ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

Empleo de la fuente cibernética para la obtención de conocimiento de inteligencia a nivel estratégico

Trabajo de Suficiencia Profesional para optar el Título Profesional de Licenciado en Ciencias Militares con Mención en Administración

Autor

Luis Gustavo Castro González
(0000-0002-4487-8654)

Asesor

Dr. Carlos Alfonso Monja Manosalva
(0000-0003-3350-1250)

Lima – Perú

2021

Dedicatoria

"A mis hijos quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

A mi esposa por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias. A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Finalmente quiero dedicar esta tesis a todas mis amigas, por apoyarme cuando más las necesito, por extender su mano en momentos difíciles y por el amor brindado cada día, de verdad mil gracias hermanitas, siempre las llevo en mi corazón."

Agradecimiento

“Dicen que la mejor herencia que nos pueden dejar los padres son los estudios, sin embargo, no creo que sea el único legado del cual yo particularmente me siento muy agradecida, mis padres me han permitido trazar mi camino y caminar con mis propios pies. Ellos son mis pilares de la vida, les dedico este trabajo de titulación. Gracias padre Luis”

ÍNDICE

ÍNDICE DE FIGURAS

RESUMEN

La suficiencia profesional titulada: ***EMPLEO DE LA FUENTE CIBERNÉTICA PARA LA OBTENCIÓN DE CONOCIMIENTO DE INTELIGENCIA A NIVEL ESTRATÉGICO,*** tiene como objetivo verificar la viabilidad de producir inteligencia a partir de fuentes cibernéticas, principalmente para suplir las necesidades de planificación a nivel estratégico en el Ejército del Perú. En este contexto, la producción de inteligencia a partir de fuentes disponibles en el ciberespacio puede considerarse un reto, desde el punto de vista tecnológico, o una oportunidad para suministrar a los responsables de la toma de decisiones conocimientos fiables y oportunos.

Con la aparición de Internet y el creciente uso del ciberespacio, impulsado por la popularización de los medios sociales, la interconexión entre personas y organizaciones y la facilidad de acceso a la información han cambiado el comportamiento de la sociedad. A pesar de ello, en el ámbito de las operaciones militares, los conocimientos de inteligencia siguen desempeñando un papel decisivo. Con esta preocupación, este estudio busca, por medio de la investigación bibliográfica (búsqueda y selección de artículos publicados), encontrar ejemplos exitosos de producción de inteligencia en el mundo, capaces de probar la viabilidad de la producción de inteligencia estratégica a partir de fuentes cibernéticas, con énfasis en los medios sociales.

Se presenta una propuesta de innovación, como resultado de modelos internacionales que demuestran la relevancia de la labor de inteligencia en las operaciones militares; mediante la validez del uso de la ciberinteligencia en la producción de inteligencia, ejemplificando los tipos de información que se pueden obtener y las herramientas que se pueden aplicar en las operaciones militares llevadas a cabo para el nivel estratégico, operativo y táctico resultando esencial para su éxito.

Palabras clave: *Fuente Cibernética, Conocimiento, Inteligencia y Nivel Estratégico*

INTRODUCCIÓN

En el ámbito de las actividades de inteligencia se encuentra la inteligencia estratégica, una actividad de investigación específica que aborda las necesidades de conocimiento con suficiente amplitud y detalle para describir las amenazas, los riesgos y las oportunidades. En la práctica, la inteligencia y el análisis estratégico se centran en la capacidad de razonar de forma creativa sobre las posibles líneas de acción a adoptar a través de cuestiones de nivel macro, pero manteniendo siempre una conexión pragmática con el respectivo impacto en los resultados tácticos y operativos. Para la producción de inteligencia, gran parte de la información necesaria para comprender los factores físicos y humanos del entorno operativo está disponible públicamente.

En este contexto el autor del presente estudio, en su situación actual de Coronel de Infantería realiza esta suficiencia profesional basado en las experiencias adquiridas en la escala militar del Ejército del Perú. La constitución del trabajo se describe a continuación:

El primer capítulo presenta la Información General, donde se indica la Dependencia, fecha y la ubicación del departamento implicado donde el autor prestó servicios. Se da a conocer además del tipo de actividad.

En el segundo capítulo, se realiza el marco teórico, donde se incluye los campos y tipo de aplicación y con la definición de los términos.

El tercer y último capítulo, constituye los modelos de antecedentes nacionales e internacionales. La descripción teórica mencionada se basa en la revisión bibliográfica. El diagnóstico muestra la realidad del contexto actual. Por último, en este capítulo se presenta una propuesta de innovación, como medida de solución y parte más relevante del trabajo. Para finalizar el trabajo se presentan las conclusiones y las recomendaciones.

CAPITULO I
INFORMACIÓN GENERAL

1.1. Dependencia (donde se desarrolla el tema)

El Batallón de Infantería Motorizada Nº 15, orgánico de la Tercera Brigada de Fuerzas Especiales, en la Segunda División Ejército del Perú, en Tocache, fue la dependencia en donde se desarrolló el trabajo de Suficiencia Profesional.

1.2. Tipo de Actividad (Función y Puesto)

El cargo que ocupado fue como Comandante de Compañía del Batallón de Infantería Motorizada Nº 15. Esta actividad cumple con la responsabilidad de supervisar las operaciones militares estratégicamente establecidas en la planificación militar, y también incluyó las operaciones de control y protección, así como el apoyo civil al orden público y la paz.

1.3. Lugar y Fecha

El Batallón de Infantería Motorizada Nº 15, se encuentra acantonado en el distrito de Tocache del Departamento de San Martín, Perú. El autor establece estas funciones en el año 2006.

1.4. Visión del BIM Nº 15

Convertirse en un Batallón que represente el reconocimiento y respeto de los valores de disciplina, honestidad, respeto y lealtad, acate las responsabilidades y principios de la Constitución Peruana, y contribuya a la construcción de la paz social.

1.5. Misión del BIM Nº 15

En base a las obligaciones del Ejército peruano, la misión del Batallón de Infantería Motorizada Nº 15, es defender a la ciudadanía y el territorio nacional mediante el uso responsable del poder militar. Con el fin de proteger la defensa nacional y la soberanía nacional de la República del Perú de cualquier evento que afecte la integridad del país.

1.6. Funciones y actividades del Puesto que Ocupó

Como Jefe de Compañía e Batallón de Infantería Motorizada Nº 15, se desempeñan las siguientes funciones:

- ✓ Organizar y supervisar los servicios exteriores que realiza el Ejército.
- ✓ Priorizar a la asignación de materiales, equipos y personal a las unidades subordinadas.
- ✓ Brindar asesoramiento sobre la actualización del plan de acción policial vigente.
- ✓ Diseñar el ejercicio estratégico y uso táctico de la unidad de ejecución.
- ✓ Determinar el orden de prioridad para la asignación de materiales, equipos y personal a las unidades subordinadas de acuerdo con el plan actual.
- ✓ Coordinar con otras fuerzas en operaciones internas, especialmente en temas relacionados con operaciones conjuntas.
- ✓ Elaborar y distribuir un plan operativo.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Antecedentes Internacionales

Romero (2020). En su artículo científico titulado: *"Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados".* Revista de la Escuela Superior De Guerra Naval, Ecuador. Tuvo como objetivo describir el uso de la Inteligencia artificial como una herramienta estratégica de seguridad en contribución a la defensa de los Estados. En un mundo encadenado a la innovación tecnológica, el lenguaje que brindan las máquinas adquiere cada día más importancia en las llamadas máquinas útiles de toma de decisiones combinadas con la inteligencia humana, la llamada inteligencia artificial, cuyo empleo, innovación y desarrollo constituyen una de las principales ocupaciones para lograr su liderazgo, especialmente aquellos países que son capaces de hacerlo, es no solo mejorar su sociedad, sino también incorporarla a la estrategia nacional. Su aporte es servir a la seguridad del país bajo estrictos planes militares.

