TRABAJO FINAL INTEGRADOR

Título: “Incorporación de ciberanalistas en apoyo a un comando de nivel Componente Terrestre del Teatro de Operaciones”.

Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor RODRIGO DAVID BORDA.

Director de TFI: Teniente Coronel JUAN CARLOS GUERRA

Ciudad Autónoma de Buenos Aires, de junio de 2024.

Resumen

El presente Trabajo Final Integrador se centra en la incidencia creciente que el ciberespacio tiene en el desarrollo de los conflictos actuales y, en consecuencia, en la necesidad de conocer por parte del decisor este nuevo dominio.

En una primera parte, el presente trabajo intenta definir la situación actual en cuanto al desarrollo legal de la República Argentina para determinar la factibilidad de desarrollar acciones en este dominio y los márgenes de acción permitidos por parte de las fuerzas armadas.

El segundo capítulo visualiza la situación estructural de ciberdefensa de la República Argentina y el desarrollo legal estructural de ciberdefensa de países de referencia, tal es el caso de Chile, Estados Unidos e Israel.

El tercer capítulo pone de relevancia la importancia de gestionar el entorno de la organización, cada vez más complejo y dinámico, para posteriormente contrastarlo con la organización del estado mayor de un componente terrestre y el ciclo de producción de inteligencia doctrinarios y vigentes, lo que permite visualizar la ausencia dentro de la organización, de especialistas que obtenga información y/o procese información proveniente del ciberespacio.

Por último, se describen las acciones que se ejecutan en el ciberespacio, el ciclo de inteligencia de fuentes abiertas (OSINT por sus siglas en inglés) y los sistemas de seguridad cibernéticas empleados por las empresas, como posibles formas de gestionar el ciberespacio.

Con el desarrollo de estos capítulos, se analizará la necesidad de incorporar analistas que produzcan ciberinteligencia y proporcionen información del ciberespacio empleando diferentes procedimientos para contribuir con el ciclo de producción de inteligencia en apoyo al comandante de un componente terrestre.

Palabras Clave

ciberespacio – ciberinteligencia – ciclo de producción de inteligencia

Índice de contenidos

Índice de figuras

Figuras **Página**

Introducción

La Cibernética fue creada por Norbert Wiener, profesor de matemáticas del Instituto de Tecnología de Massachusetts, al usar este término en 1984 para describir la teoría de los mecanismos de control como una ramificación de la teoría de los mensajes, pero entendida en un campo más amplio que no solo estudia el lenguaje, sino al mensaje como medio de control de máquinas y de la sociedad entre otros.

La cibernética debe ser entendida como una ciencia multidisciplinaria que incluye la psicología, la inteligencia artificial, la economía, la ingeniería de sistemas de control de organismos vivos, máquinas y organizaciones y los sistemas de comunicaciones. Es una ciencia que a través de la información transforma un resultado deseado. (Wiener, 1988)

Es importante destacar que, si bien el ciberespacio se encuentra concebido por el avance tecnológico, este nuevo dominio es la resultante de un fenómeno social. (Stel, 2005)

A los efectos del presente trabajo, se ha considerado importante mencionar los antecedentes históricos más importantes de acciones ejecutadas en el ciberespacio, las cuales son de difícil atribución y alcance, y describir someramente las múltiples formas de ejecutar ataques en este dominio.

En el año 2007, Estonia fue uno de los primeros países en ser víctimas de los ciberataques dentro de esta nueva forma de hacer la guerra. La agresión demostró la facilidad con la que un oponente puede aprovecharse de las tensiones internas explotando vulnerabilidades en favor propio.

Redes de robots informáticos denominados Botnets enviaban gran cantidad de mensajes basura, es decir, mensajes spam de forma automática para saturar los servidores ejecutando un ataque denominado “denegación de servicio”.

Entre las consecuencias más importantes de este ataque, podemos mencionar el colapso general de páginas web de diferentes organismos gubernamentales, medios de prensa, redes sociales, redes bancarias físicas y virtuales on line, correo electrónico, etc.

Stuxnet, fue un sofisticado malware descubierto en el año 2010, presuntamente creado por las agencias de inteligencia de Estados Unidos e Israel. Fue diseñado para sabotear el programa nuclear iraní a través de la interrupción de las cámaras centrífugas que eran utilizadas para el enriquecimiento de uranio.

Stuxnet demostró la capacidad del ciberespacio como medio para el empleo de ciberarmas que afecten las infraestructuras críticas de un país, y despertó la conciencia de la necesidad de fortalecer los sistemas de seguridad ante este tipo de nuevas amenazas.

El Ciberataque a la empresa Colonial Pipeline tuvo lugar en mayo de 2021. Esta empresa transportaba a través del sistema de tuberías, el 45 % del combustible consumido en la costa estadounidense. El ataque detuvo las operaciones del oleoducto y afectó algunos de los sistemas de información.

En el año 2014 durante el conflicto entre Ucrania y Rusia, se ejecutaron varios incidentes de ciberataques. Estos ataques tuvieron una variedad de propósitos, incluyendo la desinformación, el espionaje, la influencia sobre la percepción pública de los ciudadanos y el sabotaje entre otros.

Respaldados por Rusia, Grupos de hackers (Hacktivismo y espionaje) como Fancy Bear (APT28) y Cozy Bear (APT29) ejecutaron ataques de denegación de servicio (DDos) a sitios web gubernamentales y medios de comunicación con el objetivo de interrumpir la comunicación y la difusión de información en Ucrania, aunque esta afirmación no pudo ser comprobada fehacientemente.

En relación con los antecedentes del tema, el mismo ha sido abordado en diversas publicaciones conjuntas y específicas desde diferentes enfoques, tal es el caso de un Trabajo

Final Integrador de la Escuela Superior de Guerra Conjunta donde el autor plantea la ausencia de un sistema de inteligencia que abarque otros dominios como el ciberespacio, además de los dominios tradicionales (tierra, mar, aire). (Arenas, 2021)

Por otra parte, en un Trabajo Final de Licenciatura de la Escuela Superior de Guerra, el autor propone el diseño de un centro integrador de inteligencia conjunto en apoyo al C2 de un Comando de Teatro de Operaciones, exceptuando a la ciberinteligencia dentro de la organización. (Sponer, 2012)

En un Trabajo Final de Maestría de Ciberdefensa y Ciberseguridad de la Universidad de Buenos Aires, el autor destaca la importancia del enfoque multidimensional y multidisciplinario de los conflictos para enfrentar amenazas de carácter híbrido, mediante el empleo de especialistas expertos en el análisis de sistemas complejos en capacidad de determinar los actores intervinientes y sus interrelaciones, las fortalezas y debilidades, estructuras de apoyo, etc, para que el decisor disponga de un mapa completo y realista de la situación y de las variables que afectan la evolución de la conflicto. (Guerra, 2021)

En este sentido, la doctrina define al ciberespacio como el "Ámbito tanto físico como virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de la información y comunicaciones. Constituye un ámbito de actuación operacional del instrumento militar y otros actores cibernéticos". (EMCO, 2019)

Este escenario cibernético origina nuevas vulnerabilidades y oportunidades para desarrollar capacidades de vanguardia y combatir las nuevas amenazas en un entorno de operaciones multidominio, entendiéndose como el empleo de fuerzas que convergen de manera sincronizada para que, de forma sinérgica, obtener la superioridad mediante la ejecución de

operaciones sobre el enemigo en los cuatro dominios (terrestre, naval, aeroespacial y cibernético), en un momento y lugar determinados, evitando además, el aislamiento de los componentes propios. (EMCO, 2019)

Es en este espacio cibernético, la ciberinteligencia es la aliada perfecta de la ciberdefensa, pues permite el aumento de las capacidades de prevención, detección y respuesta ante la presencia de ciberamenazas, es decir, la ciberinteligencia facilita las operaciones de ciberdefensa para la protección de los sistemas propios. De acuerdo con la doctrina, define a la ciberdefensa como las "medidas y acciones que tienen la finalidad de proteger las infraestructuras críticas del Sistema de Defensa Nacional. Implica el planeamiento y ejecución de operaciones militares en el ciberespacio" (EMCO, 2019)

Es por ello que la capacidad de interpretar lo que está sucediendo en entornos complejos como el ciberespacio, de fronteras borrosas que se desenvuelve en el gris de lo legal e ilegal, con actores que se esconden en el anonimato ejecutando acciones de consecuencias incontrolables, donde la hiperconectividad acelera los procesos de transmisión de información en grandes volúmenes provenientes de diversas fuentes, presentan un verdadero desafío para el proceso de la información y producción de ciberinteligencia por parte del sistema de inteligencia, en lapsos de tiempo sumamente reducidos.

El ciberespacio se presenta como un nuevo dominio no reconocible por los sentidos, un espacio virtual que da contexto al nacimiento de nuevos conceptos de la guerra, nuevas armas y desarrollos tecnológicos, nuevas estrategias y operaciones.

El CTTO dispondría de formaciones acordes a las necesidades del cumplimiento de la misión, pudiendo ser una Agrupación de Inteligencia o Batallones de Inteligencia con capacidad de procesar información y producir inteligencia referida al enemigo, el terreno, las condiciones meteorológicas y otros aspectos particularizados de la Zona de Interés.

Dentro de la estructura orgánica de los elementos de Inteligencia puestos s disposición del CTTO, se encuentran medios de obtención humana, medios de obtención electrónica, medios de obtención aérea, medios de escucha radioeléctrica, además de apoyar al Oficial de Inteligencia con un Centro Integrador de Inteligencia (CII) quien es el que motoriza el ciclo de producción de inteligencia con información proveniente de diferentes medios y fuentes. La información necesaria para procesar, y producir inteligencia, debería provenir de los diferentes dominios, entre los que se encuentra el Ciberespacio.

Con esta breve explicación, intento resaltar la necesidad de disponer de especialistas capacitados en la gestión del ciberespacio, integrando el Centro Integrador de Inteligencia o conformando una organización *per se* para registrar, analizar, sintetizar, integrar e interpretar la información proveniente del ciberespacio a nivel componente terrestre para contribuir al eficiente empleo de los medios de ciberdefensa en la protección del Comando y Control, Sistemas de Armas, Infraestructuras críticas, etc, dado que las consecuencias etéreas o virtuales van mutando hacia consecuencias físicas graves y comprobables contribuyendo de manera significativa en el cumplimiento de los objetivos de la guerra.

Formulación del Problema

Formulación del problema:

¿Cómo procesar información del ciberespacio para abonar al ciclo de producción de inteligencia a nivel componente terrestre del teatro de operaciones?

Objetivos

Objetivo General

Analizar la necesidad de incorporar especialistas de ciberinteligencia y describir los procesos de producción de ciberinteligencia para contribuir con el ciclo de producción de inteligencia de nivel componente terrestre del teatro de operaciones.

Objetivos Específicos

Objetivo Específico uno

Identificar y describir el marco legal vigente en la República Argentina vinculado con la ciberinteligencia, para determinar las limitaciones y posibilidades para actuar en el ciberespacio

Objetivo Específico dos

Identificar y describir el marco legal y las organizaciones de ciberdefensa y ciberinteligencia de países de referencia, para contrastarlos con la realidad propia.

Objetivo específico tres

Describir el estado mayor del componente terrestre y el ciclo de producción de inteligencia doctrinario actual, para destacar la necesidad de procesar información del ciberespacio.

