que salen a través de los distintos dispositivos de conectividad con las redes sociales, generalmente los atacantes o personas que planeen la realización de operaciones de inteligencia es donde reunirán

alrededor del 70% (setenta por ciento) de la información necesaria para el planeamiento de la operación.

"*No hay límite a la información que un atacante puede obtener desde fuentes públicas abiertas donde, además, cada dato obtenido puede llevar al descubrimiento de más información*".[1]

A la fecha se han producido una serie de acciones llevadas adelante a través de las redes sociales en las cuales se han impulsado distintas actividades u operaciones con distintos fines desde provocar cambios políticos a la afectación de los sistemas informáticos de enlace y funcionamiento de un gobierno (Caso Primavera Árabe, Ciber Ataque a Lituania entre otros) y que las mismas han dado origen a la creación de organizaciones con importantes presupuestos para llevar adelante medidas de seguridad que protejan a los estados y a las personas, ejemplo de esto es el cibercomando organizado por Israel y que salió publicado su creación en IBL-News del 30 de mayo de 2011 y a nivel regional Brasil es pionero en la organización de un cibercomando.

"*Los eventos asociados a la primavera árabe, sobre todo en Túnez y Egipto, han hecho que las agencias de inteligencia de todo el mundo desarrollen protocolos legales y metodológicos para realizar labores de prospección en las redes sociales*"[2]

b. Formulación de la pregunta.

¿Cómo evitar que las fuerzas integrantes de un Teatro de Operaciones sean objetivo de una operación de información enemiga a través de las redes sociales de uso más común?

3. Objetivos

a. Objetivo general.

Identificar/determinar los aspectos relevantes a ser tenidos en cuenta, en el manejo de las redes sociales por parte del personal de inteligencia estratégica/militar, para producir un adecuado asesoramiento y asistencia al Comandante en un Teatro de Operaciones y niveles superiores, para evitar ser objetivo de operaciones de información enemigas.

b. Objetivos específicos.

Diferenciar cuáles son las operaciones de información más probables a desarrollar sobre las redes sociales.

Detectar cuáles serán las herramientas más idóneas que puede utilizar el opo-

[1] www.econstor.eu/dspace/Nutzungsbedingungen (German Institute for Ecomic Research)

[2] Mediterranean Council for Intelligence Studies (MCIS 2012) Intelligence Studies Yearbook. (www.i2integrity.es)

nente para llevar adelante operaciones de información en las redes sociales.

Especificar cuáles serán las medidas de seguridad de contrainteligencia más aptas para proteger a los propios medios y sistemas de la acción del enemigo.

4. Marco Teórico

El marco teórico del presente trabajo estará conformado por la doctrina del Ejército Argentino contenida en los reglamentos de Inteligencia Táctica, Inteligencia para la Acción Militar Conjunta, Medidas de Seguridad de Contrainteligencia, Seguridad en Redes Informáticas.

Además utilizaremos publicaciones del Ejército de los Estados Unidos de América, Publicaciones de organizaciones privadas especializadas en asesoramiento y seguridad informática.

Definiremos como sitios de redes sociales (SNS) a los servicios basados en internet que permiten a las personas usuarias u organizaciones construir un perfil público o semi-público dentro de ciertos límites, vinculando a otros usuarios que comparten una conexión, ver y recorrer su lista de las conexiones y las hechas por otros dentro del entorno de un determinado software o en la web, a los cuales se accede mediante distintos dispositivos que facilitan la conectividad.

Las redes sociales proporcionan el medio para interactuar socialmente a través de internet, y a través de productos tales como correo electrónico, mensajería instantánea o de algún otro modo.

Las de mayor convocatoria de los últimos 5 años son facebook, twiter, youtube, linkedin, skype, wikipedia, en otros continentes, jabook, lagbook y otras menos conocidas o con menor difusión. A raíz de la cantidad de actividades que realizan los usuarios a través de ellas es que se han convertido en medio u objetivo principal para los hackers y para la política en algunos países o para la afectación de organizaciones tanto privadas como estatales.

El trabajo está organizado en tres capítulos y conclusiones finales.

En el capítulo I desarrollaremos las operaciones de información, sus características distintivas, comparación de costos de ejecución con respecto al efecto que pueden causar y su aplicación a traves de las redes sociales.

En el capítulo II, este será un capitulo técnico, en donde explicaremos las principales herramientas de software y hardware para realizar operaciones de información a través de los sistemas informáticos como canal de base de las redes sociales.

En el capítulo III, desarrollaremos las medidas de seguridad de contrainteligencia a llevar adelante para preservar a los medios de un Teatro de Operaciones de las operaciones de información del oponente/enemigo.

Finalmente, se obtendrán conclusiones finales del trabajo de investigación.

Este trabajo final de licenciatura lo relacionaremos con los conocimientos adquiridos de las siguientes materias:

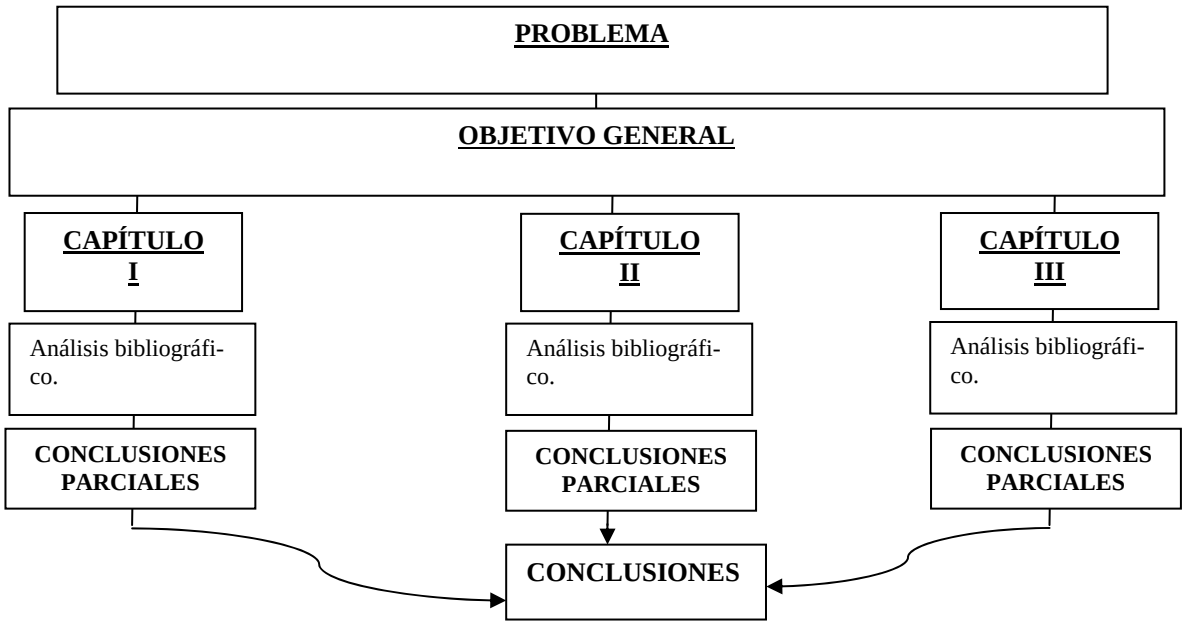
a. Inteligencia estratégica y táctica: principalmente en los aspectos referidos al ciclo de la inteligencia y los conceptos de contrainteligencia.
b. Metodología para la toma de decisiones: en los aspectos referidos al proceso de asistencia y asesoramiento al Comandante/Jefe.
c. Geografía Militar: relacionándolo con el estudio geográfico militar, dentro del cual se encuentra el factor geohumano y geomilitar que es el objetivo de las operaciones de información.
d. Historia Militar: me basaré en los ejemplos de la misma para darle mayor asidero a los conceptos vertidos en el presente estudio.
e. Planeamiento, Organización y Dirección: con los conceptos vertidos de organización y estructuración del Teatro de Operaciones y de las operaciones necesarias a desarrollar para obtener las condiciones más favorables para librar la batalla.

5. Metodología a emplear

La metodología a emplear estará basada en el método descriptivo y el diseño de la investigación será exploratorio descriptivo. Las técnicas de recolección a aplicar serán recopilación documental con el consiguiente análisis bibliográfico y el análisis lógico.

a. Método a emplear: método descriptivo.
b. Diseño de la investigación: se basa en el diseño exploratorio descriptivo.
c. Alcance: seccional de carácter cualitativo.

6. Esquema Gráfico-Metodológico



Parte 2: DESARROLLO

"The dogmas of the quiet past are inadequate to the stormy present. The ocassion is piled high with difficulty, and we must rise with the ocassion. As our case is new, so we must think anew and act anew".

"Los dogmas del tranquilo pasado son inadecuados para el tormentoso presente. La ocasión se presenta con dificultad, y debemos aprovechar el momento. Nuestro caso es nuevo, por lo que debemos pensar de nuevo y actuar de nuevo."

Abraham Lincoln, Mensaje al Congreso, 1 de diciembre de 1862.[3]

El avance tecnológico de las últimas dos décadas ha permitido el desarrollo de la industria de las telecomunicaciones mundiales, permitiendo el acceso, conectividad y menores costos a caudales de información antes impensados.

El auge de internet y sus bondades de la transmisión de información en todo tiempo todo lugar y la constante evolución de los medios de acceso a esa conectividad trajeron aparejado el surgimiento y posterior auge de las redes sociales.

Con lo cual han surgido las denominadas operaciones de información y por lógica las operaciones o medidas de seguridad para evitar el efecto de las mismas.

En la doctrina vigente en el Ejército Argentino no se desarrollan las denominadas operaciones de información, excepto en su definición, pero en los países vecinos, por ejemplo los países integrantes del Consejo de Defensa Sudamericano, dentro de sus correspondientes doctrinas definen cuales son las operaciones de información y su respectiva caracterización y cada día son más importantes en el entorno complejo en que se desarrollan las operaciones militares en la actualidad y la tecnología abre más lugares y espacios proclives a las mismas.