La importancia de la seguridad nacional de un país, cuyo objetivo es proteger los intereses nacionales durante las guerras, los conflictos y los tiempos de paz, es la piedra angular de un país. Se busca permanentemente crear fórmulas que permitan un perfecto equilibrio. Para ello, la inteligencia artificial se utiliza como una herramienta El surgimiento, por la diversidad de sus aplicaciones, puede ser el factor básico para que muchos autores creen la "Guerra Fría de la Inteligencia Artificial". Sin embargo, el uso de esta tecnología, que aún no está totalmente dirigida por humanos, tiene un largo camino por recorrer y se están estudiando sus beneficios y consecuencias.

Finalmente, grandes países como Estados Unidos, China y Rusia se dieron cuenta de la importancia de la inteligencia artificial en diversos campos del país y formularon estrategias de innovación tecnológica relacionadas con sus intereses como herramienta estratégica de defensa. Sin embargo, América Latina busca

implementar este desarrollo tecnológico en una tendencia cada vez más importante de acuerdo a sus capacidades.

Baretto (2017) en su trabajo investigativo referido a la guerra de los avances tecnológicos y del ciberespacio, enfocando específicamente todo lo concerniente a la defensa estructurada de la Nación Argentina y su plan estratégico de respuesta para garantizar la seguridad nacional, presentado para la Escuela Superior de Guerra Conjunta de Argentina. Tuvo como objetivo mediante la presente, abordar los alcances teóricos y prácticos más resaltantes brindados por los países que son potencia mundial en los temas de las variables de enfocadas en la investigación. Metodológicamente se trató de una investigación de corte descriptiva, en tanto se describirán los hallazgos de la información recabada a nivel nacional e internacional, así como los aportes de la experiencia práctica en la implementación del aspecto más resaltante de la defensa nacional de los distintos países enfocaos. Logrando concluir que aun cuando existen y se pueden identificar áreas de fragilidad en el aspecto relacionado a los sistemas cibernéticos argentinos, se propone un conjunto de conceptos básicos en aras del desarrollo de una estrategia militar que se vuelva sostenible con el tiempo, enrumbando a la argentina a ser una potencia mundial en los temas estudiados.

De Vergara y Trama (2017) en su aporte “Operaciones militares cibernéticas. Planeamiento y Ejecución en el nivel operacional.” Brindado a la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina. Tuvieron como propósito primordial realizar un estudio serio y concienzudo de la temática de la defensa de los países latinoamericanos de cara a sus carencias y realidades, en torno a la realidad europea o norteamericana en función a su trabajo por años y constante actualización en temas de defensa nacional, motivo por el cual son potencia mundial hoy en día y son los pioneros en presentar las agendas de actualidad en la problemática de la vulnerabilidad de los países frente a un ataque cibernético que pueda infligir daño a su territorio, entre otras afecciones. En ese sentido plantean una serie de reflexiones desde su perspectiva, concluyendo finalmente que en el nivel operativo de todas las fuerzas armadas, deben implementarse el trabajo desde el aspecto cibernético y en los países que ya se ha implementado es necesario actualizarse puesto que es ineludiblemente necesario

estar al día con todos los nuevos conceptos y conocimientos de defensa cibernética.

Escamilla (2018) en su aporte a la ciencia titulado “La seguridad cibernética en México”, presentada en la Universidad Nacional Autónoma de México. Buscó principalmente mediante su trabajo enfocado en la problemática de ciberseguridad, lograr aportes significativos y aplicables en el contexto mexicano en tanto se basa para realizar dichas propuestas en los alcances de la experiencia internacional de países desarrollados y no desarrollados en cuanto a la materia se trata. Metodológicamente se trata de una investigación de tipo descriptiva y se trabajó mediante una revisión de los mejores logros en la materia de ciberseguridad de países como Estados Unidos, República de Estonia, Israel, República de Corea y luego casos en vías de desarrollo hacia mejoras reales y prácticas como son los de la Unión Europea, el Reino Unido y de Colombia. De todo lo abordado el autor deriva la siguiente conclusión de su trabajo de investigación: sería ideal contar con un órgano autónomo que tenga las facultades dadas para poder emitir su propia normativa al respecto de la ciberseguridad, en tanto no tenga influencias de tipo política o económica, sino que tenga un trazo seguro y certero en el trabajo serio que necesita tener el área nacional de la seguridad cibernética que hoy en día es tan importante.

2.1.2 Antecedentes Nacionales

Sánchez (2018). En su trabajo de investigación titulado: *“Sistema de información geográfica militar y su uso en el sistema comando y control del Ejército en el CE-VRAEM año 2017”*, presentado en el Instituto Científico Tecnológico del Ejército – ICTE, Lima. Cuyo objetivo estuvo basado en dictaminar cómo el Sistema de Información Geográfica Militar puede tener relación con el Sistema de Comando y Control del Ejército en el CE – VRAEM, en el año 2017.

Dado que, en todos los niveles de operaciones militares, los comandantes de las *diferentes* unidades antiterroristas necesitan información para planificar y ejecutar sus ejercicios, especialmente en el contexto geográfico, deben aclarar la fuerza de combate contra el narcoterrorismo en el entorno geográfico en el Valle de

los Ríos Apurimac, Ene y Mantaro. Por las razones anteriores, es necesario contar con herramientas como los sistemas de información geográfica militar que puedan almacenar, analizar y actualizar la información militar geográfica requerida para la toma de decisiones con el fin de llevar a cabo operaciones antiterroristas y operaciones militares.

Por lo *tanto*, cualquier solución al problema del terrorismo debe incluir el uso de sistemas de información geográfica militar para localizar ubicaciones estratégicas y ubicaciones de transferencia de restos terroristas relacionados con el tráfico de drogas. Para situaciones necesarias, la disponibilidad de un sistema de comando y control compuesto por *instalaciones*, equipos, comunicaciones, procedimientos y profesionales, en el cual el comandante puede planificar, dirigir y controlar las operaciones de las fuerzas designadas para lograr las tareas encomendadas en el campo de operaciones, se deben incluir aspectos técnicos relacionados con aquellas partes de sistemas de misión complejos o sistemas de armas o sistemas de sistemas.

En conclusión, las funciones de estas partes están relacionadas con el campo C4I y son apoyadas por las TIC, lo que ayuda a integrar las capacidades de sus componentes y proporciona un nivel superior recopilación de inteligencia. Muchos sistemas de armas son muy importantes, como los sistemas de defensa contra misiles balísticos (BMD).