Objetivo Específico cuatro

Definir las características del ciberespacio y las herramientas de producción de ciberinteligencia para establecer la necesidad de proporcionar ciberinteligencia al comandante del componente terrestre.

Metodología a emplear

Explicación del método: Deductivo

Diseño de la estructura: Explicativo

Técnicas de Validación: Análisis Bibliográfico y Análisis Lógico

Capítulo I

Marco Jurídico y doctrinario

Este capítulo se encuentra organizado en 2 secciones, una primera sección general, introductoria y breve donde se mencionan las leyes nacionales vigentes que se encuentran

vinculadas con el empleo del ciberespacio, una segunda sección que abarca el marco normativo de las fuerzas armadas, y finaliza con el desarrollo de conclusiones parciales.

Tiene por objeto determinar el marco legal actual de las actividades de ciberinteligencia y ciberdefensa en el ámbito nacional y militar, para definir las limitaciones y posibilidades que tienen las fuerzas armadas de actuar en el ámbito del ciberespacio, y particularmente, para ejecutar actividades de ciberinteligencia en el ámbito conjunto y específico.

Sección I

Legislación Nacional relacionada al uso de la información personal

En la Argentina, la legislación que regula las actividades en el ciberespacio se encuentra en pleno desarrollo desde comienzos del S. XXI. Básicamente, nos referimos a aquellas herramientas normativas que delimitan las actividades permitidas en el ámbito de la ciberdefensa y dentro de ella a la ciberinteligencia, que nos dará las pautas para considerar la atribución de responsabilidades al Sistema de Defensa Nacional.

El Decreto N° 141/03 incorporó a la Jefatura de Gabinete de Ministros, las competencias relativas a la formulación, ejecución y control de las políticas y medios de comunicación social, y la difusión de la actividad del Poder Ejecutivo Nacional.

El Decreto Nº 624/03 establece que la Subsecretaría de Gestión Pública (SGP) de la Jefatura de Gabinete de Ministros, es el organismo responsable del diseño, implementación y seguimiento de la política de modernización del Estado y de la definición de estrategias sobre tecnologías de la información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información en la Administración Pública Nacional. (Decreto Nro 624, 2003)

La Oficina Nacional de Tecnologías de la información debe desarrollar entre otras acciones:

- Entender, asistir y supervisar en los aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica del Sector Público Nacional.

- Participar en todos los proyectos de desarrollo, innovación, implementación, compatibilización e integración de las tecnologías de la información en el ámbito del sector público, cualquiera fuese su fuente de financiamiento.

La Ley 26.388/08, establece medidas contra el cibercrimen y regula aspectos relacionados con la ciberseguridad en las actividades delictivas relacionadas con el uso de tecnologías de la información y la comunicación.

Abarca sanciones ante delitos informáticos que incluye la obtención ilegal de datos, la interferencia en sistemas informáticos, el acceso no autorizado a sistemas y redes, y la difusión de virus informáticos, entre otros.

Un aspecto para destacar de esta ley es el mecanismo de cooperación internacional en la lucha contra el cibercrimen. Argentina se compromete a colaborar con otros países en la investigación y persecución de delitos informáticos que trascienden las fronteras nacionales.

Contiene disposiciones relacionadas con la protección de datos personales y la privacidad en línea y, por otra parte, promueve la protección de infraestructuras críticas, como sistemas financieros y de comunicación.

Esta ley es fundamental porque proporciona un marco legal para abordar los delitos informáticos y proteger la seguridad en línea en el país. (Ley Nro 26.388, 2008)

La Ley de Protección de Datos Personales 25.326/00, regula el tratamiento de datos personales y establece los derechos de las personas en relación con los mismos. Esta ley es fundamental para proteger la privacidad y la seguridad de los datos personales en Argentina, de la misma podemos destacar los siguientes aspectos:

Define el término “Datos personales” e incluye en el mismo a los nombres, números de identificación, datos de contacto, datos biométricos, información médica y otros datos; abarca a todas las personas físicas o jurídicas del sector público o privado y establece la solicitud del

consentimiento para el tratamiento de datos personales de manera libre, específica e inequívoca.

Las organizaciones que recopilan y procesan datos personales deben registrarse en la Agencia de Acceso a la Información Pública (AAIP) para garantizar la transparencia y la supervisión de las prácticas de tratamiento de datos, y cumplimentan reglas para la transferencia de datos personales al exterior a los fines de su protección fuera del ámbito del país.

La Ley de Protección de Datos Personales 25.326/00 se encuentra articulada con las normativas internacionales de protección de datos, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. (Ley Nro 25.326, 2000)

Sección II

Legislación vigente en el ámbito de la defensa

La Directiva Política de Defensa Nacional (Decreto Nro 703, 2018) es el documento que establece los lineamientos centrales de la República Argentina y da inicio al planeamiento estratégico militar. Estas definiciones determinan la visión y los criterios que orientarán a la organización en lo referido al funcionamiento, la planificación, el desarrollo de capacidades operacionales, el empleo y la administración de los recursos humanos y materiales, conforme las apreciaciones estratégicas de los escenarios global y regional en materia de defensa y su impacto en la seguridad estratégica de la República Argentina.

La falta de identificación de amenazas convencionales directas no implica que la República Argentina carezca de riesgos y desafíos para la Defensa Nacional. A diferencia de las amenazas –en las que se aprecian indicios de una voluntad de daño -, los riesgos constituyen situaciones cuya probable evolución podría afectar los intereses nacionales en materia de defensa.

Los desafíos, por su parte, configuran fenómenos que, sin apreciarse como problemas específicamente militares, podrían suscitar la emergencia de conflictos interestatales, provocar situaciones de inestabilidad o la aparición de nuevos riesgos.

Riesgos:

- Competencia por los recursos estratégicos.
- Ataques externos a objetivos estratégicos.
- Utilización del ciberespacio con fines militares.
- Impacto de la criminalidad transnacional.

Desafíos:

- Utilización del espacio exterior con fines militares.
- Debilitamiento del multilateralismo.
- El Atlántico Sur y las Islas Malvinas, Georgias y Sandwich del Sur.

El artículo llamado “Consideraciones de un enfoque analítico de Defensa Nacional” (Eissa, 2018) expresa que las leyes Nº 23.554 de Defensa Nacional (1988), Nº 24.059 de Seguridad Interior (1992) y Nº 25.520 de Inteligencia Nacional (2001 y su modificatoria del 2014) se construye a partir de tres principios:

- La supresión de las hipótesis de conflicto con los países vecinos,
- La conducción civil de la política de Defensa,
- La separación orgánica y funcional de la Defensa Nacional y la Seguridad Interior.

La cuestión planteada de este debate busca establecer cuál debería ser la misión principal de las Fuerzas Armadas, mientras que una postura sostiene que la expresión "agresión externa" establecida en la Ley de Defensa Nacional, debería ser interpretada en un sentido amplio; otra postura restringe la definición a aquellas amenazas estatales militares externas, dejando fuera del ámbito de la Defensa Nacional a las nuevas amenazas como el narcotráfico y el terrorismo internacional y las ciberamenazas, entre otros.

El ROD-05-01 “Conocimientos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza”, detalla en forma muy general el concepto de empleo de la ciberdefensa en el ciberespacio mediante la ejecución de acciones pasivas para su protección. (ROD 05 - 01, 2017)

El “Manual de Seguridad Informática”, establece procedimientos, términos, definiciones, evaluaciones de riesgos y política de seguridad para la transición de datos.

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

Conclusiones parciales

La DPDN pone de relevancia la necesidad del aumento en la capacidad de transmisión de datos para el desarrollo de nuevas tecnologías e industrias, y que resulta crucial tomar en consideración al ciberespacio como una dimensión importante de la Defensa Nacional, esto origina el replanteo de las categorías de la guerra real y exige la adaptación de los sistemas de defensa.

El ciberespacio traspasa el límite entre lo interno y externo, entre la Seguridad Nacional y la Defensa Nacional. En este sentido, la República Argentina se niega a emplear medios militares en el ámbito interno salvo expresas situaciones de conmoción interna establecidas en la Ley de Seguridad interior que, junto con la Ley de Defensa Nacional y otras leyes y decretos complementarios, establecen una separación clara e inequívoca entre ambos ámbitos.

En virtud de lo expresado, cabe destacar que hoy las amenazas no se definen por el tipo o ámbito de acción, quienes afecten a un estado pueden ser terroristas, narcotraficantes, criminales, ciberterroristas, cibercriminales, organizaciones multinacionales, fuerzas

paramilitares, empresas privadas de seguridad, estafadores entre otras, dirigidas todas ellas o no, por actores estatales. Es por ello que el estado debe proporcionar herramientas legales que permitan ampliar el margen de acción de las fuerzas armadas para desarrollar capacidades acordes a los desafíos en el ciberespacio.

Capítulo II

Situación actual de países de referencia

Existen numerosos estudios, investigaciones y artículos que tratan acerca de la evolución acelerada de la ciberguerra y de la necesidad de desarrollos legales y orgánicos relacionados a la misma. Ya desde finales del S.XX, numerosos países disponen de unidades especializadas en ciberdefensa y ciberinteligencia para hacer frente a escenarios multidominio de intensa confrontación.

ARGENTINA

En la República Argentina, las Fuerzas Armadas no sólo disponen de las direcciones de ciberdefensa específicas (Ejército, Armada y Fuerza Aérea), sino también del Comando Conjunto de Ciberdefensa.

En el año 2014 se crea el Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto (EMCO), siendo su misión la de "Ejercer la Conducción de las Operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del instrumento militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo con los lineamientos establecidos en el Planeamiento Estratégico Militar" (Comando Conjunto de Ciberdefensa, s.f.)

Concretamente, el Comando Conjunto de Ciberdefensa, deberá brindar la protección cibernética a las redes informáticas de la defensa y, a orden, a las infraestructuras críticas que se le asignen.

En el año 2016, se creó la Subsecretaría de Ciberdefensa en el Ministerio de Defensa para, entre otras funciones, asistir al Ministro de Defensa en el planeamiento, diseño y elaboración de la política de ciberdefensa y ejercer el control funcional del Comando Conjunto de Ciberdefensa.

En el año 2022, se inaugura el Instituto de Ciberdefensa de las Fuerzas Armadas, ante la necesidad de coordinar y optimizar la capacitación conjunta en ciberdefensa dentro de las fuerzas armadas. El instituto dicta los siguientes cursos: Curso Básico Conjunto para personal militar superior, Curso Básico Conjunto para personal militar subalterno, Curso Avanzado de Ciberdefensa para oficiales y Curso Avanzado de Ciberdefensa para suboficiales. (Instituto de Ciberdefensa, s.f.)

Actualmente, el marco doctrinario para el desarrollo de las actividades en el ciberespacio se encuentra en desarrollo, es decir, la Argentina no dispone de doctrina propia para ejecutar actividades en el ciberespacio.

En lo que respecta al desarrollo orgánico de la ciberinteligencia, la Dirección General de Inteligencia se encuentra en un proceso de reconversión de acuerdo al Plan Estratégico del SIE 2022/2026. La Dir Grl Icia cuenta en su organización orgánica, de una División de Ciberinteligencia que, junto con la Compañía de Inteligencia de Señales, comprenden el núcleo para el futuro desarrollo del Subsistema de Ciberinteligencia.