En el "Manual de Seguridad Informática – EA Ed. 2013", se han desarrollado las medidas tendientes a proteger las redes informáticas y de comunicaciones sobre los denominados "malware"(programa malicioso o mal intencionado) , pero sin hacer referencia a su uso como parte de una operación de información.

Cada día es mayor la cantidad de información que se reúne a través de la forma denominada "Open Source Intelligence (inteligencia de fuentes abiertas)", que es la inteligencia que se realiza sobre información que se obtiene desde fuentes tales como internet, radios, dispositivos multimedia, televisión, comunicados de prensa, correos involuntarios etc., que salen a través de los distintos dispositivos de conectividad con las redes sociales.

Generalmente los atacantes o personas que planeen la realización de operaciones de información es donde reunirán alrededor del 70% (setenta por ciento) de la información

[3] Prólogo Capítulo 1, JP 3-13 Informations Operations, 13Feb2006, Defense Department EEUU.

necesaria para el planeamiento de la operación, con lo cual las medidas de seguridad de contrainteligencia toman un valor antes inesperado.

A la fecha se han producido una serie de acciones llevadas adelante a través de las redes sociales en las cuales se han impulsado distintas actividades u operaciones con distintos fines desde provocar cambios políticos a la afectación de los sistemas informáticos de enlace y funcionamiento de un gobierno (Caso Primavera Árabe, Ciber Ataque a Lituania entre otros) y que las mismas han dado origen a la creación de organizaciones con presupuestos millonarios para llevar adelante medidas de seguridad que protejan a los estados y a las personas, ejemplo de esto es el cibercomando organizado por Israel y que salió publicado su creación en IBL-News del 30 de mayo de 2011.

"Los eventos asociados a la primavera árabe, sobre todo en Túnez y Egipto, han hecho que las agencias de inteligencia de todo el mundo desarrollen protocolos legales y metodológicos para realizar labores de prospección en las redes sociales"[4]

[4] Mediterranean Council for Intelligence Studies (MCIS 2012) Intelligence Studies Yearbook (www.i2.integrity.es)

Capítulo 1: Operaciones componentes de las Operaciones de Información.

El objetivo específico de este capítulo es determinar cuáles son las operaciones de información más probables a desarrollar sobre las redes sociales.

En este capítulo se desarrollarán las definiciones de las distintas operaciones que engloban las operaciones de información de acuerdo a publicaciones provenientes de fuentes públicas.

El uso de la información puede estar dirigido a informar o a desinformar. Desinformar significa "*Dar información a alguien ocultando o falseando hechos intencionadamente*"[5], en el caso particular que vamos a desarrollar además interviene la tecnología y la inteligencia humana que hace uso de sus resultados.

La competencia en este campo se denomina *Operaciones de Información*. El objetivo es conseguir una ventaja competitiva sobre un adversario. Las operaciones de información son un conjunto de acciones para afectar la voluntad de lucha, el comando y control del oponente a la vez que protege a los propios; consiste en el empleo integrado de acciones de guerra electrónica, acciones para afectar redes informáticas (redes internas o a través de internet), operaciones psicológicas, acciones de engaño y operaciones de seguridad.[6]

Las Operaciones de Información están indisolublemente unidas a las guerras desde hace largo tiempo. El concepto se transformó más popular a partir de mediados de la última década del S XX, debido a los adelantos tecnológicos que permitieron obtener y usar información en provecho de los propios intereses, y para obstaculizar los del adversario.

En resumidas formas denominaremos como Operaciones de Información a aquellas que se caracterizan por una lucha sobre los sistemas de información. Así entendidas, se enlazan con lo que se conoce como Revolución en Asuntos Militares[7], entendiendo como tal la influencia de la tecnología en la forma de hacer la guerra.

El estudio de la historia militar demuestra que la naturaleza, el propósito y la forma de hacer la guerra cambian según lo haga la tecnología y la creatividad de los comandantes que son los responsables del empleo de los medios puestos a disposición.

Las técnicas de las Operaciones de Información darán una ventaja decisiva sobre los adversarios y quienes no posean tal capacidad, se encontrarán en una desventaja considerable, si solo pretenden basar su poder de combate en los medios materiales disponi-

[5] Diccionario del Estudiante, Real Academia Española, Ed Santillana, Talleres Gráficos de Printer Industria Grafica Newco, S.L., Barcelona, Mayo 2008.
[6] JP 3-13 Information Operations- United State Defense Department. Febrero 2006.
[7] VAN CLEVELD MARTIN, "La Transformación de la Guerra", Traducción C. A. Pisolito, Talleres Gráficos Plantie, Buenos Aires, Septiembre 2007.

bles. El problema pasa por identificar las formas que adoptan las operaciones de información.

Algunas se refieren a aspectos estrictamente militares de las luchas tradicionales o convencionales; otras, a las características de las denominadas como guerra sin restricciones.[8]

De cualquier forma, el uso de las tecnologías de información es de naturaleza dual, tanto civil como militar, por lo que es difícil establecer límites precisos o definir incumbencias y responsabilidades de sectores del poder nacional para su control y uso.

Las operaciones de información por la magnitud y capacidades con que deben contar los medios a utilizar y la preparación específica del personal integrante de las diferentes organizaciones necesarias para llevarlas adelante serán planificadas y ejecutadas a partir del nivel operacional y superiores.

Todo pasa por poner en orden las ideas y tratar de identificar las diferentes formas de llevar a cabo Operaciones de Información. En definitiva, cualquiera sea su forma, todas persiguen evitar que el oponente reaccione en forma unívoca, y se genere confusión en una organización que será más peligrosa, cuanto más verticalista sea su organización. Las Operaciones de Información tienen la particularidad de integrar un conjunto de formas, antes que formas particulares aisladas.

Pueden identificarse seis formas de Operaciones de Información: sobre la mente de los individuos en sus diferentes roles (operaciones para afectar la voluntad de lucha u operaciones psicológicas), operaciones de engaño militar, operaciones de seguridad para obtener información y llevar a cabo operaciones, operaciones sobre las emisiones electrónicas, (guerra electrónica), operaciones sobre las redes informáticas, operaciones sobre la función de comando y control. Todas estas formas se llevan a cabo para facilitar las propias operaciones, y para dificultar las del oponente, y se llevan a cabo en los ámbitos físicos, informativos y los pertenecientes al conocimiento individual, tratando de afectar fundamentalmente el comando y control de las operaciones. [9]

Estas clasificaciones no son absolutas, en muchas partes estas categorías se superponen y es difícil encontrar la clasificación ideal.

Las operaciones para afectar la voluntad de lucha.

Las operaciones psicológicas son *"planificadas para transmitir información e indicadores seleccionados para un determinado público blanco a fin de influir en sus emociones, motivos, razonamiento objetivos y en última instancia, sobre el comportamiento de sus gobiernos, organizaciones, grupos e individuos. El propósito es inducir o reforzar actitudes y comportamientos favorables a la propia fuerza."*[10].

Las operaciones psicológicas o acciones a llevar adelante son consideradas como núcleo de las operaciones de información y son *"particularmente importantes en las*

[8] Ibídem 7.
[9] Ibídem 6.
[10] Ibídem 6.

primeras etapas de la operación dado el tiempo que se tarda en desarrollar, diseñar, producir, distribuir, difundir y evaluar los productos y acciones de operaciones psicológicas"[11], y serán dirigidas a través de los programas aprobados desde los más altos niveles de la conducción.

Las operaciones psicológicas dependiendo del efecto que persiguen cuando influyan sobre la voluntad nacional, oscilan en las situaciones denominadas, entre el guante de terciopelo o el puño de hierro. Algunos lo llaman "ofensivas en la paz"; solo basta ver los desfiles rusos, chinos y coreanos, o en Chipre las ejercitaciones militares de ambos bandos, dirigidas a mostrar el poderío. Es un concepto de seguridad denominado disuasión.

Hay otras formas que emplean los más débiles. El líder del clan Somalí Mohamed Aideed pareció ser un maestro en el uso de las operaciones psicológicas. En la confrontación con los *rangers* de EEUU, conocido ampliamente en la película La Caída del Halcón Negro, que costara la vida a 19 Rangers, el bando de Aideed perdió 15 veces ese número, que representaba casi la tercera parte de su fuerza. Sin embargo, las fotografías de somalíes arrastrando los cuerpos de soldados de EEUU por las calles de Mogadisho fueron trasmitidas por CNN a los Estados Unidos y terminaron por convencer a la audiencia que era necesario evacuar la presencia de EEUU en Somalia.

También Aideed usó con ingenio las comunicaciones satelitales y radiales dentro de la ciudad, de forma tal que las ondas rebotaran y no pudieran ser localizadas[12], con estos dos ejemplos de nivel táctico/operacional, puedo comprobar como se llevaron adelante acciones que en su sinergia configuran una operación de información, más allá que apreciamos que Aideed por su falta de formación académica militar utilizo los medios en base su experiencia empírica para afectar a las fuerzas norteamericanas.

Hoy la difusión de los productos de operaciones psicológicas se ven favorecidos por los medios de comunicación globales, desde la impresión tradicional, pasando por el fax, la amplia difusión y acceso a internet, los servicios de telefonía móvil con acceso a redes sociales de amplia difusión y muy bajo control, facilidades para la utilización de los no lugares (paredes con pintadas, propaladoras), aseguran que los eventos se conozcan de inmediato o en un muy corto tiempo en una gran parte del teatro de guerra.

Se suma a esto que el ser humano tiene la tendencia de creer todo lo que dicen los medios de comunicación social y hasta que se descubra la verdad, se pierde o se gana un tiempo valioso, las contramedidas pueden resultar tardías y las consecuencias ya se han producido. Si se usan las emisiones de satélites, los líderes de una nación no necesitan permiso para hablar directamente a los habitantes de otra nación y esta posibilidad está disponible para todos a un costo relativamente bajo. También tiene su influencia la capacidad de editar videos, haciendo aparecer como real lo que no lo es.

Nada desorienta o confunde más a los comandantes enemigos que la acción psicológica apuntada a ellos, para llevarlos a decisiones erróneas o tardías. Los comandantes

[11] Ibídem 6.