Inoguchi y Macha (2017) en su trabajo investigativo “Gestión de la ciberseguridad y prevención de los ataque cibernéticos en las Pymes del Perú, 2016”, desarrollada para la Universidad San Ignacio de Loyola, sede Lima. Tuvo como finalidad primordial buscar las mejores condiciones para que las pequeñas y medianas empresas peruanas puedan desarrollarse al máximo en tanto sean las medidas de sus posibilidades. Desarrollando un enfoque de investigación cuantitativa de nivel descriptivo correlacional de corte transeccional. Obteniendo como resultados que el 100% de los encuestados refieren que tiene vital importancia el desarrollo y mejoramiento de los estándares de ciberseguridad puesto que toda empresa debe resguardar todo su sistema de información, defendiéndose de la manera más adecuada sosteniendo una respuesta a cualquier posible ataque o intento de vulneración de ataques cibernéticos. Concluyendo finalmente que se evidencia una

clara carencia de la empresa Zavala Cargo S.A.C. en tanto no cuenta con niveles óptimos de ciberseguridad y se encuentra vulnerable a ataques de carácter cibernético lo cual redundaría en una condición muy débil de su resguardo defensivo en ciberseguridad.

Farfán, Núñez y Torres (2016) en su aporte a la ciencia “Estrategias para la modernización del ejército de Perú”, presentado a la Escuela de Posgrado de la Universidad del Pacífico. Tuvieron como propósito principal describir y delimitar planes estratégicos de acción a través de los cuales se pueda realizar una proyección que redunde en la mejora desde distintos ángulos de la realidad del ejército peruano. Desde el punto de vista metodológico la presente fue enmarcada en el CEPLAN la cual establece en sus cuatro procedimientos, lo necesario para desarrollar una estrategia de esta envergadura. Concluyendo finalmente que por las constantes amenazas, que incluso cada vez son más peligrosas, a nivel cibernético, se debe contar con personal militar más capacitado, sin embargo, no solo esto, también con mejores oportunidades de capacitarse y entrenarse tanto teóricamente, psicológicamente, como procedimentalmente, de esta manera se podrá sostener una defensa cibernética también con combate directo; por otra parte, existe normativa que puede permitir que se logre la modernización del ejército peruano como es el Acuerdo Nacional, el Plan Bicentenario, Ley de Modernización del Estado, entre otras normas en las cuales se puede trabajar proyectos y programas que encaminen al país hacia la modernización propiamente dicha que se espera.

León (2018) en su trabajo “Aplicación de la ciberinteligencia en el proceso de inteligencia en la dirección de inteligencia del ejército del Perú”, plantea como fin optimizar la aplicabilidad de la Ciberinteligencia en el Proceso de Inteligencia y, como objetivo, formular una propuesta innovadora orientada a enriquecer la doctrina referente a la Aplicación de la Ciberinteligencia en la Dirección de Inteligencia del Ejército; habiendo empleado como método, una descripción razonada acompañada de análisis y su respectiva síntesis; a manera de resultado demuestra que el personal de especialistas, desconoce los nuevos conceptos de Ciberespacio y Ciberinteligencia; finalmente, concluye que la falta de conocimiento de los nuevos conceptos de ciberinteligencia y las bondades que esta posee por

parte del personal de analistas de la Dirección de Inteligencia del Ejército; no permite que la ciberinteligencia contribuya en la recolección de datos e información en el Proceso de Inteligencia que esta Dirección ejecuta.

2.2 Descripción teórica

2.2.1. El Conocimiento

El conocimiento es la información combinada con la experiencia, el contexto, la interpretación y la reflexión, siendo la fuente de ventaja competitiva característica de las economías modernas. El conocimiento puede ser considerado como una entidad, que puede ser capturada, comunicada y acumulada; sin embargo, el conocimiento puede ser visto como un stock y un flujo, debido a su naturaleza dinámica y la forma en que se genera, transmite e incrementa (Archer-Brown y Kietzmann, 2018).

En este contexto, el conocimiento es un activo que está en constante estado de flujo, lo que exige comprender la forma en que puede fluir entre varios individuos, equipos y organizaciones. La obtención del conocimiento y su gestión son procesos críticos para las organizaciones (Archer-Brown y Kietzmann, 2018).

Según Archer-Brown y Kietzmann (2018), las cuestiones clave que determinan las características del conocimiento que generan implicaciones estratégicas críticas son:

a) ¿En qué medida se pueden transferir los conocimientos de forma que proporcionen una ventaja competitiva?

b) ¿Existe la capacidad, dentro de una perspectiva social, de combinar conocimientos?

c) ¿En qué medida se puede apropiar el conocimiento para generar valor?

d) ¿El nivel de especialización del conocimiento puede generar barreras para su reproducción?

Debido a estas características, en el contexto estratégico, la capacidad de gestionar el conocimiento se convierte en una de las competencias más importantes de una organización. Gestionar el conocimiento estratégico es buscar hacer algo útil del conocimiento, convirtiéndolo en una fuente sostenible de ventaja competitiva, es decir, permitir que la organización genere valor a partir de sus activos de conocimiento, ya sean explícitos o tácitos (Archer-Brown y Kietzmann, 2018).

En el ámbito de las operaciones militares, debido a su dinámica y complejidad, la clave del éxito no es sólo la fuerza, sino la capacidad de recoger información sobre la situación y transformarla en conocimiento a tiempo para la toma de decisiones. Para ello, es necesario recoger y procesar una enorme cantidad de datos procedentes de equipos, vehículos, estructuras, sistemas de comunicación y tropas empleadas por las fuerzas amigas, así como información sobre el enemigo y su movimiento (Mohamed y Al-Jaroodi, 2014). En este sentido, es evidente que la ventaja de la decisión, como defienden Symon y Tarapore (2015), depende de la integración de varios conjuntos de datos procedentes de numerosas fuentes, y el Big Data es una de las alternativas para las soluciones de inteligencia.

2.2.2. Big Data

Según Mohamed y Al-Jaroodi (2014), las grandes masas de datos, cuyo análisis, gestión y almacenamiento, debido a su tamaño, son incompatibles con los típicos sistemas de gestión de bases de datos, se denominan "Big Data". El tamaño de estas masas de datos oscila entre unas decenas de terabytes y varios petabytes, sobre los que las aplicaciones de Big Data extraen información de inteligencia y buscan nuevos conocimientos que se traduzcan en ventajas competitivas.

Siguiendo el mismo principio, Bartlett, Omand y Miller (2012) , definieron Big Data como el término utilizado para definir la investigación que se ocupa de la

capacidad de los seres humanos para realizar mediciones sobre el mundo, registrar, almacenar y analizar dichas mediciones en cantidades sin precedentes, permitiendo nuevos tipos de predicciones. Este análisis predictivo reúne una gran variedad de infraestructuras técnicas e intelectuales, desde la modelización y el aprendizaje automático hasta la estadística y la psicología.

La expansión del acceso a Internet, las redes sociales y el uso de dispositivos móviles, sumados a los más diversos tipos de sensores instalados en vehículos, carreteras, edificios, fábricas y otras instalaciones, producen, cada segundo, una enorme cantidad de datos, en los más diversos formatos, como mensajes, imágenes y vídeos, que se suman a una gigantesca masa de datos ya existente. La organización, el acceso y el tratamiento de estos datos, en la forma en que fueron recogidos, para que puedan incluirse en la toma de decisiones de las aplicaciones en tiempo real, suele considerarse un reto técnico complejo. Debido a de esto, el volumen, la variedad y la velocidad son las características que diferencian al Big Data a partir de bases de datos tradicionales (Mohamed y Al-Jaroodi, 2014).