ESTADOS UNIDOS

El Comando de Ciberdefensa de Estados Unidos es un comando militar de combate cibernético, fue conformado en el año 2009 y desde su creación, cumple un papel cada vez más relevante en la estrategia de defensa nacional del país. USCYBERCOM es responsable de dirigir las operaciones y la defensa en el ciberespacio, protegiendo las redes de computadoras del gobierno nacional y llevando a cabo operaciones cibernéticas ofensivas y defensivas según sea necesario para proteger los intereses nacionales de Estados Unidos. Se encuentra

conformado por Cyber Protection Teams (CPTs). (Comando Cibernético de los Estados Unidos, s.f.)

Trabaja en estrecha colaboración con otras agencias gubernamentales, como la Agencia de Seguridad Nacional (NSA), el Departamento de Seguridad Nacional (DHS) y la Agencia Federal de Investigaciones (FBI), para coordinar esfuerzos en ciberseguridad y defensa cibernética.

Dentro de las Fuerzas Armadas de Estados Unidos, existen varias unidades especializadas de inteligencia cibernética dedicadas a la producción de ciberinteligencia y la ejecución de operaciones cibernéticas. A continuación, se mencionan algunas de estas unidades:

- 780th Military Intelligence Brigade (Cyber): Esta brigada está especializada en inteligencia cibernética y es parte integral del Ejército de los Estados Unidos. Está compuesta por unidades capacitadas en análisis de inteligencia cibernética, evaluación de amenazas y protección de redes militares contra ataques cibernéticos.
- Army Cyber Institute (ACI): es un instituto de investigación y educación del Ejército de los Estados Unidos centrada en temas de ciberseguridad y guerra cibernética. Aunque no es una unidad operativa, el ACI contribuye a la producción de ciberinteligencia a través de investigaciones y análisis en profundidad sobre amenazas cibernéticas emergentes y tendencias en el ciberespacio.
- 915th Cyber Warfare Battalion: Este batallón se especializa en la realización de operaciones cibernéticas ofensivas y defensivas para apoyar las misiones del Ejército de los Estados Unidos. Está conformada por personal capacitado en técnicas de guerra cibernética y contribuye a la producción de inteligencia cibernética mediante la identificación y neutralización de amenazas cibernéticas.

Escuadrones de Operaciones Cibernéticas de la Fuerza Aérea (Cyber Operations Squadrons, COS)

- Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA): La Fuerza Aérea de los Estados Unidos cuenta con la 25th Air Force, que es responsable de la inteligencia, la vigilancia y la inteligencia de reconocimiento (ISR) en el ciberespacio. Dentro de la 25th Air Force, hay unidades especializadas en inteligencia cibernética, como el 688th Cyber Operations Group, que lleva a cabo operaciones de inteligencia cibernética y proporciona apoyo a las operaciones cibernéticas de la Fuerza Aérea.

Unidades de Guerra Cibernética de la Marina (Navy Cyber Warfare Units):

- Naval Information Warfare Command (NAVWARCOM): Este comando de guerra de la información de la Marina de los Estados Unidos incluye la Naval Information Warfare Development Center (NIWDC), que se centra en el desarrollo y la operación de capacidades cibernéticas y de guerra de la información. Dentro de NIWDC, hay unidades especializadas en inteligencia cibernética que proporcionan apoyo analítico y operativo para apoyar las misiones navales y marítimas.

Batallón de Guerra Cibernética del Cuerpo de Marines (Marine Corps Cyber Warfare Battalion):

- Marine Corps Forces Cyberspace Command (MARFORCYBER): Este comando incluye la Intelligence Branch, que está encargada de la recopilación, el análisis y la producción de inteligencia cibernética para apoyar las operaciones cibernéticas y la toma de decisiones dentro del Cuerpo de Marines.

CHILE

En los últimos años, la problemática de la ciberseguridad en Chile ha cobrado relevancia debido a los avances tecnológicos y al incremento de usuarios.

En la primera mitad del año 2022, Chile recibió más de 5000 millones de intentos de ataques, lo que implica un aumento del 138% en relación con el mismo período del año anterior de acuerdo con el reporte de amenazas de la empresa Fortinet. Estas amenazas presentan un notable aumento en la peligrosidad, sofisticación y tasa de éxito.

Actualmente, Chile trabaja en el desarrollo del marco normativo, su implementación y la creación de una conciencia de ciberseguridad.

En noviembre del 2015, el gobierno presentó la Agenda Digital 2020, que considera la necesidad de elaborar una estrategia de ciberseguridad. El Comité Interministerial integrado por las Subsecretarías de Interior, Relaciones Exteriores, Defensa, Hacienda, Secretaría General de la Presidencia, Economía, Justicia, Telecomunicaciones y la Agencia Nacional de Inteligencia elaboró el primer borrador de la política, que fue sometida al proceso de consulta pública que establece la ley N°20.500. (Politica Nacional de Ciberseguridad, 2017 / 2022)

Estado actual de la ciberseguridad en Chile

Algunas normas y reglamentaciones vigentes son la ley Nº 19.223 sobre delitos informáticos, la ley Nº 19.628 sobre protección de la vida privada, la ley de Telecomunicaciones Nº 18.168 que regula el marco jurídico de las telecomunicaciones y provee de una estructura física y lógica para el desarrollo del ciberespacio, el D.S. Nº1.299/2004 que regula la Red de Conectividad del Estado (RCE), la Ley 21.663/21 conocida como la "Ley de Ciberseguridad", que busca fortalecer la ciberseguridad en el país mediante la protección de los sistemas críticos de información, la creación de la Agencia Nacional de Ciberseguridad y la implementación de medidas para detectar, notificar y responder a incidentes cibernéticos.

La estructura para la respuesta a incidentes de seguridad informática en Chile, son los Computer Security Incident Response Team, (CSIRT). Estos centros requieren de recursos humanos y financieros, un marco institucional claro y mecanismos para operar de manera coordinada entre sí. De acuerdo con la política nacional de ciberseguridad 2017/2022, Chile contaría con un CSIRT nacional de recopilación y sistematización de la información proveniente de otros CSIRT (nacionales y extranjeros), para promover la coordinación de acciones entre CSIRT sectoriales y coordinar las respuestas necesarias para responder a las acciones que comprometan la seguridad del país, también se evalúa la pertinencia de crear un CSIRT de infraestructuras críticas.

Por otra parte, la Agencia Nacional de Inteligencia en cumplimiento de la Ley 19.974 "propone normas y procedimientos de protección de los sistemas de información crítica del Estado".

La Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública coordina, evalúa y controla planes intersectoriales en materia de delincuencia, entre ellas, los ciberdelitos. Dentro del ministerio mencionado, se encuentra la Brigada Investigadora del Cibercrimen quienes de forma preventiva investigan los casos de ciberdelitos.

En el Ministerio de Relaciones Exteriores se encuentra la Unidad de Ciberseguridad, quien coordina y articula con las agencias nacionales los objetivos y acciones de política exterior en materia de ciberseguridad, las acciones de cooperación y diálogo tanto con agencias nacionales como con contrapartes internacionales, esto incluye además ámbitos de acción como ciberdiplomacia, ciberdefensa y cibercrimen. Este ministerio también dispone de la Unidad de Ciberseguridad y Tecnologías Emergentes que coordina y articula con las agencias nacionales los objetivos y acciones de política exterior en materia de ciberseguridad y cibercrimen. (Unidad de ciberseguridad, s.f.)

El Ministerio de Defensa Nacional formula políticas para enfrentar los desafíos de ciberdefensa para proteger su propia infraestructura de información. Por su parte, el Estado Mayor Conjunto es el órgano de trabajo y asesoramiento del Ministerio de Defensa Nacional que elabora y mantiene actualizada la planificación de la defensa, junto con otras tareas relevantes como la ciberseguridad del país. (Objetivos de Desarrollo Sostenible de Chile , 2017)

La Dirección de Inteligencia de la Defensa (DID), bajo el Ministerio de Defensa Nacional, proporciona inteligencia estratégica a las Fuerzas Armadas y puede estar involucrada en la evaluación de amenazas cibernéticas y la identificación de vulnerabilidades en infraestructuras críticas a nivel nacional.

Actualmente, se encuentra vigente la política nacional de ciberseguridad 2023/2028, que al igual que la anterior, esta política multisectorial se elaboró de forma colaborativa entre el sector público, el sector privado, la academia y la sociedad civil, aprovechando la experiencia de los distintos sectores, tiene el propósito de prevenir riesgos en materia de ciberseguridad. (Política nacional de ciberseguridad de Chile, 2023 / 2028)

ISRAEL

Este país se encuentra actualmente en guerra contra organizaciones terroristas como Hamas y Hezbollah, quienes ejecutan en el marco de la guerra asimétrica acciones de ciberguerra contra Israel, quien recibe más de 200 ofensivas diarias provenientes de servidores iraníes. Son aproximadamente 15 grupos de la Guardia Revolucionaria Islámica que intentan constantemente, desestabilizar la red nacional israelí.

En este marco, Israel se encuentra desarrollando un escudo de ciberseguridad similar a la llamada Cúpula de Hierro que protege su espacio aéreo para poder blindarse de los ataques a la red.

Algunas de las leyes y regulaciones generales relacionadas con la seguridad cibernética y la protección contra ciberataques que podrían ser relevantes en el contexto de la ciberguerra son:

Ley de Seguridad Informática (Ley de Computadoras) (Legislación informática de Israel, s.f.)**:**

- Esta ley, formalmente conocida como la Ley de Prohibición de Delitos Informáticos y de Protección de la Información Computarizada de 1995, regula los delitos informáticos (como el acceso no autorizado a sistemas informáticos, el fraude informático y la interrupción de servicios informáticos) relevantes en el contexto de la ciberguerra y establece regulaciones para proteger la información digital en Israel.

Ley de Defensa Militar:

- Aunque no se centra exclusivamente en la ciberguerra, la Ley de Defensa Militar regula los asuntos relacionados con la defensa y la seguridad nacional en Israel, lo que incluye la capacidad de las Fuerzas de Defensa de Israel (FDI) para defenderse contra amenazas cibernéticas.

Ley Nro 577 Protección de la Privacidad de 1981 (Privacy Protection (Data Security) Regulations 5.777, 2017)**:**

- Esta ley establece disposiciones para la protección de la privacidad en Israel y regula la recopilación, procesamiento y uso de datos personales.
- Aunque no se centra exclusivamente en el ciberespacio, la Ley de Protección de la Privacidad puede ser aplicable a la protección de datos en entornos digitales.

Algunos de los elementos más específicos de ciberdefensa y ciberinteligencia militar en Israel, pertenecientes a las Fuerzas de Defensa de Israel son:

La dirección de Inteligencia Militar de Israel, que se compone de 3 unidades principales: la Unidad 8200, la Unidad 9900 y la Unidad 504.