[12] Ejemplos de la historia militar facilitados por el Grl Br(r) Evergisto de Vergara, en un borrador de un ensayo sobre operaciones de información.

toman decisiones sobre la base de eventos esperados. Si la realidad es diferente de la que se toma como base para decidir, toma tiempo adaptarse a una nueva realidad contradictoria. Instintivamente, los eventos con baja probabilidad de ocurrencia son descartados, y si ocurren, son pocos los comandantes que pueden adaptarse. Ejemplo de esto es que la más alta conducción alemana, en la Segunda Guerra Mundial, estaba convencida que los Aliados cruzarían por el Paso de Calais, y que el ataque principal provendría donde estaba asentado el general Patton en el Reino Unido. Lo cual no ocurrió así.

Alguien que demostró ser un experto en difundir informaciones en oportunidad era Mussolini. Cuando decidía hacer algo con impacto en la comunidad internacional, lo difundía los viernes, conociendo que el ámbito diplomático se involucraba en sábado y domingo en infinitos asuntos protocolares. Cuando el lunes al reiniciar el trabajo se daban cuenta de los hechos, ya habían pasado tres días. [13]

Los medios de comunicación social pueden jugar un rol importante en esta desorientación de los comandantes. Un caso típico pasó en la Guerra del Golfo de 1991, donde los medios trasmitieron que dos portaaviones estadounidenses estaban atravesando el Canal de Suez el mismo día en que se inició el ataque aliado. Ello llevó a pensar a Sadam que el ataque aún no se lanzaría. Tal información resultó falsa[14]. Asimismo, los medios colaboraron como elemento de comando de los aliados, negando los micrófonos a Sadam, incrementando así su aislamiento internacional. En esta Guerra del Golfo, los iraquíes estaban convencidos que la guerra aérea sería corta – duró 40 días – y que el esfuerzo principal sería terrestre. También creían que la intención de los aliados era reconquistar Kuwait desde el mar. Para eso, los medios divulgaron ambas concepciones, la primera difundida a través de CNN, la segunda enviando buques de guerra aliados a patrullar intensamente las costas,[15] como parte de una operación de velo y engaño.

Históricamente, en el nivel operacional esta manera de engaño psicológico usando las Operaciones de Información han sido más exitosas en el oponente que ha tenido mejor información acerca de los objetivos o efectos que el otro oponente pretende, por lo cual es de importancia determinar que información y medios se deben proteger y de que protegerlos. El conocimiento profundo de la cultura militar imperante y la estatura estratégica del oponente juega un rol importante en esto.

Las formas de difundir los productos de operaciones psicológicas varían a través de ondas de radio (radios portátiles, teléfonos móviles, vía internet –blogs y redes sociales) y el más antiguo de los métodos pero usado hasta hoy, por panfletos arrojados desde el aire.

En la Guerra del Golfo, las fuerzas de la coalición desparramaron la idea mediante panfletos y convencieron a muchas tropas iraquíes que si abandonaban sus vehículos, vivirían más. Eso lo hicieron luego de tomar como blancos con sus armas de precisión, a vehículos blindados iraquíes. Otro caso más conocido es el de la Rosa de Tokio en la

[13] Citado por John Gunther, "Líderes del Siglo XX", Editorial Bruguera, Barcelona, 1968, original en inglés. Ibidem 12.
[14] Quiao Liang y Wang Xiangsui, Unrestrited Warfare, Pan American Publishing Company, Panama, 1999, P. 60.
[15] Ibídem 12.

2da GM, sobrenombre dado por los servicios de contrainteligencia aliados a las radioemisiones en AM en idioma inglés de locutores japoneses angloparlantes, con mensajes dirigidos a las tropas aliadas. Asimismo, en la Guerra de Malvinas, una locutora inglesa ubicada en la flota británica trasmitía noticias tanto en español como en inglés, dirigidos a las tropas argentinas.[16]

Las operaciones de engaño militar.

Las operaciones de engaño militar se definen como *"aquellas acciones ejecutadas para engañar deliberadamente a los decisores del adversario, en cuanto a las capacidades militares, intenciones y operaciones propias, haciendo así que el adversario realice acciones específicas o inacciones que contribuyan al éxito de las fuerzas propias o aliadas. Busca fomentar el incorrecto análisis, haciendo que el adversario llegue a conclusiones erróneas.*

Se basa en la comprensión de cómo el comandante adversario y sus colaboradores piensan, sienten y como realizan la gestión de la información para apoyar sus esfuerzos. Esto requiere un alto grado de coordinación con todos los elementos de actividades de las fuerzas amigas, en el denominado entorno de la información, así como en las medidas físicas para su protección."[17]

Se debe tener en cuenta que en las operaciones de engaño militar se utilizaran modos de acción que pueden ser realizados por las propias fuerzas y que la inteligencia adversaria pueda verificar que cumple con el análisis AFA (aptitud, factibilidad y aceptabilidad), teniendo en cuenta de no caer en el error que el adversario actúa "como imagen espejo", o que posee doctrina y equipamiento similar al propio.

Operaciones de Seguridad, para obtener información y llevar a cabo operaciones.

Este tipo de Operaciones de Información es la más conocida, *"es un proceso de identificación de la información crítica y posteriormente analizar acciones a llevar adelante sobre la información.*
Determinar cuál es la información que se puede facilitar el acceso al adversario y cuál es la crítica acerca de las fuerzas propias o aliadas, intenciones de los comandantes etc., que se debe proteger y que si el adversario obtiene dispone de la iniciativa suficiente para afectar a la propia fuerza o aliados.

Las operaciones de seguridad niegan al adversario la información necesaria para evaluar correctamente las capacidades e intenciones propias. Las operaciones de seguridad complementan a las operaciones de engaño negando al adversario información requerida tanto para evaluar un plan real como refutar un plan de engaño[18]*."*

Las Operaciones de Información defensivas basadas en la inteligencia son desarrolladas para preservar la invisibilidad, o por lo menos ampliar la distancia entre la imagen y la realidad del campo de combate, es decir evitar la información en tiempo real. Los sensores montados en aviones, el AWACS por ejemplo, permiten realizar un seguimiento de los vehículos terrestres y de algunas aeronaves, y recoger y trasmitir imágenes a

[16] Ibídem 12.
[17] Ibídem 6.
[18] Ibídem 6.

los comandantes tácticos. Existen diferentes tipos de aeronaves donde se muestran estos radares de inteligencia, reconocimiento, adquisición de blancos y vigilancia. Brasil los tiene montados en aviones Embraer, aunque en el mundo occidental, la mayoría se encuentran montados en aviones Boeing. Estos sensores son costosos, y la tecnología día a día nos provee de nuevos equipos y van siendo más accesibles para cualquier interesado.

Además de ser costosos, esto sensores pueden ser atacados de una manera barata, inhabilitando los sistemas que usan mediante virus informáticos, anulándolos o corrompiéndolos mediante recursos de guerra electrónica. Algunos autores argumentan que la diseminación de medios técnicos hasta el soldado individual puede crear una gran vulnerabilidad porque si es capturado, revelará la capacidad de acceso a la información que se tiene, revelará la forma en que se obtiene y aún peor, los lugares sobre los que no se puede obtener información y donde se puede actuar sin peligro. De cualquier forma, cuando la lectura técnica de un sensor sea precisa y exacta, las contramedidas que se puedan tomar consistirán en distorsionar lo que los sensores leen, y lo que los analistas concluyen. El ingenio humano tiene un amplio campo de acción aquí, ambos en el encubrimiento y en el engaño.

En los ambientes de alta densidad como las áreas urbanas o las selvas, se considera como los mejores procedimientos encubrir y negar información sobre lo que en realidad pasa es explotando o multiplicando el desorden y la confusión. Hay muchos casos en los que los elementos militares han buscado confundirse con elementos civiles. Estas tácticas de velo y engaño han sido ampliamente aplicadas en Irak, Pakistán y Afganistán. Los señuelos tendrán gran aplicación, siempre sosteniendo la teoría que es más fácil esconder un árbol dentro de un bosque, que rodeándolo con una pared.

El concepto principal es que cualquiera sea la información que puedan detectar los sensores en sus diferentes formas, siempre deberán ser comparados con otros, la información deberá filtrarse, y siempre se dudará de su confiabilidad. El analista deberá decidir que información es confiable, cuál no lo es, y decidir además cuál es el riesgo que se asume con la contramedida que se decida aplicar.

La tecnología de la información puede ser valiosa en la adquisición de blancos, y es preferible usarla en vez de hacerlo mediante adquisición directa o humana, en la relación costo-beneficio por la pérdida del medio de obtención. Sin embargo, todavía no está claro que aquel adversario que tenga tecnología de información avanzada pueda superar al adversario que posea tecnología inferior. El ingenio humano con su correspondiente cuota de iniciativa y creatividad es inagotable.

Las operaciones sobre las emisiones electrónicas.

La guerra electrónica *"se refiere a cualquier acción militar que implica el uso del espectro electromagnético y la energía dirigida para controlar el mismo o atacar al adversario"*[19].

[19] Ibídem 6.

Intenta afectar las bases físicas para transferir la información, en tanto que la criptográfica trabaja entre dígitos binarios para proteger la información blanda o digital.

Las técnicas antirradar pueden asimilarse a técnicas contra sensores (por ejemplo el uso de bengalas para confundir misiles guiados infrarrojos, o el uso de chaff para confundir el guiado de misiles). La característica de un radar es que es activo, recibe ondas reflejadas, en vez de radiación electromagnética pasiva. Por lo tanto, las ondas de radar pueden ser atacadas cuando se emiten y cuando se reciben.

Aviones de interferencia electrónica que vuelen integrados en formaciones de aviones de ataque frecuentemente borran las señales de retorno (la que se debilita engañando sobre la distancia entre el blanco y el radar) mediante el fortalecimiento de esas señales, pero al hacerlo se hacen muy visibles y se transforman en blancos. Los misiles anti radar aire-tierra como el HARM (High Speed Anti Radiation Missile) y el renovado AARGM (Advanced Anti Radiation Missile) obligan a que los radares se apaguen, o se enciendan y apaguen en cortos lapsos. Igualmente, a pesar de la tecnología y los avances de la digitalización, el ingenio humano puede superar obstáculos pensados como insalvables.