La realización de análisis sobre estas grandes masas de datos permite identificar lagunas de conocimiento, correlaciones y asociaciones hasta ahora inesperadas, así como anomalías y comportamientos irregulares. En la planificación y ejecución de las operaciones militares, el conocimiento resultante del análisis de Big Data puede contribuir decisivamente a su éxito. Estos análisis pueden aplicarse en varias situaciones, como en la identificación de patrones o anomalías en el patrón de vida de un posible objetivo terrorista, en el seguimiento automático de objetivos militares en grandes áreas de vigilancia, o incluso en la identificación y priorización de áreas que requieren asistencia humanitaria y apoyo en la recuperación de desastres (Symon y Tarapore, 2015).

2.2.3. Planificación de operaciones militares

La imprevisibilidad, la fluidez y la difusión de los conflictos actuales, que suelen ser limitados, no declarados y de duración imprevisible, exigen que las

Fuerzas Armadas (FA) sean flexibles, versátiles y móviles, capaces de permitir su acción conjunta. En este sentido, la compatibilidad de los procedimientos y la integración de las acciones de las Fuerzas Únicas se vuelven fundamentales para la eficiencia de las Operaciones Conjuntas (Mohamed y Al-Jaroodi, 2014).

Con el fin de asegurar la armonía y alineación de los procedimientos adoptados en el ámbito de la Fuerza Terrestre con los practicados en Operaciones Conjuntas, la planificación para la preparación y empleo de la fuerza sigue las disposiciones del Sistema de Planificación Conjunta de Empleo de las Fuerzas Armadas. El ciclo completo incluye cuatro niveles de planificación, que no son estancos: político, estratégico, operativo y táctico, que permiten organizar las ideas y el trabajo (Bartlett, Omand y Miller, 2012).

Nivel político

El nivel político define los objetivos políticos de la planificación conjunta, la preparación y el empleo de las Fuerzas Armadas (FA) en los conflictos, destacando las directrices y condiciones para la planificación posterior, y es responsabilidad del Presidente de la República. En este nivel, entre otras definiciones, se firman alianzas, se formulan directrices para las acciones estratégicas de cada expresión del poder nacional y se definen las limitaciones para el uso de los recursos militares y el uso del espacio geográfico (Bartlett, Omand y Miller, 2012).

Nivel estratégico

En el nivel estratégico, las condiciones y directrices políticas se transforman en acciones estratégicas, que deben desarrollar los distintos ministerios, en coordinación con las acciones militares. En este nivel, a través de la adecuación, flexibilidad o cancelación de objetivos, las directrices y los recursos pueden ser reevaluados y ajustados (Bartlett, Omand y Miller, 2012).

El Planeamiento Estratégico Militar tiene como objetivo construir una capacidad de defensa que garantice la seguridad del país frente a las amenazas externas e internas, centrándose en el empleo conjunto de las fuerzas militares de forma articulada con otras expresiones del poder nacional. Se divide en tres etapas:

- Evaluación de la Situación y Desarrollo de Escenarios

- Examen de la Situación y Planificación
- Control de las Operaciones Militares;

En la etapa de Evaluación de la situación y Desarrollo de Escenarios, se identifican las amenazas y oportunidades que podrían implicar en el empleo de las fuerzas militares y se traducen en Hipótesis de Empleo. La evaluación de la situación actual es el proceso por el cual se toma conciencia de los hechos pasados y presentes en los contextos nacional e internacional, mientras que la elaboración de escenarios prospectivos considera la secuencia de eventos y el conocimiento que traduce la evolución de estos hechos en una situación futura, como resultado de un trabajo de inteligencia especializado y permanente (Bartlett, Omand y Miller, 2012).

En la etapa de Examen de la Situación y Planificación, se elaborará un Plan Estratégico de Empleo Conjunto de las Fuerzas Armadas para cada hipótesis de empleo identificado en la etapa anterior, que servirá de base para la planificación operativa y táctica. Dentro de este plan se identificará los objetivos estratégicos, los centros de gravedad (desde el punto de vista estratégico), el estado final deseado, la estructura y los medios militares, las áreas de responsabilidad y las principales acciones estratégicas de otras expresiones del poder nacional, entre otros (Bartlett, Omand y Miller, 2012).

La etapa de Control de las Operaciones Militares comprende las acciones adoptadas para monitorear y evaluar las operaciones realizadas por los Comandos Operativos Activados, a fin de verificar si la evolución de la situación conducirá efectivamente al estado final deseado. Los cambios en la situación, así como una evolución no deseada, pueden conducir a cambios en la planificación estratégica que, entre otras medidas, pueden alterar los objetivos políticos del conflicto, cambiar los límites de las áreas de responsabilidad y adjudicar nuevos medios a los comandos operativos activados (Bartlett, Omand y Miller, 2012).

Nivel operacional

A nivel operativo, se prepara el planeamiento militar de la campaña, observando los principales conceptos estratégicos, objetivos y el estado final

deseado definidos en el Plan Estratégico de Empleo Conjunto de las Fuerzas Armadas. Esta planificación define los objetivos operativos y las misiones de las fuerzas componentes (Bartlett, Omand y Miller, 2012).

En este nivel se realiza el Examen de la Situación Operativa para verificar la necesidad de alterar los límites de las áreas de responsabilidad y la necesidad de adecuar los recursos adjudicados. Para preparar el planeamiento a nivel operativo, es fundamental la información proveniente de las actividades de inteligencia y los datos actualizados sobre el Teatro de Operaciones (Bartlett, Omand y Miller, 2012).

Nivel táctico

En el nivel táctico, el planeamiento de las Fuerzas Componentes tiene lugar en paralelo y simultáneamente con el planeamiento operativo, a fin de permitir ajustes en el Plan Operativo basados en los resultados de los análisis de la situación táctica. Durante la planificación, se destaca el análisis detallado de los actores y de las áreas de responsabilidad, prestando especial atención a las posibilidades del enemigo y al seguimiento de sus acciones, sus centros de gravedad y sus vulnerabilidades críticas (Bartlett, Omand y Miller, 2012).

Desde esta perspectiva, uno se da cuenta de la relevancia de la información sobre el enemigo para la planificación de las operaciones militares. En este sentido, Handel (1990) destaca esta relación al tratar la inteligencia militar como factor de reducción de riesgos durante la planificación de las operaciones militares. El autor refuerza esta conexión, destacando la importancia de considerar sólo la información relevante sobre el enemigo en relación con lo que las propias fuerzas están haciendo o planeando.

2.2.4. Inteligencia Militar

En el ámbito militar, la inteligencia puede definirse como el producto resultante de la recopilación, el procesamiento, la integración, la evaluación, el análisis y la interpretación de la información disponible en relación con las naciones extranjeras,

las fuerzas o los elementos hostiles o potencialmente hostiles y las áreas de operaciones actuales o potenciales (Wilson, Gahan, Lennard y Robertson, 2018).

Según Wilson et al. (2018), la Inteligencia Militar (IM) es el resultado del procesamiento de información específica para un área de operaciones real o potencial, diferenciándose del proceso de construcción de la información, ya que requiere, además del procesamiento para dar un significado a los datos, un análisis relativo a sus implicaciones en las operaciones militares. Es un proceso que requiere, además del tratamiento de los datos para dotarlos de significado, un análisis de sus implicaciones para las operaciones militares.

La IM busca reducir el grado de incertidumbre existente en los diversos entornos operativos a partir del análisis e integración de los datos obtenidos por varios sensores, identificando amenazas y oportunidades. Para planificar y conducir las operaciones, desde el nivel táctico hasta el estratégico, es esencial comprender el entorno operacional, por lo que es responsabilidad de IM analizar las condiciones, circunstancias e influencias que pueden afectar a la ejecución de las acciones necesarias para cumplir la misión (Wilson et al., 2018).