- Unidad 8200 (Unidad de Inteligencia de las FDI) es una de las más conocidas, sus áreas de especialización incluyen la interceptación de comunicaciones electrónicas, el análisis de datos y la realización de operaciones cibernéticas ofensivas y defensivas. Esta unidad ha sido fundamental en el desarrollo de tecnologías avanzadas de ciberseguridad y ha llevado a cabo operaciones cibernéticas de alto perfil. (Unidad 8200 , 2015)
- Centro Nacional de Seguridad Cibernética (NCSC) es el principal organismo gubernamental encargado de coordinar la respuesta a amenazas cibernéticas en Israel con otras agencias gubernamentales, el sector privado y organizaciones internacionales para compartir información y coordinar respuestas a incidentes cibernéticos. Supervisa la infraestructura crítica del país y trabaja para protegerla contra ciberataques que podrían tener un impacto significativo en la seguridad nacional. (Israel crea una Ciber Dirección General Nacional, 2011)
- Oficina de la Cibernética (CDD): es responsable de la formulación de políticas y estrategias de ciberdefensa a nivel nacional en Israel. Trabaja en estrecha colaboración con la Unidad 8200 y otras unidades de inteligencia para evaluar las amenazas cibernéticas y desarrollar contramedidas efectivas.
- Unidad de Ciberdefensa de la Fuerza Aérea de Israel (IACDC): La IACDC se especializa en proteger las redes y sistemas de información de la Fuerza Aérea de Israel contra amenazas cibernéticas. Proporciona apoyo cibernético durante las operaciones militares, incluyendo la identificación y neutralización de amenazas cibernéticas en tiempo real.

Conclusiones Parciales

Dado que los países de primer orden referenciados en el presente trabajo como Estados Unidos e Israel se encuentran en constante tensión y bajo amenaza en un entorno de conflicto

permanente en todos los dominios, inclusive el ciberespacio, y debido a los posibles ataques de actores estatales, grupos terroristas o hackers individuales con motivaciones diversas, es que reconocen la importancia de la cooperación internacional en la lucha contra la ciberdelincuencia y la defensa cibernética. El intercambio de información y las alianzas estratégicas son fundamentales para fortalecer la seguridad cibernética a nivel nacional y global.

En virtud de lo expuesto, podemos advertir un desarrollo avanzado de organizaciones y elementos para asesorar, asistir, desarrollar nuevas tecnologías cibernéticas, producir ciberinteligencia, etc, en los niveles estratégico nacional, estratégico militar, y también en el nivel estratégico operacional, y que no solo pueden ejecutar operaciones defensivas, sino también operaciones ofensivas.

Por otra parte, países no tan desarrollados como Argentina y Chile también reconocen la importancia de proteger las redes informáticas nacionales, la infraestructura crítica de cada país, y proteger la privacidad de la información de cada uno de sus habitantes, pero se encuentran en pleno proceso de desarrollo del marco legal y administran la seguridad digital nacional de forma centralizada en los niveles estratégicos nacionales y militares, es decir, aún no desarrollaron elementos de ciberinteligencia y ciberdefensa que operen en los menores niveles, como el estratégico operacional. Asimismo, estos países sólo ejecutan acciones defensivas debido que el desarrollo de ciberarmas ofensivas comprende mayores costos y tiempo producto de los trabajos de investigación.

Capítulo III

La complejidad del entorno, el estado mayor de nivel componente terrestre y del ciclo de producción de inteligencia doctrinarios

Este capítulo busca definir y describir las características generales del entorno cercano de las organizaciones actuales y las variables independientes que lo comprenden, para poner

en relevancia la importancia de una comprensión lo más cercana a la realidad por parte del comandante, especialmente para aquellas organizaciones como el Componente Terrestre que se organiza para el cumplimiento de la misión, es decir, posee orden de batalla, y debe bajar certezas a las organizaciones que le dependen, con estructuras y capacidades limitadas y predeterminadas definidas en un cuadro de organización.

Para ello definiremos al estado mayor del componente terrestre y al ciclo de producción de inteligencia que conduce el Oficial de Inteligencia vigente en la doctrina, quienes asesorarán y asistirán al decisor en la toma de decisiones.

Sección I

Necesidad de comprender el entorno para decidir

Este nivel llamado antiguamente como Táctico Superior se caracteriza por la necesidad de proyección en el tiempo (inmediato y mediato) para alertar acerca de contingencias futuras; la amplitud de los espacios y la dificultad para anticipar la amenaza principal del enemigo incrementará el grado de incertidumbre.

La base de la inteligencia disponible en el órgano de dirección será la producida desde la paz bajo el concepto de continuidad. Será necesario conformar un centro integrador de inteligencia cuya finalidad será la de mantener la vinculación de los medios por el canal técnico. Este enlace debe contemplar también a los elementos de inteligencia del Componente Naval y Aéreo, y analistas que permitan un gran flujo de información y facilite el procesamiento en tiempo real.

El entorno de la Organización (Visceglie, 2019)

En relación a la gestión del entorno, el CR Visceglie explica en un artículo acerca de las representaciones sociales en las organizaciones militares en entornos complejos de alta incertidumbre, que por medio de este tipo de representación y los procesos comunicativos es que los integrantes de un sistema socio técnico conocen la realidad de su entorno, dado que

ofrece explicaciones que son compartidas por toda la organización, es por ello que cobra particular importancia la comunicación, la interacción y la cohesión entre los integrantes.

El concepto de representación social es similar, dependiendo del autor, a los conceptos de modelos mentales o paradigmas. Los modelos mentales son una forma o intento de explicar cómo funciona el mundo real. Según Peter Senge los modelos mentales no sólo determinan el modo de interpretar el mundo, sino el modo de actuar. Estos modelos mentales no se aplican conscientemente y no tenemos noción de los efectos que tienen sobre nuestra conducta.

Los modelos mentales permiten comprender "la realidad" en forma directa, pero "la realidad" que uno capta, no es "la realidad verdadera", sino "la realidad procesada por ese modelo mental". Gran parte de esta construcción proviene de la cultura organizacional, que opera inconscientemente y define la visión que la organización tiene de sí misma y de su entorno.

A la dificultad de comprender la realidad mencionada en el párrafo anterior, se le agrega la naturaleza compleja de los conflictos actuales, de carácter multidimensional, donde entran en juego diferentes variables de carácter político, cultural, económico y social que afectan el proceso de toma de decisiones del comandante militar; por lo que una respuesta sesgada reforzará el problema y lo empeorará. En este marco de complejidad, interaccionan las variables independientes provenientes del entorno, sobre las cuales no se posee control y condicionan la operatividad y la eficiencia de las organizaciones, no es posible ignorarlas, sino conocerlas y actuar en consecuencia.

Entonces es el líder quien debe tomar decisiones de acuerdo con el entorno actual, el pasado y el entorno proyectado en base a una mirada común de su estado mayor que permita lograr una visión compartida del problema y de las posibles alternativas que le den solución.

En otro artículo titulado "Hacia la supervivencia al borde del caos" elaborado por el mismo autor plantea que, en organizaciones complejas que se caracterizan por la

descentralización y conformación multidisciplinaria, es necesario contar con profesionales calificados, sumamente preparados y adoctrinados. (Visceglie C. G., 2014)

Menciona también que las organizaciones del tipo mecanicista son más aptas en ambientes estables, en cambio, las organizaciones del tipo orgánicas son exitosas en entornos más inestables o caracterizados por una incertidumbre alta. En cuanto a la estructura de la organización, deberá ser flexible, orgánica y descentralizada.

El autor expresa que, en el marco de la doctrina de la batalla aeroterrestre, la responsabilidad de la conducción del Componente Ejército del Teatro de Operaciones o del nivel divisional, será la de estructurar la situación a los elementos que le dependen absorbiendo para sí la incertidumbre, aceptando el riesgo, transmitiendo certezas, para permitir que organizaciones que poseen cuadro de organización fijo puedan planificar, organizar, coordinar, controlar y dirigir los medios para el logro de los fines.

Sección II

Organización de un estado mayor del componente terrestre del teatro de operaciones

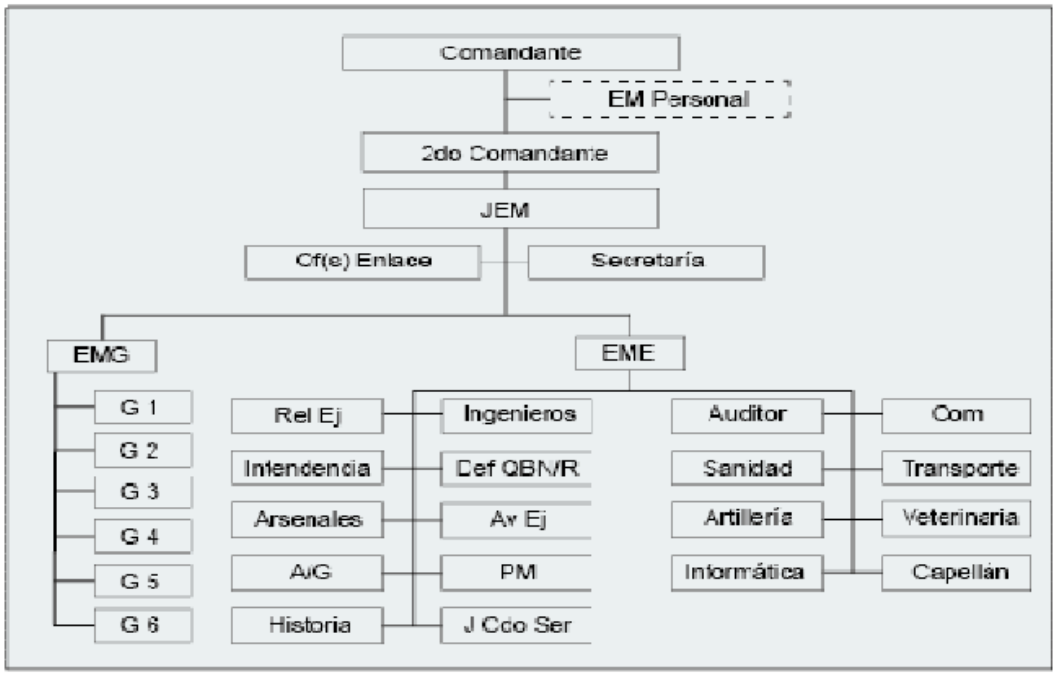
El reglamento de Organización y Funcionamiento de los Estados Mayores Tomo 1 hace mención a las diferentes características del ambiente operacional actual y cómo afectan el tipo y magnitudes de las fuerzas a emplear. Este ambiente operacional ejercerá una influencia directa sobre la estructura de la organización, la cual deberá ser lo suficientemente flexible para que, con mínimos cambios, pueda adaptarse rápidamente. Con esta finalidad, se deberá reducir la superposición de responsabilidades y adoptar organizaciones de las fuerzas y de los estados mayores que permitan ejercer un adecuado control sobre organizaciones que operen de forma descentralizada asignando responsabilidades definidas y delegando la autoridad para el cumplimiento de la misión.

La doctrina mencionada caracteriza a un estado mayor de nivel componente terrestre de un teatro de operaciones de la siguiente manera:

- Estado mayor de elementos significativos de la Fuerza Ejército a disposición de un Comando Conjunto del Teatro de Operaciones
- “En el caso de que una GUB/GUC comprenda la única fuerza integrante del componente ejército de un teatro de operaciones, el comando de esa GUB/GUC podrá asumir las funciones y responsabilidades inherentes al comando de componente.” (EA, 2023)

Figura Nro 1

Organización básica de un estado mayor del componente terrestre



Nota: esta imagen define el estado mayor del componente terrestre vigente en el reglamento de Organización y funcionamiento de los estados mayores

Esta es la organización reglamentaria que debería asesorar y asistir al comandante para apoyarlo en la toma de decisiones mediante el desarrollo de las actividades básicas de la conducción (Planeamiento, Organización, Coordinación, Control y Dirección). Como se puede observar en la figura, esta organización de cuadros y líneas se presenta de forma esquemática.