Las acciones de guerra electrónica contra las comunicaciones generalmente es más difícil de llevar a cabo que las acciones contra radares. El concepto inicial es que las radios trabajan en diferente tipo de modulación, y hay algunas que son más seguras que otras.

Las Operaciones Electrónicas también son usadas para ubicar geográficamente al emisor. Cuantas más emisiones se detecten más dificultosa resultará esta tarea. Una manera de defenderse es multiplicar las fuentes emisoras, o dispersar los medios. En el S XXI han aparecido misiles denominados “inteligentes” con capacidad de ubicar fuentes de emisión electrónica. También ha hecho su aparición el GPS (Global Positioning System) que permite ubicar coordenadas que pueden introducirse en la base de datos de los misiles. La principal vulnerabilidad de los sistemas de comunicaciones posicionados en el terreno es que requieren enlaces de comunicaciones entre sensores, sistemas de comando y armas dispersas. Estos enlaces son los que hay que atacar.

Aunque el hecho todavía no está completamente aclarado por ser la información clasificada, se dice que el líder guerrillero de las FARC Raúl Reyes fue abatido en mayo de 2008 en territorio ecuatoriano, cuando un misil se “montó” en las emisiones de su teléfono portátil, de acuerdo a versiones periodísticas.

En cuanto a la criptografía, mezclar el contenido de los propios mensajes y ordenar los del otro bando es la esencia de las Operaciones de Información. Cuanto más barata sea la codificación, y más profusas las técnicas de esconder señales como saltos de frecuencia, o espectro ampliado, será más difícil descifrar mensajes cifrados.[20] Teniendo en cuenta que normalmente los fabricantes de los sistemas de criptografía cuando los venden, mantienen como cláusula de venta, la no entrega de la clave secreta, con lo cual no se puede modificar el algoritmo matemático de base del sistema.

[20] www.afceaargentina.org

Aparte de estas dificultades en la codificación, en la actualidad se ha difundido la firma digital para conocer y certificar el grado de seguridad de quien envía un mensaje.

Las operaciones sobre la red informática.

Las operaciones sobre la red informática *"se derivan de la creciente utilización de computadoras en red y sistemas de soporte de tecnología de la información y de infraestructura de organizaciones civiles y militares. Las operaciones sobre la red informática junto con las operaciones electrónicas se utilizan para atacar, engañar, degradar, interrumpir las comunicaciones del adversario y a su vez negar, explotar y defender la infraestructura de informatización y electrónica propia o aliada.*

Las operaciones de información consisten en las medidas adoptadas a través del uso de las redes informáticas, para interrumpir, denegar, degradar o destruir información residente en ordenadores y redes informáticas, o las computadoras y propias redes.

Implica además acciones tomadas a través de la utilización de redes de ordenadores para proteger, controlar, analizar y responder a la actividad no autorizada en los sistemas de información en todas las operaciones militares, fundamentalmente de los mayores niveles de la conducción.[21] *"*

Como la capacidad de las computadoras y las capacidades de transportes de los sistemas de redes aumentan día a día, nuevas debilidades y oportunidades continuaran apareciendo, y será el ingenio humano el que continuara estando a la vanguardia como principal factor para afectar las redes informáticas.

Las operaciones sobre la función Comando y Control.

Si se toman las Operaciones de Información destinadas a disminuir la capacidad de comando y control, van desde eliminar físicamente al comandante enemigo hasta la destrucción de los Centros de Comando.

No obstante, más importante que la destrucción física del Comandante, siempre ha sido más efectiva la destrucción de los centros de comando. Aunque es natural que concentrar las estructuras de comando en un espacio reducido es una debilidad muy grande, todos los intercambios de información que involucren dirección y decisión tienden a concentrarse en espacios reducidos. Hoy los centros de comando son relativamente fáciles de identificar, porque tienen equipos de comunicaciones e informática visibles asociados a emisiones electromagnéticas, y por el movimiento físico de personas y toda clase de efectos.

Los sistemas de comando y control pueden ser inhabilitados si se les corta la energía, si se los interfiere electromagnéticamente o si se les importa *malware* en sus sistemas informáticos. A pesar de ello, ninguno parece ser más importante que la destrucción física, ya que la mayoría de las armas denominadas *blandas* requieren conocer la exacta ubicación del centro de comando en el terreno.

[21] Ibidem 6.

Se puede disminuir el tamaño de las computadoras, las emisiones de comunicaciones enmascararse electrónicamente, o reemplazarse por una red redundante de cables o *relays* de trasmisión fuera de la vista. Todas las redes generalmente pueden descentralizarse. Las reuniones pueden reducirse por video conferencias en línea. La energía eléctrica puede ser provista o suplementada por generadores, o por energía proveniente de células solares dispersas, de forma tal que no revele la ubicación del centro de comando.

Estos medios facilitan que un centro de comando puede no ser diferenciado de cualquier otro espacio habitado. Si se fracasa en este ocultamiento, el grado en que una instalación de comando pueda ser dañada dependerá de la existencia de una arquitectura de nodos de reemplazo.

La influencia potencial de las operaciones de comando y control descansa en la arquitectura de las relaciones entre los componentes. En culturas militares que restringen ampliamente la iniciativa, cortar los delgados lazos entre la cabeza y el cuerpo puede fácilmente inmovilizar al cuerpo. Pudo verse en la Guerra del Golfo en el bando iraquí, donde la ausencia de órdenes motivó la parálisis de las tropas desplegadas en el terreno, sin que mostrara ninguna respuesta creativa o la iniciativa suficiente para resolver la situación. Un oponente sin flexibilidad y sin iniciativa asegura una clara posibilidad de éxito.

No obstante, otras culturas militares fomentadas en época de paz pueden permitirles más autonomía a los comandantes locales. Esto permite el ejercicio de iniciativa que compensa las fallas propias de una carencia de coordinación que podía haber resultado de la ausencia de conducción central. Una cultura militar burocrática antes que las tecnologías, va a determinar el grado de vulnerabilidad de cualquier sistema de información.

Interrumpir estas líneas de comunicaciones es algo antiguo; lo que es nuevo es el actual volumen de comunicaciones en la era de la información, para dimensionar esto podemos mencionar que algunos autores consideran que la cantidad de información que una persona recibe en un año en la actualidad equivaldría a diez años en la edad media.

El impacto del ataque depende del adelanto tecnológico que tenga el oponente.

Cuando finalizó la Guerra del Golfo donde el primer Plan de Operaciones consistía en destruir las instalaciones de comando y control iraquíes, los aliados se dieron cuenta que quedaban más que los iniciales, a pesar del número que destruyeron.

No obstante, parece ser que los iraquíes tenían muchos sistemas de comunicaciones, más aún de los que se conocían, desde sistemas de radio hasta líneas telefónicas rurales que contratistas de petróleo occidentales habían dejado en el lugar y que unían a las principales ciudades.

Claro que esto fue una redundancia de medios accidental, que es menos eficiente que una redundancia de medios planeada.

El ataque sobre el comando y control puede rendir mejores frutos si se degrada a los sistemas y no se los destruye totalmente. Si se destruyen canales de comunicación seguros, eso va a inducir al uso de canales menos seguros y eso generará demoras en la reacción, permitiendo obtener tiempo para el atacante.

El impacto de la denominada Revolución de Asuntos Militares en las tecnologías de información permite ahora reducir la vulnerabilidad de los centros por la duplicación de los sistemas, y ahora no puede asegurarse que todos los centros de comando puedan ser destruidos en el primer intento.

Conclusiones particulares.

La importancia de las Operaciones de Información se ha acentuado con la aparición y desarrollo de la denominada tecnología de la información. Aunque no se disponga de todos los adelantos tecnológicos, para poder tomar contramedidas será necesario conocer cómo se ejecutan.

Toda esta proliferación de información afectará la rapidez en la toma de decisiones, los conocimientos se vuelven rápidamente obsoletos y se puede decidir erróneamente, con lo cual se incrementan los riesgos a la hora de asesorar y como consecuencia aumenta la incertidumbre para el decisor.

Dentro de las operaciones de información y en un orden decreciente concluimos que serán las operaciones sobre la mente de los individuos, las operaciones de seguridad para obtener información y llevar a cabo operaciones, operaciones sobre las redes informáticas y por último las operaciones sobre la función de comando y control, las que cumplen el análisis AFA (aptitud, factibilidad y aceptabilidad) de poder ser ejecutadas a través de las redes sociales; en función de las capacidades que tienen las redes sociales de facilitar la interacción del personal integrante de las distintas fracciones.

Capítulo 2: Herramientas a utilizar en las redes sociales.

> *"Pero, vamos, pasa a otro tema y canta la estratagema del caballo de madera que fabricó Epeo con la ayuda de Atenea; la emboscada que en otro tiempo condujo el divino Odiseo hasta la Acrópolis, llenándola de los hombres que destruyeron Ilión."*[22]

El objetivo del presente capítulo es determinar cuáles son las herramientas más idóneas que puede utilizar el oponente para llevar adelante operaciones de información en las redes sociales.

Siendo el enfoque del presente trabajo posibles formas para contrarrestar operaciones de información sobre las redes sociales y siendo estas las principales vías para desarrollar las mismas (operaciones sobre la mente de los individuos, las operaciones de seguridad para obtener información y llevar a cabo operaciones, operaciones sobre las redes informáticas y por último las operaciones sobre la función de comando y control), comenzaremos con la descripción del principal procedimiento de reunión de información para la realización de una operación de información.

Uno de los principales procedimientos, sino el principal es la inteligencia sobre las fuentes abiertas OSINT (*acrónimo en inglés Open Source Intelligence*).

Nuestra doctrina no la considera, pero publicaciones especializadas en general la definen como a "proceso de la información obtenida desde fuentes públicas y abiertas".

Normalmente y de la misma forma que evoluciona la tecnología de la información, se diseñan nuevas técnicas de ataque que permiten el acceso o la penetración a los sistemas de seguridad por más complejos y sofisticados que sean.