Sin embargo, el valor de la inteligencia depende de cómo el responsable de la toma de decisiones decida utilizar la información que se le proporciona. Incluso si la recopilación y el análisis de los datos de inteligencia pueden ser totalmente precisos, y los resultados encontrados se comunican eficazmente, la decisión final sigue recayendo en la autoridad competente, que puede estar totalmente desconectada de los resultados de inteligencia (Wilson et al., 2018).

Para satisfacer las demandas de conocimiento durante las operaciones, los IM deben producir una combinación precisa y adecuada de conocimientos, independientemente del escalón en el que se originen. En este contexto, el IM debe emplear medios para suplir, de forma adecuada y dirigida, las necesidades de inteligencia de los comandantes en los niveles estratégico, operativo y táctico (Wilson et al., 2018).

Inteligencia a nivel estratégico

En el plano estratégico, la IM busca principalmente suministrar a los responsables de la toma de decisiones conocimientos sobre las expresiones de poder del enemigo, además de desarrollar evaluaciones y planificaciones estratégicas relacionadas con la seguridad y la defensa nacional. El foco de la IM, en este nivel, es la producción y salvaguarda de los conocimientos necesarios para la formulación de evaluaciones estratégicas para la producción de políticas y planes militares de alto nivel, destinados a la consecución de los objetivos nacionales (Wilson et al., 2018).

La labor de inteligencia a nivel estratégico es un proceso permanente de recopilación de información sobre las naciones de interés y las zonas de tensión internas, que se utilizan en la elaboración de directrices y planes militares a nivel nacional e internacional. En la planificación de las operaciones, el conocimiento de la IM es esencial: en la definición de los objetivos estratégicos, las amenazas, los riesgos, la logística y las misiones; en el dimensionamiento, la organización y el despliegue de las fuerzas componentes; en la delimitación del teatro de operaciones; y en la percepción de la opinión pública (Wilson et al., 2018).

Inteligencia a nivel operativo

En el nivel operativo, la Inteligencia Militar busca producir y salvaguardar los conocimientos de inteligencia necesarios para el planeamiento, la conducción y el sostenimiento de las operaciones militares en el contexto de la zona de acción de un mando operativo activado. Las actividades de IM en este nivel se ejercen permanentemente, tanto en situaciones de paz para el desarrollo y aplicación de planes operativos, como en situaciones de conflicto para la conducción de operaciones militares (Wilson et al., 2018).

Las acciones y actividades de IM a nivel operativo abarcan todos los factores que determinan cómo se emplearán conjuntamente los recursos terrestres, navales y aéreos, generando productos de carácter estimativo, que permiten analizar la importancia, intensidad y magnitud de una amenaza. Además, la IM debe contribuir

en la concepción, planificación y conducción de las campañas militares; y obtener conocimientos sobre el entorno de las operaciones y las posibles fuerzas hostiles (Wilson et al., 2018).

Inteligencia a nivel táctico

En el plano táctico, la prioridad de la IM se dirige a los objetivos esenciales de la campaña, con el fin de identificar las vulnerabilidades del enemigo, sobre las que se pueden desencadenar acciones decisivas. Las actividades de IM en este nivel buscan el conocimiento del entorno operacional y de las amenazas que en él se encuentran, con el fin de proporcionar conciencia situacional al comandante de la operación (Wilson et al., 2018).

El Comando Operativo es "el comando organizado de acuerdo con la Directiva para el Establecimiento de la Estructura de Defensa Militar, que es responsable de la ejecución de la campaña militar y otras acciones militares, de acuerdo con las directrices específicas de planificación", que es activado por el Presidente de la República de forma permanente o por el tiempo necesario para la ejecución de una determinada campaña militar (Wilson et al., 2018).

En este nivel, los conocimientos producidos y salvaguardados por las IM, son limitados y de corto alcance en el tiempo debido a la volatilidad del ambiente de batalla, razón por la cual, el principio de oportunidad crece en importancia, para proporcionar al comandante la capacidad de reevaluar frecuentemente la situación militar (Wilson et al., 2018).

El éxito de las operaciones militares tiene como factor determinante la oportunidad y la precisión de la inteligencia producida a todos los niveles. Estas cualidades están directamente relacionadas con la disponibilidad y fiabilidad de las fuentes de información (Wilson et al., 2018).

2.2.5. Fuentes de información

Cualquier persona, objeto o actividad de la que sea posible obtener datos e información sobre las fuerzas enemigas, el terreno, las condiciones climáticas o cualquier otro actor presente en el teatro de operaciones, se denomina "fuente" o "fuente de información". Una fuente importante para la construcción del conocimiento de inteligencia es el ciberespacio, un dominio global dentro del entorno informativo, que consiste en una red interdependiente de infraestructuras de tecnología de la información, que incluye internet, redes de telecomunicaciones, así como cualquier otro sistema informático capaz de almacenar o almacenar transmitir información (Quick y Choo, 2018).

La fuente cibernética es el recurso que permite obtener datos, protegidos o no, del ciberespacio, a través de acciones realizadas con herramientas computacionales. La integración de datos e informaciones obtenidas de la fuente cibernética, con las de fuentes humanas y fuentes abiertas, así como el análisis de imágenes, la exploración de información geográfica, el análisis del espectro electromagnético, entre otros, permite la producción de conocimiento de (Quick y Choo, 2018).

Las fuentes humanas son las personas de las que se obtiene la información y pueden ser amistosas, neutrales u hostiles. Por otro lado, las fuentes abiertas son cualquier medio a través del cual se ponen a disposición o se transmiten hechos, instrucciones u otros materiales, legalmente para el consumo del público en general, sin ninguna expectativa de privacidad (Quick y Choo, 2018).

Entre los principales vehículos de difusión de información que provienen de fuentes abiertas están los medios de comunicación mundiales, los blogs de la web, los informes gubernamentales, las imágenes de satélite (por ejemplo, Google Maps), los artículos académicos, Youtube, Facebook y otros grandes sitios publicados en Internet. Debido al crecimiento exponencial de la información publicada, se espera que en 2020 internet alcance un volumen de datos de 44 ZB (zettabytes), duplicando su tamaño cada dos años (Quick y Choo, 2018).

La información de código abierto puede definirse como "la información que está disponible públicamente y a la que se puede acceder legalmente mediante solicitud, compra u observación". Los anuncios publicitarios, las noticias sobre adquisiciones y negocios, las opiniones de los expertos y las publicaciones científicas producidas tanto por el sector privado como por los organismos gubernamentales y las instituciones académicas son ejemplos de información de fuente abierta (Quick y Choo, 2018).

Aunque Internet es un medio excelente para recoger información de fuentes abiertas, los datos recogidos deben someterse a un riguroso proceso de evaluación para determinar la fiabilidad de su origen. Además, en el entorno cibernético, no todos los datos están disponibles, siendo necesaria, en algunos casos y según la necesidad de conocimiento, la aplicación de técnicas de inteligencia para obtenerlos (Quick y Choo, 2018).

Open-Source Intelligence

A partir de la recopilación, procesamiento y análisis sistemático de información relevante que está disponible públicamente (fuentes abiertas), y que no está bajo el control directo del gobierno, se produce inteligencia de fuente abierta, en inglés llamada Open-Source Intelligence y conocida en sus siglas como OSINT. (Quick y Choo, 2018).