Asesorar y asistir implica proporcionarle bases sólidas al comandante para resolverse facilitando las herramientas e información necesaria de la propia fuerza, del enemigo y del

entorno para contribuir a darle solución al problema militar con la mínima incertidumbre y asumiendo riesgos de forma controlada.

La información proveniente de los diferentes dominios debe converger en el comandante de una forma clara, sencilla, breve y gráfica para lograr una rápida comprensión con un "golpe de vista táctico". Es decir, las organizaciones de producción de inteligencia deben reunir la información de todos los dominios para interpretar el entorno lo más cercano posible a la realidad.

A los fines de este trabajo, dentro del estado mayor de un componente terrestre no existe una organización, célula o personas especializadas conformadas previamente o Ad Hoc para brindar la información que facilite la interpretación de la realidad en el Ciberespacio por parte del comandante.

Sección III

Inteligencia Militar

"La Inteligencia será el conocimiento resultante del proceso a que se someterá la información sobre el enemigo real o potencial y el ambiente geográfico de interés para las operaciones militares, para el empleo del instrumento militar terrestre." (EA, Inteligencia Táctica, 2008)

La Inteligencia se encuentra abonada por información de distinta procedencia las que, debidamente procesadas, darán como resultante una nueva idea denominada Inteligencia. Este producto o nueva idea proporcionará conocimiento necesario para apoyar las resoluciones del comandante durante el planeamiento y conducción de las fuerzas.

Distintos son los factores que afectarán la actividad de inteligencia y pueden ser determinantes para la propia fuerza, es por ello, que deberán ser analizados para orientar la actividad de inteligencia y la elaboración de los modos de acción.

Entre estos factores, se encontrará la misión, que mediante su análisis desde el punto de vista de inteligencia orientará la dirección del esfuerzo de obtención.

Las características del enemigo, por cuanto será la voluntad inteligente que se opone y tendrá la capacidad en mayor o menor grado, de estar en capacidad de afectar el cumplimiento de la propia misión.

Las características del ambiente geográfico de interés que podrá afectar las operaciones desarrolladas por la propia fuerza y las operaciones del enemigo.

Las características de las propias tropas, quienes dotarán a la inteligencia, de personal y medios suficientes para las actividades propias.

En términos generales, los aspectos mencionados precedentemente, afectarán la ejecución de las actividades de inteligencia que tendrán como finalidad última, evitar la sorpresa, reducir la incertidumbre, asesorar y asistir al comandante.

El Ciclo de Producción de Inteligencia

Como se mencionó anteriormente, la inteligencia es el conocimiento resultante de un proceso, este proceso desarrollado como una secuencia lógica de pasos se denomina Ciclo de Producción de Inteligencia. Este ciclo tiene ciertas características que deberán cumplirse como condiciones *sine qua non:*

- Estará siempre orientado al cumplimiento de la misión impuesta.
- Será continuo y permanente, es decir, se trabajará desde la paz para ser actualizado en la guerra,
- Cada paso del ciclo deberá estar articulado con los requerimientos operacionales y en el momento adecuado para ser material de consumo que permita apoyar la resolución del comandante.

El Ciclo de Producción de Inteligencia estará conformado por cuatro pasos:

Dirección del Esfuerzo de Obtención, este paso consistirá en el análisis de la misión desde el punto de vista de inteligencia, para determinar la Zona de Interés y dilucidar las actividades de inteligencia impuestas y deducidas, y tiempos de interés; la determinación de los vacíos de información existente y formulación de requerimientos denominados Elementos Esenciales de Inteligencia (EEI) y Otros Requerimientos de Inteligencia (ORI) que serán propuestos al Comandante por parte del Oficial de Inteligencia.

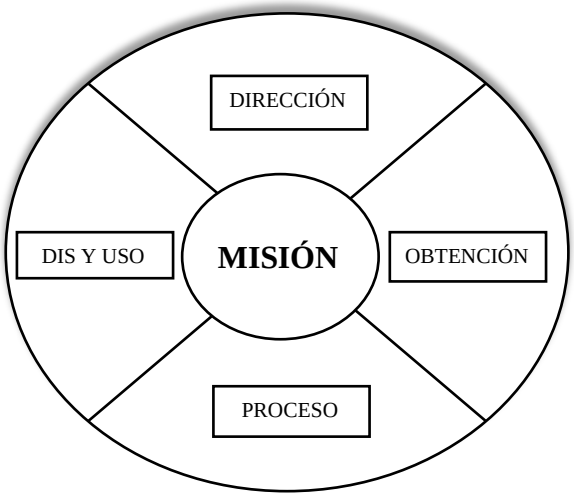
La Obtención de Información, que consistirá en la búsqueda y obtención propiamente dicha, incluye la transmisión de la información al órgano de dirección correspondiente.

El proceso de la información obtenida, consistente en el registro de la información, valorización de la información para determinar su pertinencia, confiabilidad y exactitud, análisis o descomposición de partes para ser procesada, la integración de la información y la interpretación resultante.

La diseminación y uso de la inteligencia resultante mediante la transmisión oportuna a quienes tengan la necesidad de saber.

Figura Nro 2

Ciclo de Producción de Inteligencia



Nota: la imagen representa el ciclo tradicional para la producción de inteligencia de acuerdo con el reglamento de Inteligencia Táctica (EA, Inteligencia Táctica, 2008)

Conclusiones Parciales

Este capítulo destaca cómo el conocimiento del entorno es fundamental para adoptar decisiones que permitan dirigir a la organización hacia la consecución de los objetivos, y que este entorno no es absoluto, inequívoco, sino que es producto resultante de la interpretación que cada integrante del estado mayor y que el decisor realice en base a su experiencia, conocimiento, convicciones, personalidad, tiempo, etc. Para que las interpretaciones de cada participante de la cadena de toma de decisiones no alejen al comandante de una interpretación objetiva y más cercana a la realidad, es necesario disponer de la mayor cantidad y calidad de información proveniente de diferentes ámbitos y dominios, para arribar a la definición de las posibles soluciones al problema militar planteado de la forma más acertada posible, considerando todas las variables.

Las operaciones en el ciberespacio cobran mayor preponderancia con el avance de los desarrollos tecnológicos, siendo cada vez más decisivo en el conflicto, y a pesar de ser transversales a todos los dominios, la organización doctrinaria del estado mayor de un componente terrestre no contempla asesores del dominio ciberespacial, es decir que, actualmente el comandante decidiría sobre bases de conocimiento sesgadas, parcializadas, esto incrementa los riesgos y la incertidumbre induciéndolo al error.

Capítulo IV

El ciberespacio

Sección I

Conceptos Generales

En el área de la ciberinteligencia se desarrollan actividades que son totalmente concurrentes y estrechamente coordinadas con la ciberdefensa, con el objetivo de identificar,

definir, clasificar y cuantificar información del ciberespacio (capacidades e intenciones del enemigo/ciberamenazas, oportunidades, limitaciones y opciones en el ciberespacio).

Se identifican los siguientes tipos de ciberactores:

- Grupos delictivos.
- Grupos terroristas.
- Grupos subversivos.
- Estados hostiles.
- Hackers aislados.
- Competencia (ciberespionaje).

El ciclo de Producción de ciberinteligencia se nutre de la información obtenida por los sistemas de ciberdefensa, del análisis de fuentes abiertas, del conocimiento de nuevas ciberamenazas y tendencias de ciberataques para la obtención de ciberinteligencia de forma permanente que será fundamental en el éxito de las operaciones de ciberdefensa.

Sección II

Descripción del Ciberespacio (CESEDEN, 2012)

Actualmente, los organismos internacionales y los estados han tomado real conciencia de los riesgos existentes en el ciberespacio, como la afectación la infraestructura crítica privada y pública de un estado, o la posibilidad de moldear la percepción de la información por parte de la población para canalizarla hacia fines específicos.

En el ciberespacio se encuentra contenido un gran volumen de información veraz y falsa, se encuentra en forma de videos, fotos, documentos de investigación, blogs, drivers, etc, ancladas en millones de páginas webs, mensajes de correo electrónico, chats y repositorios almacenados en una estructura física conformada por servidores y computadoras de todo tipo presentes en todo el planeta.

Figura Nro 3

Foto del ciberespacio

Nota: un instante cualquiera en el ciberespacio, disponible en www.map.ipviking.com

Características diferenciadoras del ciberespacio

El ciberespacio presenta singularidades que le son propias: inicialmente, podemos decir que el ciberespacio es un dominio casi infinito. Los dominios aéreo, terrestre y naval están delimitados físicamente, sin embargo, el dominio ciberespacial no posee límites.

Generalmente, pero cada vez menos, los medios de combate en los escenarios que se configuran en los dominios aéreo, terrestre y naval, son dirigidos por el estado. Por otra parte, los medios del ciberespacio se encuentran a disposición de toda la población mundial, solo se debe poseer los conocimientos necesarios y acceso a la red.

En el ciberespacio, el poder se encuentra en el dominio de la información, la que se protege defensivamente, y se altera o sustrae ofensivamente al enemigo, siendo la cantidad de información menos importante que la calidad. En este sentido, la información no tiene peso, volumen, no tiene materia, es decir, no le caben las leyes de la física, es inmaterial.

Así como los conflictos tradicionales se desarrollan en el campo de batalla, el combate en el ciberespacio extiende las acciones hasta el mismo corazón de la nación, al poder afectar

la infraestructura crítica de un estado y consecuentemente, afectar la vida de cada uno de sus ciudadanos.

El ciberespacio no necesita sistemas de armas con poder cinético como los dominios tradicionales. Existen armas ofensivas y defensivas, pero son de características totalmente diferentes, compuestas por mecanismos de análisis y control de tráfico de red, hardware y software de seguridad, y personal con alta formación profesional. Las armas ofensivas se diseñan en base a la investigación, generación de códigos y aplicación de técnicas y tácticas adecuadas que confieran un daño al oponente, desarrolladas hoy, por los países de primer orden

Sección III

Ciberamenazas

Para continuar con el presente trabajo, es necesario clarificar los tipos de ciberamenazas, debido que no existe una única clasificación aceptada por la comunidad internacional. Podemos definir a los tipos de ciberamenazas como ciberespionaje, amenazas híbridas, cibercrimen y hacktivismo, y para cada una de ellas se ejecutan diferentes acciones en el ciberespacio que comprenden delitos específicos mediante técnicas, herramientas y vectores de ataque de acuerdo con el siguiente cuadro:

Figura Nro 4

Ciberamenazas

CIBERAMENAZAS	ACCIONES EN EL CIBERESPACIO	DELITOS EN EL CIBERESPACIO	TECNICAS –VECTORES DE ATAQUE
Ciberespionaje	Amenazas Avanzadas Persistentes	Robo de Información	Hackeo Adware
		Acceso no autorizado a sistemas de información	Malware
		Violación a la propiedad intelectual	
		Clonación de tecnología	Phishing
Amenazas Híbridas	Acciones Militares	Secuestro digital	Ransomware
	Ciberataques	Acceso no autorizado a sistemas de información	Phishing
	Manipulación de Información	Desinformación	Fake news – deep fakes
	Sabotaje	Extorsión	Malware
Cibercrimen	Ciberterrorismo	Financiación al terrorismo	Criptomonedas
		Ataques cibernéticos	Ransomware
			DDOS – DOS
		Ataques Infraestructura Crítica	Malware – troyanos
			Botnes
	Ciberdelitos	Extorsión	Ransomware
		Secuestro digital	
		Lavado de activos	Cryptojacking
			Botnes
		Falsificación de medios de pago electrónicos	Phishing – Malware – clonación
		Pornografía infantil	Ciberbulling
		Piratería informática	Cracking
		Prestación de servicios ilícitos	Deep Web – Dark Web
Hacktivismo	Ciberataques	Denegación de servicios	DDOS – DOS
	Manipulación de Información	Desinformación	Fake news – Deep fakes
	Difusión de datos personales	Violación de datos	Doxing
	Acosos cibernéticos	Robo de identidad - Suplantación	Cyberbulling

Nota: tipos, acciones, delitos y técnicas de las ciberamenazas, http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992019000200024

A continuación, se describirán los tipos de ciberamenazas y alguna acción, delito, técnica/herramienta/vector de ataque de interés particular.