Los analistas que se ocupen de lograr este objetivo mediante la investigación, son en general personas dotadas de gran paciencia y perseverancia, por la cantidad de tiempo que insume su obtención y proceso.

Normalmente la primera etapa de un ataque informático consiste en la reunión de información que se realiza a través de diferentes procedimientos conocidos con el nombre de "*reconnaissance, discovery, footprinting o Google Hacking"*y la técnica preferida que es ***Open Source Intelligence*** *(Inteligencia de fuentes abiertas).*

Normalmente la información que reúne el atacante, deriva de una paciente investigación sobre el objetivo o blanco, priorizada a obtener la mayor cantidad de información en recursos públicos, como por ejemplo disponible en la web.

Se considera que un adversario que intenta realizar una operación ofensiva invertirá entre el 70% y el 80% de su tiempo en las denominadas actividades de reconocimiento y reunión de información, porque cuanto más sabe el atacante del objetivo, más fácil será obtener el éxito de la operación ofensiva.

[22] La Odisea de Homero, Canto VIII, 490. Citado en el artículo del Lic Jorge Mieres "Ataques Informáticos".

La producción de inteligencia sobre el objetivo se realiza desde varios meses antes de comenzar con las *"primeras interacciones lógicas contra el objetivo a través de diferentes herramientas y técnicas como el scanning, banner grabbing (captura de titulares) y rastreo de los servicios públicos".*

Estas actividades en general son muy leves, buscando simplemente verificar los datos o buscar huecos o fallas en los sistemas.

Los responsables de las organizaciones, sean jefes o comandantes dependiendo de los niveles, o los miembros del estado mayor que se especialicen en la explotación de internet descubrirán, con no menor sorpresa, el volumen de información de las diferentes organizaciones que se encuentra en la misma, no solo información de la organización sino también información personal y actividades de los integrantes de la misma.

Podemos citar como ejemplo de lo antes mencionado a pruebas desarrolladas con programas de los denominados P2P (conexión puerto a puerto, emule, ares, torrent entre otros), que posibilitaron encontrar disponible en internet información de cuadros de organización e información de las unidades.

A modo de ejemplos concretos cito las características de la información que se puede obtener realizando *OSINT:*[23]

· Los nombres de sus altos jefes/ejecutivos y de cualquier empleado pueden ser obtenidos desde comunicados de prensa".
· La dirección de la empresa, números telefónicos y números de fax desde diferentes registros públicos o directamente desde el sitio web.
· Qué, o cuáles, empresas proveen el servicio de Internet (ISP) a través de técnicas sencillas como DNS lookup y traceroute.
· La dirección del domicilio del personal, sus números telefónicos, currículum vitae, datos de los familiares, puestos en los que desempeña funciones, antecedentes penales y mucho más buscando sus nombres en diferentes sitios.
· Los sistemas operativos que se utilizan en la organización, los principales programas utilizados, los lenguajes de programación, plataformas especiales, fabricantes de los dispositivos de networking, estructura de archivos, nombres de archivos, la plataforma del servidor web y mucho más.
· Debilidades físicas, accesspoint, señales activas, endpoint, imágenes satelitales, entre otras.
· Documentos confidenciales accidentalmente, o intencionalmente, enviados a cuentas personales de personas que no en la actualidad no guardan relación alguna con la organización, más allá del paso por la misma.
·Vulnerabilidades en los productos utilizados, problemas con el personal, publicaciones internas, declaraciones, políticas de la institución.
· Comentarios en blogs, críticas, jurisprudencia y servicios de inteligencia competitiva."[24].

[23] La información que se cita es a modo de ejemplo y considero que sirve claramente de ejemplo de información de interés militar que se puede obtener mediante OSINT.
[24] Lic Jorge Mieres, Ataques Informáticos, www.evilfingers.com (enero 2009).

El límite que un atacante puede tener para la obtención de información de fuente públicas abiertas depende prácticamente y casi exclusivamente de las características personales y del tiempo que se disponga para realizar el ataque, en función que cada información que se descubre lleva necesariamente a vincularla con otra y producir nuevo conocimiento.

A continuación desarrollaremos posibles formas de ejecución de las distintas formas particulares de las operaciones de información, determinadas como más factibles a ejecutar, en el capítulo 1, sobre las redes sociales.

Operaciones para afectar la voluntad de lucha.

Cualquier manipulación de datos personales, difamación a través de perfiles falsos de imágenes o video provocará la afectación a la voluntad de lucha al producir en el individuo la sensación de inseguridad, de sentirse desprotegido y ver que mientras él se encuentra combatiendo o afectado a una misión militar, su entorno o seres queridos podrían estar recibiendo a través de las redes sociales información intencionalmente manipulada para menoscabar la escala de valores en los cuales el individuo y su entorno se han desarrollado.

Las operaciones para afectar la voluntad de lucha son netamente ofensivas en esencia.

Teniendo en cuenta según lo describe el Lic. Jorge Mieres, *"La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos.*

Bajo esta perspectiva, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades en alguno de los tres elementos de seguridad.

Para que, conceptualmente hablando, quede más claro de qué manera se compromete cada uno de estos elementos en alguna fase del ataque, tomemos como ejemplo los siguientes casos hipotéticos según el elemento que afecte.

Confidencialidad. *Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (ARP Poisoning).* Se entiende por ataque de ARP a la ejecución del mismo desde una máquina controlada o bien la máquina del atacante está conectada directamente a la red.

Integridad. *Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información.*

El ataque no se lleva a cabo de manera directa contra el sistema de cifrado pero sí en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede

convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado.

Disponibilidad. *En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información".*[25]

Engaño Militar.

Los procedimientos ofensivos sobre redes sociales y redes informáticas se basan en la explotación de las debilidades del factor humano, que se transforman en vulnerabilidades, a través del engaño y son los denominados procedimientos de ingeniería social, destacamos en este punto que le asignamos la denominación de uso civil en lo que se refiere a seguridad de redes informáticas porque la doctrina militar no considera ningún procedimiento particular.

"La Ingeniería Social como técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a una sistema u organización explotando ciertas características que son propias del ser humano.

Sin lugar a dudas, las personas constituyen uno de los problemas más importantes de seguridad para cualquier organización porque a diferencia de los componentes tecnológicos, son el único elemento, dentro de un entorno seguro, con la capacidad de decidir "romper" las reglas establecidas en las políticas de seguridad de la información.

Ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización.

Por ejemplo, en este sentido, la confianza y la divulgación de información son dos de las debilidades más explotadas para obtener datos relacionados a un sistema."[26]

Operaciones de seguridad para obtener información y llevar a cabo operaciones.

En general se tiende a creer que los equipos que se dedican a atacar sistemas informáticos son personas de identidad encubierta que operan de lugares remotos y en horarios impensados, en algunos casos es cierto pero varios registros de incidentes y hechos dados a conocer han demostrado que los realizan los mismos integrantes de las organizaciones desde dentro de las mismas.

Lo antes mencionado es lo denominado en seguridad informática "Factor Insider" es decir, que los mismos integrantes de la organización desde adentro realizan la violación del sistema de seguridad de la organización.

"Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización. Por ejemplo, el atacante podría

[25] Ibídem 23.
[26] Ibídem 23.

conseguir un empleo en la organización que desea atacar y obtener el suficiente nivel de confianza en la organización para luego explotar los puntos de acceso. Del mismo modo, cualquier integrante puede convertirse en un empleado disgustado y decidir robar información y/o causar daños como una forma de venganza.

Cuando este tipo de actos es cometido con intenciones de obtener beneficios económicos a través de información corporativa, es denominado Insiders Trading (comercio de personal interno)"[27].

Si bien en el párrafo anterior se hace mención a integrantes de la organización que realizan la extracción de información en forma intencional, consideraremos también como una forma de salida a la publicación de información propia de la organización en distintos formatos a través de las redes sociales en forma inintencional y con la sola intención de fomentar el ego propio del individuo o dar a conocer sus actividades dentro de la organización. (Ejemplo de esto es la colocación en perfiles de facebook, de fotografías utilizando material de reciente adquisición o actividades de instrucción o adiestramiento con nuevos sistemas de armas, como así también la publicación de actividades de adiestramiento realizadas o próximas a realizarse).

Operaciones sobre la red informática.

Las operaciones sobre la red informática son de las operaciones de información la que requiere mayores medios tecnológicos o con capacidades superiores a los del adversario y el personal operador con mayor capacitación técnica específica.

Básicamente la operación sobre la red informática consistirá en la introducción de software, denominado código malicioso o malware, el cual facilitará el acceso a la información de los equipos informáticos a través de una red ya sea vía cable o inalámbrica.

"Los códigos maliciosos, o malware, se refieren a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.

Actualmente, casi el 80% de los ataques informáticos llevados a cabo por códigos maliciosos, se realizan a través de programas troyanos. Este tipo de malware ingresa a un sistema de manera completamente subrepticia activando una carga dañina, denominada payload, que despliega las instrucciones maliciosas.

La carga dañina que incorporan los troyanos puede ser cualquier cosa, desde instrucciones diseñadas para destruir algún sector del disco rígido, eliminar archivos, registrar las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, entre tantas otras actividades.

Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de códigos maliciosos. Por ejemplo, cuando han ganado acceso a través del troyano, implantan en el sistema otros códigos maliciosos como rootkits que permite esconder las huellas que el atacante va dejando en el equipo (Covering Tracks), y backdoors para volver a ingresar al sistema cuantas veces considere necesario; todo, de manera remota

[27] Ibídem 23.

y sin que, en la mayoría de los casos, los administradores de la red adviertan su actividad.

Si bien cualquier persona con conocimientos básicos de computación puede crear un troyano y combinar su payload con programas benignos a través de aplicaciones automatizadas y diseñados para esto, los troyanos poseen un requisito particular que debe ser cumplido para que logren el éxito: necesitan la intervención del factor humano, en otras palabras, tienen que ser ejecutados por el usuario.