Al producir OSINT, hay que tener cuidado con la información de dominio público, ya que no está necesariamente verificada y puede ser sesgada e inexacta. La identificación de las fuentes de información es un proceso continuo ya que los diferentes medios de comunicación pasan por un ciclo de popularidad (Quick y Choo, 2018).

Sin embargo, Kalden (2018), destaca como principales ventajas, su flexibilidad, dinamismo, bajo coste y rapidez de producción. La OSINT también permite: identificar los riesgos y las estrategias a nivel estratégico, operativo y táctico; pasar de una evaluación rápida a un análisis más profundo en todos los

niveles de planificación; y contextualizar las necesidades de inteligencias tanto históricas como actuales.

Debido a estas características, el papel principal de la OSINT en las decisiones políticas nacionales e internacionales es generar resiliencia y ventaja competitiva. Además, otro factor importante es que, al producirse a partir de información de fuente abierta, la OSINT puede compartirse con otras agencias de inteligencia, así como con las inteligencias de otras naciones, aumentando recíprocamente los respectivos grados de confianza entre los implicados. En la actualidad, la información procedente de plataformas de medios sociales, como Facebook, ha alcanzado un gran protagonismo en la producción de inteligencia; sin embargo, no toda la información insertada en estas plataformas encaja como información de fuente abierta (Quick y Choo, 2018). Por ello, sumado a la relevancia que la inteligencia producida a partir de los medios sociales ha ido adquiriendo en los últimos años, incluso compartiendo el mismo ciclo de producción del OSINT (recolección, procesamiento y análisis, y difusión), es tratada como un tipo específico de inteligencia (Quick y Choo, 2018).

Social Media Intelligence

A partir de la explosión de los medios sociales, las actividades sociales, culturales e intelectuales comenzaron a ser capturadas en forma digital y compartidas en estas plataformas, haciendo que la vida social sea registrable y medible (Kalden, 2018). Así, estos medios de intercambio se han convertido en fuentes de obtención de información de inteligencia, dando lugar al Social Media Intelligence (SOCMINT), que es la inteligencia derivada de los medios sociales.

El SOCMINT puede definirse como la exploración analítica de la información disponible en el medio de comunicación social. Los autores añaden que se trata de la capacidad de monitorizar millones de cuentas y hashtags en tiempo real, y luego analizar y almacenar esos datos, con poco coste y, sobre todo, con poco impacto en la privacidad de las personas (Kalden, 2018).

Los medios sociales son un conjunto de tecnologías no estáticas cuya infraestructura tiende a cambiar con el tiempo. Por ello, el SOCMINT abarca una amplia variedad de aplicaciones, técnicas y capacidades, destinadas a recoger y utilizar los datos de las redes sociales para la producción de conocimientos de inteligencia (Kalden, 2018).

Entre las técnicas para acceder y procesar grandes conjuntos de datos directamente desde las plataformas de medios sociales, destaca el uso de las interfaces de programación de aplicaciones (API). Sin embargo, las condiciones de uso, el formato y la utilidad de los datos varían mucho de una plataforma a otra. Sin embargo, debido al crecimiento de la importancia y el valor asignado al análisis de Big Data, la disponibilidad de APIs para la recolección de datos en las diversas plataformas son cada vez más comunes (Kalden, 2018).

Al igual que en la OSINT, la SOCMINT requiere la validación de las fuentes y la interpretación de la información obtenida. Además, otro punto fundamental en la producción de SOCMINT, considerando la posibilidad de compartir la inteligencia producida, es distinguir la información de fuente abierta de aquella que tiene algún nivel de restricción de acceso (Kalden, 2018).

Las cuentas y grupos de Facebook, por ejemplo, suelen tener distintos grados de restricción de acceso y, además, las distintas plataformas suelen tener términos, condiciones y normas de uso completamente diferentes, por lo que no hay una definición clara de lo que puede considerarse información privada. Por ello, la inteligencia producida exclusivamente a partir de información de fuente abierta obtenida de los medios sociales se denomina específicamente “Open SOCMINT” (Kalden, 2018).

2.3. Definición de términos

Blogs: Son espacios web, donde se publica contenidos temáticos de manera intermitente bajo forma de artículos y, ordenados según la fecha de publicación; a menudo comentados por los lectores. (RAE, 2020).

Cibernética: Ciencia que estudia los sistemas de control, comunicación y regulación automáticas aplicado a los sistemas electrónicos y mecánicos. (Campos, 2021)

Ciberespacio: Espacio virtual creado con medios cibernéticos (Campos, 2021)

Ciberinteligencia: La ciberinteligencia trata del conocimiento acerca de las amenazas del ciberespacio, los actores, capacidades, vulnerabilidades, formas de acción y sus respectivos escenarios de riesgos, proporcionado para la toma de decisiones y la salvaguarda de los activos críticos nacionales. (León, 2018).

Conocimiento: es un conjunto de información almacenada a través de la experiencia o el aprendizaje mediante la introspección. En el sentido más amplio, tener múltiples datos interrelacionados, cuando se usa solo, tiene un valor cualitativo bajo (RAE, 2021).

Conocimiento estratégico: Es un tipo de conocimiento consustancial en la organización al saber acerca de planificación, descripción, impacto, predicción, evaluación y generación de estrategias.(Campos da Rocha, 2008)

Espectro electromagnético: Está conformado por el conjunto de longitudes de onda de las radiaciones electromagnéticas. Ejemplo rayos gamma.
(Revista Actualidad, 2021)

Estrategia de Seguridad Nacional: La Estrategia de Seguridad Nacional es el marco doctrinario-técnico para la política de Seguridad Nacional, siendo una política de Estado que parte de una concepción general de seguridad. (Jiménez, 2018)

Fuentes abiertas: Son fuentes de información, cuyos datos están a disposición del público de manera gratuita. (ej: internet, redes sociales, periódicos, etc.) (Jiménez, 2018)

Fuentes cerradas: Son fuentes de información, cuyos datos están protegidos, son confidenciales o su disponibilidad requiere un pago.
(Jiménez, 2018)

Fuente Cibernética: recurso que permite obtener datos, protegidos o no, del ciberespacio, a través de acciones realizadas con herramientas computacionales (Quick y Choo, 2018).

Innovación tecnológica: Es el cambio en materia de tecnología que comprende, tanto el lanzamiento de nuevos productos en el mercado por parte de las empresas, como la mejora o rediseño de las existentes con consecuencias en la industria y sus procesos internos.
(Noguera, Vargas y Collante, 2010)

Inteligencia: es la capacidad de elegir la alternativa más conveniente para resolver un problema (RAE, 2021).

Inteligencia Artificial: Es una combinación de algoritmos propuestos para crear máquinas con las mismas capacidades que los humanos (RAE, 2021).

Inteligencia estratégica:
Es el conocimiento sobre el cual se determina, tanto en la guerra como en la paz, las relaciones exteriores de una nación; siendo la política exterior el escudo de la República; vinculado a la prevención y la prospectiva. (Sherman, Kent, 1948)

Inteligencia estratégica militar: Es un conocimiento específico, codificado, y secreto, constituido por entidades militares y gubernamentales; cuya concepción como producto integrado es inherente a la Seguridad Nacional.
(Cifuentes, 2008)

Inteligencia militar: Es un conjunto de tareas desarrolladas por unidades especializadas de las fuerzas armadas, para recoger información sobre el adversario (medios y capacidades de combate actual o potencial), cuyos datos, permiten a los decisores, la planificación de posibles operaciones militares (táctica u operacional). (Prieto del Val, 2014)

Internet: se puede definir como una red informática global cuyo propósito es permitir que todos los usuarios intercambien información libremente. Simplemente podemos considerar la computadora como un medio para transportar información (RAE, 2021).