El ciberespionaje es una actividad que puede ser realizada por individuos, grupos, organizaciones o gobiernos, que utilizan técnicas de ciberseguridad y tecnología informática para acceder de manera no autorizada a sistemas informáticos y redes con el propósito de recopilar información confidencial o secreta del tipo militar, gubernamental, empresarial, industrial o datos personales.

Los ciberespías suelen utilizar malwares, virus, troyanos o técnicas de Phishing para infiltrarse en sistemas informáticos o redes de sus objetivos y recopilar datos sensibles como documentos, correos electrónicos, contraseñas, información financiera o de investigación. También ejecutan vigilancia y monitoreo de las actividades de la víctima para obtener información en tiempo real o para mantener un acceso continuo a sus sistemas.

Posteriormente, los ciberespías transfieren los datos robados a ubicaciones remotas, generalmente en servidores controlados, para su análisis y uso posterior.

Las amenazas híbridas en el ciberespacio hacen referencia a la combinación de tácticas y técnicas que los actores estatales y no estatales utilizan para alcanzar sus objetivos, estas amenazas son complejas y multifacéticas, algunos ejemplos en el ciberespacio son:

Ataques cibernéticos como los sabotajes a la infraestructura crítica (sistemas de energía, agua o transporte, etc), y al mismo tiempo realizar acciones físicas, como ataques terroristas o ataques armados, para crear un caos generalizado.

La difusión de información falsa son operaciones de desinformación cibernética que implican la creación y promoción de noticias falsas, historias ficticias, rumores infundados o información engañosa en línea. Esta información se divulga a través de redes sociales, medios

de comunicación social, propaganda en papel, uso de deepfakes (vídeos o imágenes generadas por inteligencia artificial), y pueden parecer auténticas y creíbles a primera vista, lo que dificulta su detección,

El cibercrimen es una actividad delictiva cometida por cibercriminales o hackers dirigidas a una computadora, una red informática o un dispositivo en red. El objetivo del cibercrimen es ganar dinero o afectar computadoras o redes por motivos personales o políticos. El phishing, cryptojacking, ransomware y las violaciones de la seguridad de los datos son algunas formas de cibercrimen.

El hacktivismo comprende la ejecución de acciones maliciosas en internet, para promover ideas políticas, religiosas o sociales con el fin de propagar y defender ideas o valores concretos. Puede promover fácilmente por medio de la propaganda en internet ideas radicales y extremistas y llevar a cabo ciberataques que puedan facilitar una posible ciberguerra.

Entre los métodos de ataque más frecuentes, destacan los malwares, los ransomwares, los ataques zero-day, etc.

Sección IV

Ciclo de Producción de Ciberinteligencia

En la actualidad, las fuerzas armadas argentinas no desarrollaron una doctrina que sea de guía para desarrollar actividades en el ciberespacio, como las actividades de ciberinteligencia. Es por esta razón, que producto de la exploración de diferentes fuentes de información, se tratará de describir un ciclo de producción de ciberinteligencia y las herramientas que se utilizan que permitan establecer de forma general, las actividades que debería ejecutar un analista para producir ciberinteligencia con la finalidad de determinar lo que ocurre en esta parte del ambiente operacional, a los fines de reducir la incertidumbre, reducir riesgos, establecer las capacidades e intenciones del enemigo, y asesorar y asistir al

comandante en el proceso de toma de decisiones teniendo en cuenta la actividad existente en el ciberespacio.

La ciberinteligencia es el producto resultante de un proceso similar al Ciclo de Producción de Inteligencia utilizado en el dominio terrestre descripto en párrafos precedentes.

Uno de los métodos más utilizados es el Proceso de Inteligencia de Fuentes Abiertas (OSINT por sus siglas en inglés), que utiliza información no clasificada y la procesa para producir inteligencia, la clave se encuentra en procesar la información disponible y valorizarla en un tiempo cada vez menor.

Proceso de Inteligencia de Fuentes Abiertas (Open Source Intelligence) (Clark, 2022)

Robert M. Clark, oficial retirado de la Fuerza Aérea de Estados Unidos especialista en Guerra electrónica e Inteligencia, escribió el libro “Intelligence Collection” donde presenta de forma sistemática y analítica el "cómo y por qué" de la recopilación de inteligencia en sus tres etapas principales: la fase inicial (planificación), la recopilación y la fase final (procesamiento, explotación y difusión). El libro proporciona una visión clara de los complejos sistemas de recolección utilizados en todo el mundo, entre ellos, del ciclo OSINT.

El autor destaca que actualmente la inteligencia de código abierto abarca mucho más que las fuentes públicas tradicionales, y el término inteligencia de código abierto (OSINT) se ha convertido en una herramienta de uso generalizado.

Incluye medios como periódicos, revistas, radio, televisión e información basada en computadoras, material profesional y académico de conferencias, simposios, asociaciones profesionales y artículos académicos, informes gubernamentales con datos oficiales y contenido web generado por los usuarios en redes sociales, sitios para compartir vídeos, Twitter, wikis y blogs.

Aunque gran parte del negocio de inteligencia no es lineal, se explicará el ciclo OSINT secuencialmente para una mayor comprensión, siendo cada paso la resultante del anterior, aunque en la realidad así no lo sea. Los pasos principales son:

- Planificación e identificación de fuentes:

Debido a la gran cantidad de información de código abierto disponible, la recopilación debe ser planificada en base al conocimiento de interés de inteligencia. Históricamente, la mayor parte del material de código abierto se encontraba presentada en copia impresa. Hoy, las fuentes más utilizadas están en la nube, es por ello que la World Wide Web se ha convertido en la fuente dominante.

- Recolección:

Tiene dos pasos principales, localizar la información buscada y validarla. Uno de los mitos sobre el código abierto, es que se encuentra fácilmente disponible, pero un problema de la inteligencia de código abierto es el de la abundancia, un analista de todas las fuentes no puede aprovechar todo el material disponible, necesita recurrir a expertos en investigación.

La información abundante trae aparejado el problema de la confiabilidad para separar lo verdadero de lo falso, es necesario examinar el material y analizarlo con detalle para determinar la exactitud, credibilidad y autenticidad. El código abierto es una excelente forma de difundir información engañosa.

- Procesamiento (traducción):

En aquellos países con intereses globales, el autor destaca la importancia de disponer de traductores en numerosos idiomas con la problemática que ello trae aparejado. En este sentido, la opinión personal de los traductores puede interferir en la interpretación de la información, o producirse sesgos de fuentes, etc.

Las persistentes deficiencias en los lenguajes críticos, junto con los crecientes volúmenes de información disponibles a través de código abierto y otros medios, limitan la capacidad de recopilación y análisis de inteligencia.

- Análisis

En este paso se distinguen 3 tipos de analistas, el analista de código abierto, el de contenidos y el analista de todas las fuentes. El análisis de código abierto, y el análisis de contenido en particular, no realizan juicios sobre el contenido del material, ese papel lo ocupa el analista de todas las fuentes, que recurre a una amplia gama de fuentes.

El análisis de contenido, en cambio, es una herramienta de investigación de patrones, se utiliza para determinar la presencia de ciertas palabras, conceptos, temas, frases, personajes u oraciones dentro de textos o conjuntos de textos. El objetivo es cuantificar y analizar la presencia, significados y relaciones de las palabras y conceptos. A partir de esto, un analista de contenido puede luego hacer inferencias sobre los mensajes dentro del material, el autor y el público.

- Difusión

El material de código abierto no está clasificado, siendo el medio de difusión natural, el internet. Los gobiernos y las corporaciones pueden optar por controlar la difusión utilizando redes privadas virtuales. La OTAN, por ejemplo, tiene una red de este tipo, y la utiliza para la difusión de código abierto.

Herramientas OSINT para la obtención de información

Como fue mencionado anteriormente, uno de los inconvenientes de la inteligencia de fuentes abiertas es el enorme volumen de datos con el que trabajamos, por eso es imprescindible emplear herramientas para recopilar información y organizarla. A continuación, se presentan diferentes herramientas que facilitan la tarea:

Motores de búsqueda genéricos

Para encontrar resultados relevantes, es necesario aplicar técnicas de búsqueda avanzadas (lo que se conoce como hacking con buscadores) como Google, Bing o DuckDuckGo.

Buscadores especializados

También existen motores de búsqueda diseñados para ejecutar una labor muy específica.

Algunos de ellos son:

- Personas: permiten obtener información de una persona a partir de sus datos personales. Uno de los más famosos es PIPL.
- Emails: existen variadas opciones para encontrar la dirección de correo electrónico de una persona, tal es el caso de HUNTER.IO.
- Imágenes: a través de herramientas como TINYEYE o IMGOPS puedes realizar una búsqueda inversa de imágenes.

Incluso existen buscadores como HAVE I BEEN PWNED, que permiten localizar datos personales que hayan sido comprometidos en una fuga de información de una web.

Redes sociales

Mediante la aplicación del proceso SOCMINT (Social Media Intelligence), es posible obtener información relevante de redes como Facebook, Twitter, LinkedIn, TikTok o Tinder.

Extracción de metadatos

Mediante la aplicación de técnicas de IMINT (Imagery Intelligence) es posible realizar el análisis de los metadatos de una imagen (información que está “oculta” en el código informático del archivo) para obtener información acerca de:

- La fecha y la hora en que se realizó la foto.
- El modelo de la cámara o móvil.

- Quien es el dueño del dispositivo (si ha registrado esta información en el aparato previamente).
- Si la imagen ha sido recortada, editada o modificada de algún modo.

Protección de identidad

Esta herramienta permite proteger datos personales. Para ello las opciones son:

- Crear un avatar anónimo
- Ocultar IP: La red TOR o sistemas operativos especiales como TAILS permiten ocultar la IP, esto es fundamental al navegar por la DARK WEB.
- También existen herramientas para crear emails falsos, números de teléfonol, tarjetas de cuentas bancarias, etc.

Geolocalización

Existen ciertos casos en los que es necesario:

- Determinar la ubicación de una persona o de un sitio web.
- Averiguar dónde se ha tomado una imagen.
- Buscar evidencias en una localización geográfica muy concreta

Para esta finalidad, se pueden usar herramientas específicas como:

- Herramientas para geolocalizar IPs como Grabify o IPLogger.
- YouTube Geofind te permite buscar vídeos que se han grabado en una ubicación específica.
- Google Maps y Google Earth combinan imágenes satelitales con las tomadas en la calle para recabar información sobre un lugar.