Es por ello que estas amenazas se diseminan por medio de diferentes tecnologías como dispositivos USB, mensajería instantánea, redes P2P, e-mail, etcétera; a través de alguna metodología de engaño (Ingeniería Social), aparentando ser programas inofensivos bajo coberturas como protectores de pantalla, tarjetas virtuales, juegos en flash, diferentes tipos de archivos, simulando ser herramientas de seguridad, entre tantos otros.

Con respecto a los ataques internos, Factor Insiders, suele ser común la ejecución de malware por parte de los empleados, instalar programas keyloggers o realizar ataques, con el ánimo de capturar información privada como datos de autenticación."[28]

Otro punto a considerar y de no menor importancia por la creencia que está instalada en el común de las personas es sobre el falso concepto de seguridad que brindan las contraseñas de accesos a los distintos servicios brindados sobre las redes sociales.

De por si las contraseñas brindan la suficiente protección en función de la cantidad de caracteres de las mismas, el principal inconveniente radica en el individuo, que al tener que ser de más de diez caracteres se le dificulta su memorización y se tiende a colocar la misma en los diferentes sitios o accesos a redes además de escribirla en lugares de relativamente fácil acceso para evitar su pérdida con lo cual se tiende a que la contraseña pierda la seguridad implícita en sí misma, como se demuestra con el texto a continuación.

"Otro de los factores comúnmente explotados por los atacantes son las contraseñas. Si bien en la actualidad existen sistemas de autenticación complejos, las contraseñas siguen, y seguirán, siendo una de las medidas de protección más utilizadas en cualquier tipo de sistema informático.

En consecuencia, constituyen uno de los blancos más buscados por atacantes informáticos porque conforman el componente principal utilizado en procesos de autenticación simple (usuario/contraseña) donde cada usuario posee un identificador (nombre de usuario) y una contraseña asociada a ese identificador que, en conjunto, permiten identificarse frente al sistema.

En este tipo de proceso, llamado de factor simple, la seguridad del esquema de autenticación radica inevitablemente en la fortaleza de la contraseña y en mantenerla en completo secreto, siendo potencialmente vulnerable a técnicas de Ingeniería Social cuando los propietarios de la contraseña no poseen un adecuado nivel de capacitación que permita prevenir este tipo de ataques.

Si el entorno informático se basa únicamente en la protección mediante sistemas de autenticación simple, la posibilidad de ser víctimas de ataques de cracking o intrusiones no autorizadas se potencia. Sumado esto a que existen herramientas automatizadas

[28] Ibídem 23.

diseñadas para "romper" las contraseñas a través de diferentes técnicas como ataques por fuerza bruta, por diccionarios o híbridos en un plazo sumamente corto, el problema se multiplica aún más.

Sobre la base de lo anteriormente explicado, se puede suponer que la solución ante este problema es la creación de contraseñas mucho más largas (lo cual no significa que sean robustas). Sin embargo, esta estrategia sigue siendo poco efectiva.

Si bien es cierto que una contraseña que supere los diez caracteres y que las personas puedan recordar, es mucho más efectiva que una contraseña de cuatro caracteres, aún así, existen otros problemas que suelen ser aprovechados por los atacantes. A continuación se expone algunos de ellos:

· La utilización de la misma contraseña en varias cuentas y otros servicios.

· Acceder a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos como keyloggers que capturen la información.

· Utilización de protocolos de comunicación inseguros que transmiten la información en texto claro como el correo electrónico, navegación web, chat, etcétera.

· Técnicas como surveillance (videoconferencia) o shoulder surfing (mirar por detrás del hombro), entre otras tantas, que permiten evadir los controles de seguridad."[29]

Normalmente el software que se utiliza en los equipos militares es de uso dual sobre todo en lo que se refiere a sistemas operativos, pudiendo tener programas propios para aplicaciones particulares de uso específico militar, con lo cual el problema de las contraseñas está latente en todos los sistemas.

Otro inconveniente que se plantea al trabajar con software propio de redes sociales o de uso en sistemas informáticos es el uso de las denominadas "Configuraciones predeterminadas", que normalmente tienden a dejar accesos abiertos sea con intención o sin ella en la idea de facilitar el uso del programa.

*"Las **configuraciones por defecto**, tanto en los sistemas operativos, las aplicaciones y los dispositivos implementados en el ambiente informático, conforman otra de las debilidades que comúnmente son poco atendidas por pensar erróneamente que se tratan de factores triviales que no se encuentran presentes en la lista de los atacantes.*
Sin embargo, las configuraciones predeterminadas hacen del ataque una tarea sencilla para quien lo ejecuta ya que es muy común que las vulnerabilidades de un equipo sean explotadas a través de códigos exploit donde el escenario que asume dicho código se basa en que el objetivo se encuentra configurado con los parámetros por defecto.
Muchas aplicaciones automatizadas están diseñadas para aprovechar estas vulnerabilidades teniendo en cuenta las configuraciones predeterminadas, incluso, existen sitios web que almacenan bases de datos con información relacionada a los nombres de usuario y sus contraseñas asociadas, códigos de acceso, configuraciones, entre otras, de los valores por defecto de sistemas operativos, aplicaciones y dispositivos físicos. Sólo basta con escribir en un buscador las palabras claves "default passwords" (contraseña por defecto) para ver la infinidad de recursos disponibles que ofrecen este tipo de información."[30]

[29] Ibídem 23.
[30] Ibídem 23.

Operaciones para afectar la función de comando y control.

Cada una de las tareas o actividades puntualizadas anteriormente como partes de una operación de información actuarán también más allá de cumplir con su finalidad propia afectando a los sistemas de la función de comando y control.

Tomando como ejemplo el artículo “Ataques Informáticos” del Lic. Jorge Mieres y trasladándolo a la actividad específica de una fuerza militar ya sea en operaciones o en tiempo de paz, podemos comprobar que realizando inteligencia sobre fuentes abiertas, perfiles de facebook, twiter, correos electrónicos, linkedin y cualquier otra red social de acceso común se puede obtener un caudal de información tal que se puede afectar a la función de comando y control relativamente fácil, obviamente disponiendo del hardware (equipos informáticos) y del personal capacitado para dirigir la operación como para operar los equipos informáticos.

A través de la OSINT (inteligencia sobre las fuentes abiertas), se puede obtener números telefónicos, prestadores de servicios de internet, datos personales, identificación de los equipos informáticos conectados a una red, dispositivos de networking, estructura de archivos, nombres de archivos, plataformas de servicios web, debilidades físicas y forma en que se puede actuar sobre la misma para ingresar subrepticiamente y modificar funciones, obtener información o anular directamente la operación de los mismos.

Además de la afectación de los sistemas de la misma forma con la información que se obtiene se puede afectar a los operadores de la organización obteniendo información particular o creando falsos perfiles que generen menoscabo sobre los valores tradicionales esgrimidos en la organización (atentar contra la disciplina, contra la familia, contra características propias de la personalidad y gustos del individuo, difamación o simulando ingresos a páginas o entornos que atentan contra los valores de la institución).

En resumen estaríamos afectando a los dos componentes básicos de un sistema de comando y control, los medios técnicos y los medios humanos.

En general con cada dato que se descubre o se encuentra a través de un entorno de redes sociales se puede seguir descubriendo más información y continuar avanzando con las posibilidades de mayores variantes para afectar al sistema de comando y control.

Si bien cada uno de los procedimientos que hemos detallado, los hemos particularizado haciendo hincapié sobre la operación o tarea particular para la cual son más aptos, lo normal en el entorno complejo de una operación de información será que se utilicen todos o por lo menos más de uno para incrementar la sinergia propia que genera la operación de información.

Conclusiones particulares.

El acceso a la información de una organización que facilitan las redes sociales a través de sus integrantes, genera una fuente de información de un volumen e importan-

cia tal que permite la planificación de operaciones de información para desarticular todos sus subsistemas.

El proceso de obtención de información es un proceso paciente y particularizado para lograr la integridad y objetividad necesaria para la inteligencia producida a fin de fijar las bases para el planeamiento de las operaciones de información.

Logrado el acceso al sistema, se buscará no dejar huellas visibles que permitan detectar el ingreso, para de esa forma ingresar a los equipos cada vez que se necesite, sin tener en cuenta desde donde se accede, para de esta forma lograr el máximo control posible sobre el objetivo, tratando de evitar la detección por el mayor tiempo posible.

La información y los recursos se deben proteger mientras tengan el suficiente valor que justifique su seguridad, protegiendo tanto los datos, los recursos y la “reputación de la institución” y por lo tanto en función de esto se instrumentan las medidas de seguridad de contrainteligencia.

Normalmente las mayores vulnerabilidades se presentan a través de los integrantes de la organización que por diversos motivos facilitan la obtención de información al oponente de diversas formas y maneras.

Capítulo 3: Medidas de Seguridad de contrainteligencia a aplicar.

El objetivo específico de este capítulo es determinar cuáles serán las medidas de seguridad de contrainteligencia para proteger a los propios medios y sistemas de la acción del enemigo.

Habiendo sido determinado a los efectos particulares del presente trabajo, en el capítulo dos, cuáles serán las herramientas más idóneas que puede utilizar el oponente para llevar adelante operaciones de información sobre las redes sociales que puedan afectar a la propia fuerza, llega ahora la oportunidad de desarrollar las posibles contramedidas para proteger preventivamente de manera efectiva los propios medios y sistemas de la acción del oponente.

Destacamos que para minimizar el impacto negativo provocado en la organización por las operaciones de información del oponente existen tácticas y procedimientos que facilitan las contramedidas y a su vez reducen considerablemente el campo de acción de las operaciones de información del oponente, pero a pesar del avance constante de la tecnolo-gía sigue siendo la principal y más importante medida: “La Educación”, en lo que se refiere al manejo de la información y de los sistemas afines como así también en el conocimiento de las debilidades del eslabón más débil que es el hombre.

A continuación desarrollaremos posibles formas de ejecución de las principales medidas de seguridad de contrainteligencia para contrarrestar las distintas formas particulares de las operaciones de información sobre las redes sociales.

Operaciones para afectar la voluntad de lucha.