Nivel estratégico: está estrechamente relacionado con la prevención, previsión y advertencia de amenazas a los intereses vitales de la seguridad nacional y las oportunidades nacionales, convirtiéndose así en la principal herramienta del poder del gobernante para diseñar y formular políticas diplomáticas y de seguridad nacional (Glosario Militar, s.f.).

Obtención: Comportamientos y resultados de obtener, conquistar o lograr algo (RAE, 2021).

Ondas electromagnéticas: Están constituidas por la combinación de ondas de campos eléctricos y magnéticos, cundo se mueven juntos los dos campos generan ondas electromagnéticas. Así al acelerarse una partícula, ésta oscila en su campo eléctrico, lo cual produce un campo magnético.
(Revista Actualidad, 2021)

CAPÍTULO III
DESARROLLO DEL TEMA

3.1. Campos de Aplicación

El área en la cual se basa el estudio de investigación es el Batallón de Infantería Motorizada Nº 15, orgánico de la Tercera Brigada de Fuerzas Especiales, en la Segunda División Ejército del Perú, en Tocache, lugar donde el autor realizo funciones.

Línea de la investigación de la suficiencia profesional se direcciona al Proceso de aprendizaje-enseñanza. Técnicas, procedimientos y métodos activos. Estrategias de Enseñanza y Aprendizaje. Tecnología educativa. Didáctica de la enseñanza. La propuesta pedagógica: Constructivismo. Sistema de información.

3.2. Tipos de aplicación

Se ha mostrado la relevancia de la producción y aplicación de conocimientos de inteligencia en la resolución de conflictos mediante operaciones militares. En este caso, el uso de la inteligencia desempeña un papel decisivo en la eficacia de las operaciones y en la reducción de las bajas, tanto civiles como militares. En este sentido este estudio de suficiencia profesional se direcciona al uso operacional del Ejército del Perú.

Para demostrar el uso de la ciberinteligencia en las operaciones militares, se selecciona el uso de la inteligencia a nivel estratégico, operativo y táctico, con el objetivo de apoyar diferentes tipos de operaciones militares, producidos a partir de los medios sociales, utilizando diferentes técnicas y herramientas. Estos ejemplos no sólo confirmaron la posibilidad de utilizar fuentes cibernéticas en las operaciones militares, sino que también permitieron darse cuenta de que, independientemente del nivel de inteligencia que se produzca, sin los datos procedentes de los medios

de comunicación social, los resultados obtenidos en la ejecución de cada una de las misiones enumeradas se verían seriamente comprometidos, si no inviables

3.3. Diagnostico

El mundo virtual ha ganado cada vez más adeptos en las últimas décadas, creando un nuevo abanico de posibilidades, que hacen la vida más agradable gracias a la facilidad de acceso a la información y los servicios. Como consecuencias de la comodidad que ofrece el mundo virtual, una parte importante de la población ha entrado en la sociedad de la información, teniendo ésta como su activo más importante, que juega un papel importantísimo en la vida económica, política y social de las personas, organizaciones y naciones.

En el ciberespacio se realizan una gran variedad de actividades, como los mensajes de texto, el correo electrónico, las operaciones bancarias, el acceso a las noticias y las interacciones a través de las redes sociales. La capacidad de vigilar, recopilar y analizar la información que circula en el ciberespacio se ha convertido en algo fundamental para comprender el entorno operativo y dar forma a las operaciones militares, especialmente aquellas en las que el teatro de operaciones abarca grandes áreas urbanas.

La actividad de recoger, analizar y distribuir información sobre las capacidades, actividades y probables cursos de acción de países extranjeros o actores no estatales se denomina inteligencia. En el mismo sentido, la ciberinteligencia es la inteligencia producida a partir de la información obtenida en el ciberespacio.

En el ámbito de las actividades de inteligencia se encuentra la inteligencia estratégica, una actividad de investigación específica que aborda las necesidades de conocimiento con suficiente amplitud y detalle para describir las amenazas, los riesgos y las oportunidades. En la práctica, la inteligencia y el análisis estratégico se centran en la capacidad de razonar de forma creativa sobre las posibles líneas de acción a adoptar a través de cuestiones de nivel macro, pero manteniendo

siempre una conexión pragmática con el respectivo impacto en los resultados tácticos y operativos.

Para la producción de inteligencia, gran parte de la información necesaria para comprender los factores físicos y humanos del entorno operativo está disponible públicamente. Sin embargo, para que los esfuerzos por explotar los contenidos públicos sean eficaces, es necesario establecer procedimientos una adecuada validación y verificación tanto de las fuentes como de la información obtenida.

En este contexto, es importante subrayar la importancia del papel de la inteligencia en la producción de información que puede apoyar las operaciones militares. Para ello, se llevó a cabo esta investigación de carácter aplicado que, busca a través de un relevamiento bibliográfico, seleccionar informes cuyas evidencias fueran capaces de determinar la relevancia de la inteligencia en las operaciones militares, validar el uso de fuentes cibernéticas en la producción de inteligencia y demostrar el uso de fuentes cibernéticas en las operaciones militares, con énfasis en los medios sociales.

3.4 Propuesta de innovación

Durante la búsqueda bibliográfica, se encontraron casos de éxito que demuestran el uso de la inteligencia militar en situaciones de conflicto, que validando su uso para la producción de inteligencia militar y que benefician a las operaciones militares.

3.4.1. Objetivo de la propuesta

Tiene como objetivo la innovación e implementación en el uso de la fuente cibernética en la Producción de Inteligencia de las Operaciones Militares.

La propuesta presentada se basa a partir del análisis de una serie de referencias bibliográficas sobre la validación del uso de fuentes cibernéticas en la producción de inteligencia militar, a partir de las cuales se presentaron las razones

que hacen de las fuentes cibernéticas una fuente adecuada, si no indispensable, para la producción de inteligencia militar en los tiempos actuales.

La función de la inteligencia es proporcionar al responsable de la toma de decisiones información independiente e imparcial que sea oportuna, precisa, relevante, verificable, que responda a las preguntas y que permita la toma de decisiones de forma proactiva. Acostumbrar a los responsables de la toma de decisiones a los riesgos puede reducir sus temores e impotencia para tomar decisiones oportunas.

Por los puntos anteriores y los resultados presentados en la sección 3.2.1, es posible inferir que el conocimiento que produce el trabajo de inteligencia sigue siendo un diferencial en la planificación y ejecución de las operaciones militares, a pesar de los cambios en los formatos de los conflictos actuales. Otro rasgo importante observado en el análisis de los tres ejemplos seleccionados es que independientemente del tipo de conflicto, las especificidades del teatro de operaciones, así como el nivel de organización de las fuerzas opuestas, el conocimiento producido por la inteligencia fue esencial para reducir los efectos secundarios, las bajas de civiles y el tiempo necesario para lograr los respectivos objetivos militares.