Sección V

Organizaciones que gestionan el ciberespacio

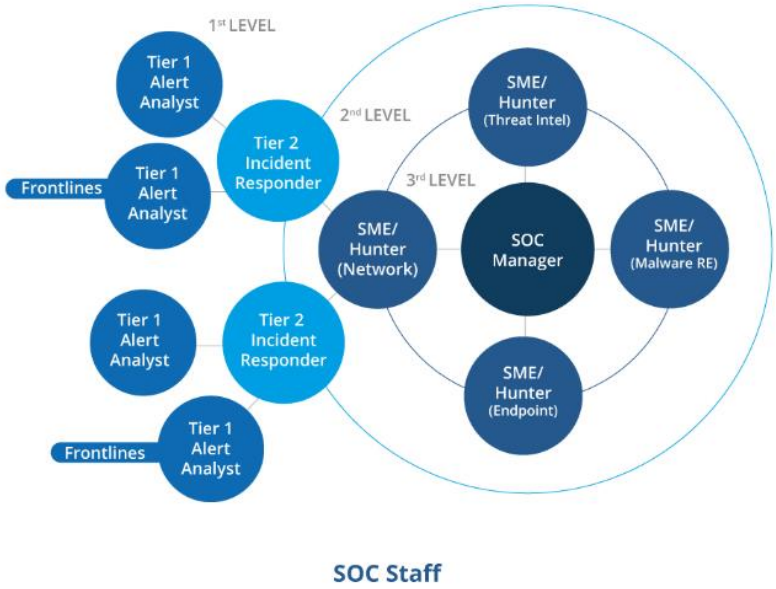
Actualmente, las empresas conforman sistemas de seguridad e inteligencia de amenazas organizados en tres niveles, y en cada nivel, se conforma un centro de operaciones integrado

por analistas con diferentes grados de especialización. Cada uno de los niveles con su centro correspondiente, trabaja en la red para cumplir funciones específicas de acuerdo con la complejidad de la tarea en relación con la capacitación del personal.

Organización del Sistema de Ciberseguridad y Ciberinteligencia

Figura Nro 5

Organización de un sistema de seguridad



Nota: la imagen detalla los niveles y las tareas de un SOC, fuente https://www.innovery.net/es/seguridad-de-la-red/#1619022374002-bfa4d82c-06e7

El nivel 1 corresponde a los analistas que ejecutan actividades de monitoreo y diagnóstico permanente de las alertas que se reciben en el sistema en tiempo real, para posteriormente evaluarlas de acuerdo con el riesgo que comprende para la infraestructura propia, y determinar la necesidad o no de que actúe el siguiente nivel.

La organización que ejecuta las tareas de este nivel se denomina NOC (Network Operation Center).

El monitoreo de un NOC en la actualidad tiene objetivos tales como detectar condiciones que puedan afectar al estado del sistema, la misma se concreta mediante la ejecución de las siguientes tareas:

Gestión de eventos, el NOC se enfoca en los cambios de estado que la organización define como un evento. Una vez monitoreado el evento, se determina la importancia y se identifica para iniciar una respuesta apropiada a los mismos. La información sobre estos eventos se registra y se proporciona a las partes relevantes implicadas en ello.

En la gestión de servicios, el tiempo de actividad, el rendimiento y la visibilidad juegan un papel clave. Incluye la administración de versiones, la gestión de incidentes, la gestión de la seguridad de la información o la gestión de la continuidad del servicio.

En el nivel 2 los analistas realizan una evaluación de daños del sistema y la información, en caso afirmativo, solicitarán una respuesta al incidente, pasando al siguiente nivel. (Microsoft, s.f.)

La organización que ejecuta las tareas de este nivel se denomina Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés, Security Operations Center), esta es una unidad centralizada dentro de una organización o gestionada por un proveedor de servicios externo formada por un equipo de expertos que se encarga de monitorear, detectar, analizar, responder y mitigar amenazas e incidentes de ciberseguridad. Algunas tareas relevantes afín al objeto de este trabajo son:

Monitoreo: Los equipos SOC monitorean de forma permanente la red, sistemas, aplicaciones y datos de una organización en busca de signos de actividad sospechosa o maliciosa. Algunas herramientas importantes son los sistemas de detección de intrusiones (IDS), los sistemas de prevención (IPS) y plataformas de gestión de información y eventos de seguridad (SIEM).

Detección de incidentes: cuando se detectan posibles incidentes de seguridad, los analistas del SOC investigan y evalúan la gravedad de la amenaza, utilizan registros, alertas y otras fuentes de datos para determinar la ocurrencia de un incidente.

Respuesta a incidentes: en caso de confirmarse un incidente de seguridad, los equipos del SOC siguen procedimientos predefinidos y desempeñan un rol importante para contener, mitigar y realizar la recuperación después de ocurrido el incidente. Esto puede implicar aislar sistemas afectados, corregir vulnerabilidades y comunicarse con las partes afectadas intervinientes.

Las acciones van desde el bloqueo de direcciones IP maliciosas, la actualización de firmas antivirus o incluso la colaboración con fuerzas de seguridad externas.

Dada la velocidad a la que pueden ocurrir los incidentes, muchos SOC incorporan la automatización para responder rápidamente con procedimientos predeterminados a amenazas conocidas y liberar a los analistas para tareas más complejas.

Inteligencia de amenazas: en algunos casos, los equipos del SOC se basan en fuentes de inteligencia de amenazas y en el intercambio de información para mantenerse informados sobre amenazas y vulnerabilidades emergentes. Esto contribuye a la defensa proactiva (Threat Hunting) contra posibles ataques futuros mediante la comprensión de las tácticas, técnicas y procedimientos de los actores maliciosos.

Forense y análisis: los analistas del SOC realizan exhaustivos análisis de los incidentes para comprender la raíz de la causa y su posible impacto. Esta información se utiliza para mejorar las medidas de seguridad y prevenir incidentes futuros.

Reportes y documentación: los equipos SOC mantienen registros detallados de los incidentes, incluyendo su cronología, las acciones tomadas y las lecciones aprendidas. Esta documentación es esencial para los trabajos de auditoría y también la retroalimentación para mejorar las acciones de seguridad y producción de inteligencia.

Colaboración: la ciberseguridad es un esfuerzo de equipo para asegurar la respuesta coordinada. Los SOC a menudo trabajan en estrecha colaboración con otros departamentos, como el de tecnología, el legal y la alta dirección. Esto permite junto con la retroalimentación

mencionada anteriormente, evolucionar junto con los avances de la tecnología y los cambios de las ciberamenazas.

Evaluación de Riesgos: Un SOC participa continuamente en la evaluación de los riesgos de la red, lo hace reconociendo las vulnerabilidades de la infraestructura propia y evaluando la probabilidad y la gravedad de posibles amenazas.

Equipo Multidisciplinario: Los equipos de un SOC se encuentran formados por profesionales con diferentes habilidades, como analistas de seguridad, expertos en redes, ingenieros de sistemas y especialistas en inteligencia de amenazas.

En el nivel 3, se encuentran los profesionales altamente cualificados en ciberseguridad, en capacidad de dar respuesta a los incidentes producidos y solucionarlos. También pueden desarrollar nuevas respuestas superadoras contra amenazas para dar solución ante la actividad de amenazas desconocidas.

La organización que ejecuta las tareas de este nivel se denomina Equipo de Respuesta ante Amenazas Informáticas (o por sus siglas en inglés CERT / Center Emergency Response Team), ejecuta tareas preventivas y reactivas ante amenazas de seguridad conocidas y realiza alertas relativas a amenazas y vulnerabilidades, todo ello, para aumentar la resiliencia de la organización. También se denomina Equipo de Respuesta ante Incidentes de Seguridad Informática (o por sus siglas en inglés CSIRT / Computer Security Incident Response Team)

Otras herramientas que se utilizan en el campo de la Ciberinteligencia

La ciberinteligencia es un campo que implica recopilar, analizar y utilizar información sobre amenazas y actividades cibernéticas para proteger sistemas, redes y datos. Para llevar a cabo estas tareas, existen varias herramientas y softwares especializados disponibles. Algunos ejemplos de software que se utilizan en el campo de la ciberinteligencia son:

MISP (Malware Information Sharing Platform & Threat Sharing) es una plataforma de código abierto diseñada para compartir y analizar información de amenazas. Permite a los analistas de seguridad cibernética colaborar en la recopilación y el análisis de datos.

AlienVault OSSIM (Open Source Security Information and Event Management) es una solución de gestión de seguridad de código abierto que integra capacidades de detección de amenazas, correlación de eventos y análisis de registro.

Wireshark es un analizador de protocolos de red que permite la captura y el análisis de paquetes de datos en una red. Puede ser útil para la detección y el análisis de tráfico malicioso.

Splunk es una herramienta de análisis de datos y registro que puede ser utilizada para la búsqueda y el análisis de eventos de seguridad y datos de registro en tiempo real.

Esto incluye la búsqueda de tendencias o patrones para tomar mejores decisiones sobre qué información es más importante y cómo debe presentarse a los usuarios finales.

ThreatConnect es una plataforma de ciberinteligencia que permite recopilar, analizar y compartir información sobre amenazas cibernéticas.

FireEye iSIGHT Intelligence proporciona servicios de inteligencia de amenazas cibernéticas que incluye informes detallados sobre amenazas, indicadores de compromiso (IOCs) y análisis de malware.

Cyber Threat Intelligence (CTI) Feeds ofrece datos sobre amenazas cibernéticas para su integración en plataformas y herramientas de seguridad.

Conclusiones Parciales

El ciberespacio es un dominio particular, se encuentra en desarrollo y es totalmente diferente a los dominios tradicionales. Posee características que le son propias, y estas actúan como variables que, en casi su totalidad, son independientes, es decir, difícilmente se tiene control de la actividad en el ciberespacio ya sean estas propias o no, o en la ejecución de una operación cibernética, difícilmente se podrán gobernar los resultados o el daño colateral.

Entre las características mencionadas en este capítulo, destacamos la necesidad de desarrollar o implementar herramientas que permitan procesar un gran volumen de información para producir inteligencia acerca de las capacidades del enemigo, intenciones, debilidades del enemigo, vulnerabilidades propias y los efectos del ciberespacio sobre las operaciones, pero surge aquí otra cuestión ¿Cómo determino quién es el enemigo? El factor del Orden del Batalla denominado Identificación del enemigo es de determinación casi imposible, es por ello que la ciberinteligencia procesa la información para producir inteligencia acerca de la actividad *per se* que pueda afectar los sistemas propios y desarrollar una adecuada inteligencia cibernética de alertas.

Surge aquí la necesidad de organizaciones inteligentes que se encuentren en constante aprendizaje para hacer frente a la evolución de las tecnologías de la información y comunicación, de los protocolos y algoritmos, las plataformas y aplicaciones y capacitación de los ciberatacantes. Para ello, actualmente las empresas emplean analistas de ciberinteligencia y ciberdefensa que monitorean las redes propias y el ciberespacio de forma permanente, apoyados en plataformas y software que ejecutan diferentes tareas de forma automática y se encuentran en constante desarrollo. Splunk por ejemplo, es un software que monitorea, recopila, registra datos de forma permanente para utilizar de pruebas de respaldo de ser necesario, pero además analiza y procesa esa información, detectando patrones que se repiten, indicios, crea indicadores claves de desempeño (KPI) personalizados, permite ver resultados de forma gráfica, clara y sencilla. Las actividades mencionadas son propias de un proceso de producción de ciberinteligencia.