Cualquier manipulación de datos personales, difamación a través de perfiles falsos de imágenes o video provocará la afectación a la voluntad de lucha al producir en el individuo la sensación de inseguridad, de sentirse desprotegido y ver que mientras él se encuentra combatiendo o afectado a una misión militar, su familia o seres queridos podrían estar recibiendo a través de las redes sociales información intencionalmente manipulada para menoscabar la escala de valores en los cuales el individuo y su entorno se han desarrollado.

Ante la vulnerabilidad de los datos personales, la medida de seguridad de contrainteligencia más eficaz sería que el individuo no esté en ninguna red social on line, así no habría ningún problema sobre la privacidad y la seguridad.

Pero esta medida es prácticamente inviable, en la actualidad, porque se ha producido un cambio en el paradigma de la comunicación en donde la denominada conectividad ha pasado a ser casi una necesidad del individuo, por lo tanto su suspensión creará un ambiente contraproducente menoscabando la moral y dando el espacio necesario para que el oponente lleve adelante operaciones psicológicas para afectar al entorno del combatiente ante la ausencia de este en el ciberespacio.

Ante lo cual se debe buscar que los datos personales, como la misma palabra indica sean personales y privados, posibilitando sobre servidores seguros que los individuos conecten sus dispositivos y obviamente con una adecuada política de seguridad y el compromiso suficiente con la institución en cuanto a la preservación se refiere y obviamente aparece como principal medida de seguridad de contrainteligencia la educación del individuo.

Se debe tratar que un usuario divulgue el mínimo de información o información falsa sobre el perfil de usuario para que en el momento que sus emisiones privadas pasen a ser públicas en la red se dificulte la obtención de información útil al oponente. Ejemplo de acciones sencillas a realizar puede ser la publicación de fechas importantes en forma incorrecta, utilizar sobrenombres o alias etc.

Utilizar la función que permite al usuario seleccionar que información del perfil será visible para los demás usuarios o contactos.

Otra medida de seguridad de contrainteligencia que surge como contrapartida son las denominadas operaciones psicológicas defensivas o de protección, para obviamente preservar a los individuos y a la institución de las acciones del oponente, a través de distintos productos.

Engaño Militar.

Luego de la descripción realizada en el capítulo dos de los denominados procedimientos de ingeniería social, surge que como principal medida de seguridad de contrainteligencia, nuevamente es la educación. Todos los integrantes de la organización desde el ápice estratégico hasta el menor nivel de la organización independiente de los métodos y procedimientos de trabajo, deben estar instruidos y adiestrados en cuanto a las debilidades y procedimientos de engaño más empleados sobre las redes sociales, para que de esta forma logren detectarlos y dar la alerta correspondiente sobre cualquier indicio que se produzca sobre sus equipos o respectivos perfiles en las redes sociales. Sirve mencionar de ejemplo los casos de cambios de perfiles o falsos perfiles para accionar sobre las redes sociales.

Esto no significa que todo el personal integrante de la organización deba realizar cursos específicos afines a seguridad informática y en las redes sociales, sino que es algo mucho más profundo que tiene que ver con la concientización sobre los riesgos que implica y las ventajas que puede obtener el enemigo de nuestros propios errores o mal uso de las redes. Dentro del proceso educativo (instrucción y adiestramiento) deben desarrollarse planes de concientización sobre las denominadas medidas de seguridad de contrainteligencia en lo que se refiere a seguridad informática y sobre redes sociales.

El personal para evitar el engaño debe consultar la información personal recibida a través de las redes sociales por lo menos a través de dos medios distintos, por ejemplo las redes sociales y una llamada telefónica, esto que es un procedimiento normal de trabajo del personal de inteligencia debe ser enseñado a todo el personal integrante de las distintas organizaciones.

"Es muy común que el personal crea erróneamente que su posición dentro de la institución es de poca importancia y que por lo tanto no podrían ser objeto de ataque, pero contrariamente, son en realidad los objetivos preferidos por los atacantes; en consecuencia, la educación es una contramedida muy efectiva, pero es de suma importancia que las personas tomen real conciencia de que ellos son el blanco perfecto de la ingeniería social.[31]

Operaciones de seguridad para obtener información y llevar a cabo operaciones.

Las medidas de seguridad de contrainteligencia son para afectar al denominado "Factor Insider" (integrantes de la institución que desde adentro realizan la violación del sistema de seguridad de la organización).

Teniendo en cuenta que la extracción de información en forma intencional, también incluye la publicación de información propia de la organización en distintos formatos a través de las redes sociales en forma inintencional y con la sola intención de fomentar el ego propio del individuo o dar a conocer sus actividades dentro de la organización, tal como fue indicado en el capítulo dos.

Como principales medidas de seguridad de contrainteligencia para protegerse del denominado "factor insider", se encuentran las denominadas en seguridad informática *"estrategias internas y específicas para el control de posibles ataques ocasionados por el personal de la organización."*[32]

Y las mismas se encuentran en el apoyo tecnológico, en lo referido al uso de programas "*keyloggers(mecanismos que impiden por software o hardware la instalación de programas por parte del personal, estricta configuración del principio de privilegios mínimos, des- habilitación de puertos USB y prohibición del uso de dispositivos de almacenamiento extraíbles para evitar la fuga de información y entrada de otras amenazas tales como malware, si las computadoras forman parte de un dominio es necesario establecer políticas rigurosa en el Active Directory, entre otras.).*[33] Un ejemplo de esta acción son las redes internas en donde los usuarios tienen las denominadas terminales "bobas" y deben concurrir a donde se encuentra el servidor para desde ahí utilizar los periféricos de entrada o salida.

"*…si piensas que la tecnología puede resolver todos los problemas de seguridad, entonces no entiendes el problema y no entiendes la tecnología.*"[34]

Operaciones sobre la red informática.

Básicamente la operación sobre la red informática consistirá en la introducción de software, denominado código malicioso o malware, el cual facilitará el acceso a la información de los equipos informáticos a través de una red, ya sea vía alámbrica o inalámbrica.

[31] Lic. Jorge Mieres, Ataques Informáticos, www.evilfingers.com (enero 2009).
[32] Ibídem 30.
[33] Ibídem 30.
[34] Bruce Schneier, Secrets & Lies, citado en el Articulo del Lic. Jorge Mieres.

Las medidas de seguridad de contrainteligencia tendientes a proteger y prevenir operaciones sobre la red informática están basadas principalmente en la instalación de software antivirus que operen bajo mecanismos de detección complejos que se basan en la "heurística"[35], y que también permitan el control y la administración de manera centralizada cada uno de los nodos involucrados en la red, junto a planes de instrucción y adiestramiento orientados a crear conciencia en el personal sobre los riesgos de seguridad que representa el malware.

Haciendo ahora referencia a las medidas de seguridad de contrainteligencia con respecto a las contraseñas, en la actualidad la que permite una mayor fiabilidad es implementar mecanismos de autenticación de los denominados de doble factor, esto significa que no solo es necesario saber una combinación de caracteres alfanuméricos sino también es necesario contar con un mecanismo físico tal como una llave electrónica USB o una tarjeta que almacene certificados digitales para que a través de ellos se pueda validar o no el acceso de los usuarios a los recursos de la red.

Nuestra doctrina denomina a esta actividad como "Administración de Contraseñas Críticas".

"En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.

Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa. Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.

La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.

Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.

Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas.

Dicho registro será revisado posteriormente por el Responsable de Seguridad."[36]

---

[35] En computación, dos objetivos fundamentales son encontrar algoritmos con buenos tiempos de ejecución y buenas soluciones, usualmente las óptimas. Una **heurística** es un algoritmo que abandona uno o ambos objetivos; por ejemplo, normalmente encuentran buenas soluciones, aunque no hay pruebas de que la solución no pueda ser arbitrariamente errónea en algunos casos; o se ejecuta razonablemente rápido, aunque no existe tampoco prueba de que siempre será así. Las heurísticas generalmente son usadas cuando no existe una solución óptima bajo las restricciones dadas (tiempo, espacio, etc.), o cuando no existe del todo. En definitiva técnicas para reconocer códigos maliciosos. (www.infospyware.com InfoSpyware.com, www.av-comparatives.org AV-Comparatives)

[36] Manual de Seguridad Informática – Ejercito Argentino Ed. 2012.

Con referencia al control de acceso a una red informática, independientemente que sea inter o intranet en general se deberá cumplir con la reglamentación establecida por la institución como punto de partida para proteger los sistemas.

"Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos. El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia. Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la Fuerza. Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:
(1) Identificar las redes y servicios de red a los cuales se permite el acceso.
(2) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
(3) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red. " [37]

Con respecto a la debilidad que presenta el problema de las "Configuraciones predeterminadas", en la idea de cerrar accesos abiertos, sea con intención o sin ella, consiste simplemente en cambiar los valores por defecto, teniendo en cuenta de no caer en los extremos de la seguridad que provoque la falta de disponibilidad de recursos que hagan del equipo ineficaz para el trabajo para el cual fue adquirido. Se debe buscar el justo equilibrio entre seguridad y disponibilidad o acceso a los recursos del equipo informático sin que pierda las capacidades para la cual fue pensado.

La actividad de protección de los equipos modificando los valores por defecto, en seguridad informática se denomina "hardening", y esta actividad recae en los responsables de SCD (Servicio de Computación de Datos).

Cuando se determinan las medidas de seguridad de contrainteligencia se debe determinar que tareas incluyen el proceso de *hardening*, opciones de instalación de sistemas operativos y demás recursos, nombres de directorios, carpetas, componentes, servicios, configuraciones y otros ajustes que brinden un adecuado nivel de protección.

Operaciones para afectar la función de comando y control.

Las medidas de seguridad de contrainteligencia referidas a OSINT, se diferencian entre la información que al momento se encuentra en internet y la que en el futuro se cargará en fuentes públicas.