Conclusiones finales

De los temas desarrollados en los cuatro capítulos, podemos concluir que existe una necesidad de categorizar el ámbito de empleo de las Fuerzas Armadas (salvo excepciones puntuales establecidas en el marco legal) y el tipo de amenaza a enfrentar del tipo externa,

estatal y militar, que no hace más que ir a contramano de la realidad de los conflictos armados actuales donde los dominios tradicionales como el aire, tierra y mar se encuentran traspasados por otros dominios como el ciberespacio, que si hay algo que este dominio no reconoce, es de límites.

Asimismo, es menester desarrollar el marco doctrinario y nuevas reglas, desde donde se desmembrarán estándares de comportamiento para la producción de ciberinteligencia.

Por otra parte, es indudable la necesidad de contar con una organización de analistas de ciberinteligencia cuyo conductor de fracción se encuentre en condiciones de interpretar las actividades importantes, recientes y actuales en tiempo real en el ciberespacio, de definir las capacidades del enemigo que puedan afectar el cumplimiento de la misión, como así también, las debilidades que comprendan una ventana de oportunidad para explotarlas, que asesore acerca de las características del ambiente ciberespacial que afecten las operaciones propias y del enemigo, identifique indicios, proporcione alerta, etc.

Todo ello proporcionará certezas necesarias que deben ser contempladas en el planeamiento, organización, coordinación, control y dirección de los medios hacia el logro de los fines.

Considero que la tecnología transforma o incide de alguna manera en todos los factores del ambiente operacional, y las operaciones que se desarrollan en el dominio del ciberespacio no requiere el desarrollo o la adquisición de recursos materiales de gran costo, en este sentido, requiere de material informático con las capacidades adecuadas y acceso a la red.

La fortaleza radica en la capacitación altamente especializada del personal que ejecute actividades de ciberinteligencia quienes deberán tener gran adaptabilidad para adecuarse al cambio, integrar grupos para realizar trabajos interdisciplinarios, con capacidad

de pensamiento crítico, capacitación continua y resiliencia a la presión, como así también, minuciosos en la elaboración de informes.

El sistema de ciberdefensa conformado en el nivel 1 por Centro de Operaciones de Redes (NOC), en el nivel 2 por el Centro de Operación de Sistemas (SOC) y en el nivel 3 por Equipo de Respuesta ante Amenazas Informáticas (CERT / SIRT) aplicado en las empresas actualmente, es perfectamente adaptable, por ejemplo, al funcionamiento de la Red Digital de Integración de Sistemas del Ejército (REDISE) o al Sistema Único de Comunicaciones (SUCOM). En este sistema se desarrollan actividades afines a la ciberinteligencia cuando se registra la información como respaldo legal, se valoran las fuentes, se realiza análisis, detección de patrones de comportamiento o de rendimiento (Key Performance Indicator (KPI)), se determinan alertas, etc.

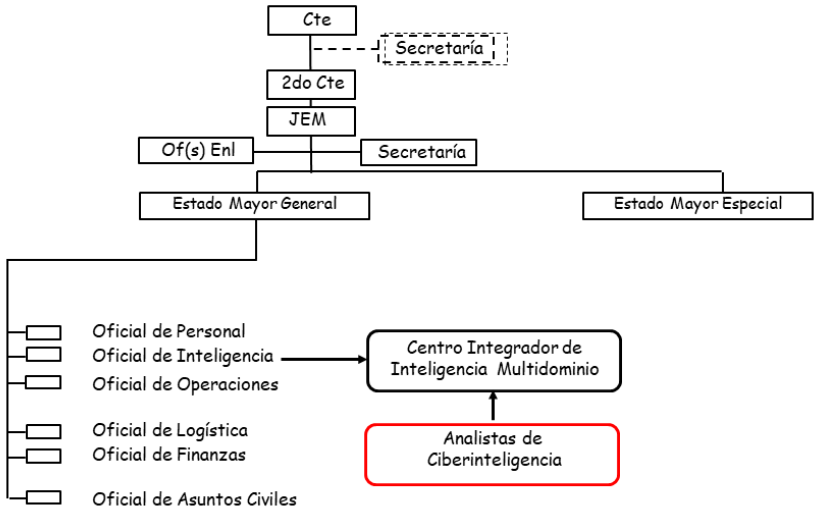
Para complementar los productos resultantes del ciclo de ciberinteligencia, es necesario determinar las capacidades y debilidades de los sistemas enemigos en el ciberespacio, el Orden de Batalla Cibernético y los efectos del ciberespacio sobre las operaciones propias y del enemigo.

Aporte Personal

De acuerdo a lo expresado en el presente trabajo, el estado mayor del componente terrestre debe estar conformado por la cantidad de especialistas necesarios para proporcionar toda la información de los actores, hechos o circunstancias de interés provenientes de todos los dominios. En este sentido, sería conveniente reforzar el centro integrador de inteligencia con analistas del ciberespacio, para que produzcan ciberinteligencia en apoyo directo al oficial de Inteligencia.

Figura Nro 6

Incorporación de analistas de ciberinteligencia



Nota: la imagen corresponde a la Figura 1, con el agregado de analistas de ciberinteligencia.

Glosario de términos

A continuación, se desarrollarán conceptos doctrinarios incorporados en la doctrina militar, necesarios para aclarar su significado y cuyo entendimiento contribuirá al desarrollo de esta investigación, los que se encuentran en el glosario para la acción militar conjunta (EMC, 2019)

a. Ambiente operacional cibernético (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 21): "Conjunto de condiciones y características que existen en forma estable o semiestable en el ciberespacio y, consecuentemente, influyen sobre las Infraestructuras Críticas y Activos de la Información del Sistema de Defensa Nacional y que, junto a otros elementos, forma parte del Ambiente Operacional"
b. Ambiente Cibernético o ciberespacio (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 89): "Ámbito tanto físico como virtual en el que se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de datos e información digital, a través de redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter distintivo está dado por el empleo excluyente de las tecnologías de la información y comunicaciones. Constituye un ámbito de actuación operacional del Instrumento Militar y otros actores cibernéticos".
c. Guerra cibernética (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 105): "Conjunto de actividades desarrolladas en el ámbito militar con el propósito de determinar y explorar la presencia de actividad enemiga en el ciberespacio, neutralizar y reducir el empleo del ciberespacio por parte del enemigo y asegurar el empleo del ciberespacio por los medios propios."
d. Seguridad cibernética (ciberseguridad) (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 182): Término general que se refiere a la situación en la cual una infraestructura crítica se considera protegida de amenazas, incidentes o agresiones

cibernéticas, proporcionando libertad de acción para el empleo de dicha infraestructura, de acuerdo con los lineamientos establecidos en la Política de Ciberseguridad Nacional.

e. Ciberamenazas o amenaza cibernética (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 26): Factor externo representado por la posibilidad que ocurra un fenómeno o un evento adverso en el Ciberambiente de Interés, en un momento, lugar específico, con una magnitud determinada y que podría ocasionar daños a las personas y/o a las instalaciones o medios TIC; la pérdida de personal o medios de vida y/o trastornos al empleo del Instrumento Militar u Objetivos de Valor Estratégico nacionales.
f. Ciberinteligencia (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 53) Actividades de Inteligencia realizadas en o desde el ciberespacio.
g. Infraestructuras críticas del Sistema de Defensa Nacional (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 112): Instalaciones, redes, servicios, medios técnicos y de tecnología de la información y comunicaciones, que proporcionan un servicio esencial al Sistema de Defensa Nacional y cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes.
h. Activos Críticos de Información: Son aquellos activos de información que cuentan con una criticidad MEDIA o ALTA en la matriz de identificación y clasificación de activos[1]. Los activos de información incluyen: datos, información, servicios y procesos de un sistema, software, hardware, comunicaciones, recursos materiales y recursos humanos que componen un sistema de información

A continuación, de desarrollan conceptos que no son doctrinarios, pero que son necesarios definirlos para continuar con el desarrollo del presente trabajo

i. Ciberataque o Agresión cibernética (Glosario de términos para el empleo militar para la AMC - PC 00 02 - Pág 21): “Acción ofensiva, voluntaria o no, que se ejecuta en el ciberespacio, sobre una infraestructura crítica o activo de información del sistema de defensa nacional y ocasiona, como consecuencia, daños a su disponibilidad, integridad y confidencialidad, afectando el desarrollo de las operaciones que ejecuta en cumplimiento de su misión”

Referencias

Aguilar, J. A. (2019). *Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad*. http. //scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992019000200024

Anónimo (S/F). *Servicios Gestionados*. https://www.innovery.net/es/seguridad-de-la-red/#1619022373984-cd0ad7c1-f910

Anónimo (2023). *¿Qué es el cibercrimen?* https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime

Anónimo (S/F). *Hacktivismo: definición, tipos, modus operandi y motivaciones*. https://www.lisainstitute.com/blogs/blog/hacktivismo-definicion-tipos-modus-operandi-motivaciones

Arenas, E (2021). *Organización de la Jefatura de Inteligencia del Comando Operacional de las fuerzas armadas en las operaciones multidominio*

Decreto 457/21 (2021). *Directiva de Política de Defensa Nacional (DPDN)*

Eissa (2019). *Defensa nacional: consideraciones para un enfoque analítico*

Ejército Argentino (2021) *Conocimientos Básicos Sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza*.

Ejército Argentino (2008) *Manual de inteligencia para el comandante o jefe de elemento*

Ejército Argentino (2008) *Inteligencia Táctica.*

EMCOFFAA (2019). *Terminología Castrense para la acción militar conjunta*.

Ejército Argentino (1995). *La Conducción Táctica Superior Terrestre.*

Directiva del Jefe del Estado Mayor General del Ejército Nro 918/18 (2018). *Régimen de funcionamiento del Subsistema Informático del Ejército - SUIE*

García, R. (S/F). *Consejos para un buen informe de inteligencia competitiva*. https://www.futurespace.es/consejos-para-un-buen-informe-de-inteligencia-competitiva/

Guerra, J. C. (2021). *Conformación de equipos multidisciplinarios para ciberseguridad y ciberdefensa*

Gutierrez, J. (2020). *El proceso de ciberinteligencia.* https://ciberpatrulla.com/ciberinteligencia-que-es/#%F0%9F%91%89_El_proceso_de_la_ciberinteligencia

Ley Nro 26.388 (2008) *Delitos Informáticos.* https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley Nro 25.326 (2001). *Protección de Datos Personales.* https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales

Ministerio de Defensa (2014). Resolución ministerial de defensa Nro 343

Ministerio de Defensa de España (2012). *El ciberespacio. Nuevo escenario de Confrontación.*

Maidana Mur, J. A. (2022). *Apoyo de ciberinteligencia a las operaciones militares.*

Orden Especial del Subjefe del Estado Mayor General del Ejército Nro 05/g/19 (2018)

Plan Estratégico del sistema de inteligencia del Ejército Argentino (2022/2026)

Sponer, J. M. (2012). *Diseño de un centro integrador de inteligencia conjunto en apoyo al C2 de un comando de teatro de operaciones*

Visceglie, G. (2019) Las Representaciones Sociales en las Organizaciones Militares en entornos complejos y de alta incertidumbre.

Visceglie, G. (2019). El liderazgo y la adopción de nuevos modelos mentales: Los Arquetipos Sistémicos.

Voiped (2023). *¿Qué es un NOC o Network Operation Center?.* https://www.voiped.eu/que-es-noc-o-network-operation-center