La información que al momento ya se encuentra publicada en internet prácticamente siempre estará disponible, aunque sean páginas dinámicas o de gran capacidad de mi-

[37] Ibídem 35.

gración, pudiéndose modificar pero en definitiva por la gran cantidad de buscadores disponibles, siempre se encontrará, no pudiendo eliminarse o solo se podrá modificar en la idea de confundir o engañar a quien realiza la explotación de la fuente pública y por lo tanto continuará afectando a la institución directamente, en definitiva dificultará su rastreo o monitoreo.

Con respecto a la información que se publicará, antes de hacerlo debe ser controlada para que cumpla con la clasificación de seguridad de la misma, además de verificar su impacto desde el punto de vista táctico y estratégico, algo que hoy puede ser considerado un dato menor en el futuro puede tener implicancias directas sobre la institución y sobrados ejemplos vemos en estos días en los medios de comunicación social con la publicación de información acerca de las instituciones.

En general con cada dato que se descubre o se encuentra a través de un entorno de redes sociales se puede seguir descubriendo más información y continuar avanzando con las posibilidades de mayores variantes para afectar al sistema de comando y control.

Conclusiones particulares.

Se debe tener en cuenta como principal medida de seguridad de contrainteligencia para el uso seguro en las redes sociales del punto de vista técnico, radica en el "*anonimato del usuario"* y de su entorno, este es el nombre genérico del procedimiento, porque en realidad a través del IP (dirección de red de la computadora personal), se puede llegar a una seudo identificación, que pondría al anonimato es un estado relativo.

Utilizar además el software complementado con el hardware necesario para la utilización de servidores y protocolos de seguridad tratando de preservar la integridad de la información para conocer si personas no autorizadas pueden ingresar de alguna forma.

La utilización de firmas digitales con sus distintas variantes producto del avance casi a diario de la tecnología contribuyen a incrementar las restricciones de acceso y determinar la identidad de los participantes, buscando dificultar la identificación del emisor.

Con la tecnología se pueden proteger las contraseñas y a su vez integrarla con lectores biométricos para aumentar sus niveles de seguridad.

Las medidas de seguridad de contrainteligencia a aplicar para contrarrestar o evitar los efectos de una operación de información se llevaran adelante en forma integrada y a través de un trabajo de un equipo multidisciplinario a raíz de la complejidad de las mismas y que en algunos casos no queda claramente determinado el límite entre una actividad y la otra, debiendo ser multi-nivel y multi-lateral.

La educación, seguirá siendo la medida de contrainteligencia más importante en la que deberán invertir las organizaciones para proteger su información clasificada y sus sistemas afines.

CONCLUSIONES FINALES

La importancia de las Operaciones de Información se ha acentuado con la aparición de las denominadas tecnologías de información. Aunque no se disponga de todos los adelantos tecnológicos, para poder tomar contramedidas será necesario conocer cómo trabajan.

La abundancia de información va a causar tres efectos: el primero de ellos será que la información de los diferentes tipos de sensores puede ser contradictoria, y eso va a valorizar más la estimación humana sobre la confiabilidad; el segundo efecto será la proliferación de información que va a tener que ser procesada por el ciclo de producción de inteligencia, antes que llegue como elemento de decisión al Comandante, ya que mucha información será útil, y mucha más solo generará volumen y lentitud en los procesos de la misma, con lo cual se demorará la toma de decisiones; y el tercer elemento devendrá de la disponibilidad de la misma información en todos los niveles, esto sembrará dudas sobre la eficacia y oportunidad de las resoluciones.

Toda esta proliferación de información afectará la rapidez en la toma de decisiones, los conocimientos se vuelven rápidamente obsoletos y se puede decidir erróneamente, con lo cual se incrementan los riesgos para el decisor.

Dentro de las operaciones de información y en un orden decreciente concluimos que serán las operaciones sobre la mente de los individuos, las operaciones de seguridad para obtener información y llevar a cabo operaciones, operaciones sobre las redes informáticas y por último las operaciones sobre la función de comando y control, las que cumplen el análisis AFA (aptitud, factibilidad y aceptabilidad) de poder ser ejecutadas a través de las redes sociales.

El acceso a la información de una organización que facilitan las redes sociales a través de sus integrantes, genera una fuente de información de un volumen e importancia tal que permite la planificación de operaciones de información para desarticular todos sus subsistemas.

El proceso de obtención de información es un proceso paciente y particularizado para lograr la integridad y objetividad necesaria para la inteligencia producida a fin de fijar las bases para el planeamiento de las operaciones de información.

Logrado el acceso al sistema, se buscará no dejar visibles huellas que permitan detectar la intrusión, para de esa forma ingresar a los equipos cada vez que se necesite, sin tener en cuenta desde donde se accede, para de esta forma lograr el máximo control posible sobre el objetivo, tratando de evitar la detección por el mayor tiempo posible.

La información y los recursos se deben proteger mientras tengan el suficiente valor que justifique su seguridad, protegiendo tanto los datos, los recursos y la “reputación de la institución” y por lo tanto en función de esto se instrumentan las medidas de seguridad de contrainteligencia.

Para minimizar el impacto negativo provocado en la organización por las operaciones de información del oponente existen tácticas y procedimientos que facilitan las contramedidas y a su vez reducen considerablemente el campo de acción de las operaciones de información del oponente, pero a pesar del avance constante de la tecnología sigue siendo la principal y más importante medida: “La Educación”, en lo que se refiere al manejo de la información y de los sistemas afines como así también en el conocimiento de las debilidades del eslabón más débil que es el hombre.

Las medidas de seguridad de contrainteligencia en las redes sociales deben buscar accionar permanentemente por acción, para de esa forma tener la iniciativa en lo que se refiere a la protección de la propia fuerza. Si accionamos por reacción estamos perdiendo iniciativa, sorpresa y flexibilidad en las acciones a implementar porque no tenemos la capacidad de realizar la correcta evaluación de las medidas que se implementan y por lógica estamos detrás del problema, en vez de anticiparnos al mismo, siendo la anticipación base en las acciones a llevar adelante a través de la contrainteligencia.

El actual avance tecnológico obliga necesariamente a la constante renovación e innovación en la aplicación de las medidas de seguridad de contrainteligencia en las redes sociales, porque lo que hoy es novedoso, con el amanecer de un nuevo día, ya se encuentra desactualizado.

Por lo tanto nuestra organización se ve obligada a invertir recursos tanto materiales como humanos para por lo menos alcanzar los estándares regionales en lo que ha medidas de seguridad de contrainteligencia en redes sociales se refiere o aunque más no fuere proteger las redes informáticas de las operaciones de información que el oponente puede llevar adelante sobre las mismas.

BIBLIOGRAFIA

a. Reglamentos:

-ROD 11-01 “Inteligencia Táctica”, Ed 2008.
-PC 12-01 “Inteligencia para la Acción Militar Conjunta” (Proyecto), Ed 2007.
-ROP 11-06 “Medidas de Seguridad de Contrainteligencia” Ed 1996 Reim 2007.
-RFP 99-01 “Terminología Castrense de Uso en el Ejercito Argentino” Ed 2001.
-Manual de Seguridad Informática-EA- Ed 2013.
-JP 3-13 “Information Operations”, Defense Department-USA-Feb 2006.
-RDO 2009 “Reglamento de Operaciones de Información” Ejército de Chile – 2010.

b. Libros:

-Kent, Sherman. Inteligencia Estratégica. Segunda Edición, Buenos Aires: Editorial Pleamar, 1978, 249 páginas.
-Koontz, Christopher. Enduring Voices: Oral Histories of the U.S. Army Experience in Afghanistan, 2003-2005. Primera Edición, Washington, D.C.: Center of Military History United States Army, 2008, 582 páginas.
-Brown, S. Todd. Battleground Iraq: Journal of a Company Commander. Primera Edición, Washington, D.C.: Department of the Army, 2007, 306 páginas.
-The United State Army Social Media Handbook. Version 2. Agosto 2011.
-Kevin Mitnick, The Art of Intrusion. Jhon Wiley & Sons, 2005.

c. Revistas Especializadas:

-Grl Div(R) Evergisto de Vergara, Revista de la ESG-Ene Abr 13- “La Seguridad Informática y de Telecomunicaciones de un Estado”.
-Ing Jorge Mieres “Ataques informáticos” Debilidades de Seguridad Comunmente explotados. (www.evilfingers.com) Enero 2009.
-Mayor General Michael Flynn, Capitán Matt Pottinger y Batchelor Paul. Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan. Center for a New American Security, 2010, 28 páginas.
-Libicki Martin, What is Information Warfare, National Defense University, Institute for National Strategy Studies, Washington DC 1996.
-Patrik Thomé, Major, Swedish Army, The Role of Information Operations in Strategy, Conventional War and Low Intensity Conflict, 2006, obtenible en http://www.au.af.mil/info-ops/iosphere/iosphere_summer06_thome.pdf
- Susan Barnes “A privacy paradox: Social Networking in the United States”, First Monday Journal-Volume 11-Number 9-4-September 2006.
- Matías Concha “Análisis de la Primavera Árabe” Periódico de la Universidad Gabriela Mistral de Chile. 26 de junio de 2012.
-Areitio J. “Nuevos enfoques en el análisis de sistemas de detección - prevención y gestión de ataques-intrusiones”. Revista Conectronica Nro 123. Enero 2009.
- Areitio J. “Seguridad de la Información: Redes, Informática y Sistemas de In-

formación". Cengage Learning-Parainfo. 2010.
-Najat Dammou, Sanae Saoud, M. Angustias Martinez Aguilar "Privacidad y seguridad en redes sociales.
- Shafi M. Abdulhamid, Sulaiman Ahmad, Victor O. Waziris, Fatima N. Jibril "Privacidad y asuntos de seguridad nacional en las redes sociales: los retos."- Revista Internacional de la computadora, internet y la gestión Vol 19, N° 3. (Septiembre-Diciembre de 2011) pág. 14-20.

d. **Sitios web**:

-www.eset-la.com/threat-center/1732-informe-malware-america-latina.

-www.econstor.eu/dspace/Nutzungsbedingungen (German Institute for Ecomic Research).

-www.i2integrity.es.

-www.au.af.mil/info-ops/iosphere/iosphere_summer06_thome.pdf.

-www.redeszone.net.

-www.//images-globalknowledge.com