Los estudios seleccionados presentan los distintos tipos de datos disponibles en el entorno cibernético y su aplicabilidad a la producción de conocimiento de inteligencia. También demuestran las razones que los hacen diferenciales en la búsqueda del éxito, tanto en las operaciones militares como en el mercado empresarial.

La explosión en el uso de las redes sociales junto con la evolución de técnicas y herramientas para la recolección, clasificación y procesamiento de información de fuentes cibernéticas, corrobora la viabilidad de su uso en una producción eficiente y eficaz, con conocimientos de inteligencia compatibles con las necesidades militares.

Otro punto que conviene destacar es la rápida evolución de las herramientas informáticas utilizadas en la labor de procesar y analizar las grandes masas de datos disponibles en las redes sociales.

Los ejemplos seleccionados y presentados representan propuestas viables para el uso de los conocimientos de inteligencia producidos a partir de los medios sociales para las operaciones militares. Aunque muchos estudios han demostrado el uso potencial de las fuentes cibernéticas para la producción de inteligencia, especialmente las redes sociales, hay pocos trabajos científicos publicados que informen de los resultados prácticos de su uso.

Dadas las limitadas fuentes de investigación, hemos optado por seleccionar tres ejemplos de operaciones militares llevadas a cabo en tres países diferentes que demuestran el uso de la inteligencia en sus tres niveles: estratégico, operativo y táctico. Los tres ejemplos tienen a los medios sociales como fuente principal para producir inteligencia; sin embargo, utilizan diferentes herramientas y métodos para la recolección, clasificación y procesamiento de la inteligencia.

En el primer ejemplo, el de Estados Unidos, que se centra en la vigilancia de las células terroristas en todo el mundo, el objetivo principal es producir inteligencia a nivel estratégico, identificando para cada célula su capacidad militar (potencia de fuego) y el nivel de amenaza que representa. Los conocimientos de inteligencia producidos por EE.UU. se utilizan para realizar la planificación necesaria dentro de todas sus fuerzas para garantizar la seguridad de su territorio, así como de sus tropas cuando operan en otros países.

En el segundo ejemplo, el holandés, que se enfoca en proteger sus aguas costeras, el objetivo principal es producir inteligencia a nivel operacional que permita mapear riesgos geoespaciales, anticipando la probabilidad de que ciertos eventos ocurran en ciertos lugares. Todo esto con el fin de producir un conocimiento de la situación, en el área de operaciones de la Guardia Costera holandesa, suficiente para la planificación y uso de sus escasos recursos marítimos.

Del mismo modo, en el último ejemplo, el británico, cuyo objetivo principal es la seguridad interna de la ciudad de Londres durante las protestas y

manifestaciones, el objetivo es producir inteligencia para el nivel táctico, identificando con antelación, y durante las manifestaciones, a los líderes de los movimientos, a otros participantes que muestren signos de comportamiento extremista, y los probables puntos de encuentro de estos participantes. El objetivo es planificar con antelación la actuación policial durante las manifestaciones y permitir que la Policía de Londres responda de forma eficiente, eficaz y efectiva a cualquier acto hostil/extremista inminente o en curso.

Por lo expuesto en esta discusión de los resultados, es posible afirmar que el uso de la fuente cibernética y las tecnologías relacionadas con ella son lo suficientemente maduros para su uso en la producción de inteligencia a nivel estratégico. También se puede inferir que, en unos años, la producción de inteligencia a partir de fuentes cibernéticas, especialmente las redes sociales, ya no será un diferencial para el éxito de las operaciones militares, convirtiéndose en un prerrequisito para que su negligencia inevitablemente resulte en un fracaso.

3.4.2. Descripción simple de la propuesta

- ✓ Establecer una Estrategia de Seguridad e inteligencia Nacional basado, por lo general, no sólo en el consentimiento y la comprensión de los ciudadanos, sino también en la colaboración y participación activa de los individuos y las comunidades. Se producen graves daños a la seguridad cuando los esfuerzos del Estado no son aceptados o no se confía en ellos.

- ✓ Por ello, medir y comprender el punto de vista de millones de personas a través de lo que están discutiendo, hablando, bromeando, condenando y aplaudiendo digitalmente es de amplio interés y de enorme valor para las más diversas áreas del conocimiento, gobiernos y otras organizaciones. Las organizaciones usan herramientas llamadas "Social Media Analytics" para rastrear en las redes sociales las actitudes de sus clientes hacia sus marcas, productos y servicios con el fin de monitorear su reputación, al igual que los gobiernos de todo el mundo usan las mismas herramientas para mapear el

conocimiento popular para la planificación. soluciones para situaciones de emergencia.

✓ Los nuevos programas informáticos y las herramientas de análisis de las redes sociales han hecho posible el mayor nivel de vigilancia jamás visto, lo que conlleva tanto riesgos como oportunidades. En consecuencia, en los últimos años se ha producido un importante crecimiento de los estudios académicos sobre los denominados "Social Big Data", que combinan las ciencias sociales y la informática para recopilar, agregar y comprender cantidades muy grandes de datos sociales extraídos de los medios sociales.

El uso de la fuente cibernética en las operaciones militares

El uso de las fuentes cibernéticas mediante proyectos/operaciones militares en los diferentes niveles la producción de conocimientos de inteligencia utilizando los medios sociales como fuente principal es fundamental para su éxito.

- ✓ Las inteligencias de Infantería del Ejército del Perú deben mapear desde las redes sociales, entre otros objetivos, las actividades, intenciones y logística a nivel global de grupos con sesgo terrorista. Para ello, se debe utilizar una variedad de software de análisis / métricas como Visible: Socializing the Enterprise, Geofeedia (herramienta de reconocimiento facialo DoD's Information Volume and Velocity, o Recorded Future, e o Palantir.

- ✓ Incluso con el apoyo de estas herramientas, y su eficacia cuando se trata de fines específicos, en el ámbito de la inteligencia estratégica, la capacidad para recoger información debe superar con creces su capacidad para analizarla. A pesar de la potencia de estas plataformas, y aunque todos los datos obtenidos sean Marcados temporal y geoespacialmente, también es necesario que el analista sepa específicamente qué buscar.

- ✓ Debido al creciente uso de los medios sociales para la organización y movilización de masas, la utilización de Social Media Intelligence (SOCMINT) resulta una herramienta para obtener un eficaz conocimiento de

la situación y desarrollar estrategias para contener los desórdenes y el extremismo en el ámbito doméstico, especialmente en las manifestaciones y protestas.

- ✓ Para recoger y analizar la información de las redes sociales, adquirir herramientas comerciales de proveedores, como TweetDeck y Hootsuite, que deben adaptarse a las características de los principales tipos de análisis que realizan las herramientas como: la búsqueda de palabras clave que permiten encontrar potenciales amenazas, la evaluación de riesgos y recursos, y la identificación de organizadores/influenciadores, todo ello apoyado por algoritmos capaces de filtrar el ruido y permitir que el análisis trabaje solo sobre los datos relevantes.

- ✓ Una parte esencial para extraer el mayor potencial de inteligencia artificial de los sistemas expuestos es la interconexión. La información debe intercambiarse continuamente entre sistemas para que cada sistema pueda responder a amenazas inminentes o futuras lo más rápido posible, lo cual es crucial. Por ello, el protocolo de intercambio de información debe ser lo suficientemente robusto y seguro para no perder información y evitar intrusiones enemigas.

La siguiente figura representa de forma esquemática los bloques en los que se puede utilizar la sonsorización y la inteligencia artificial en el campo de batalla.

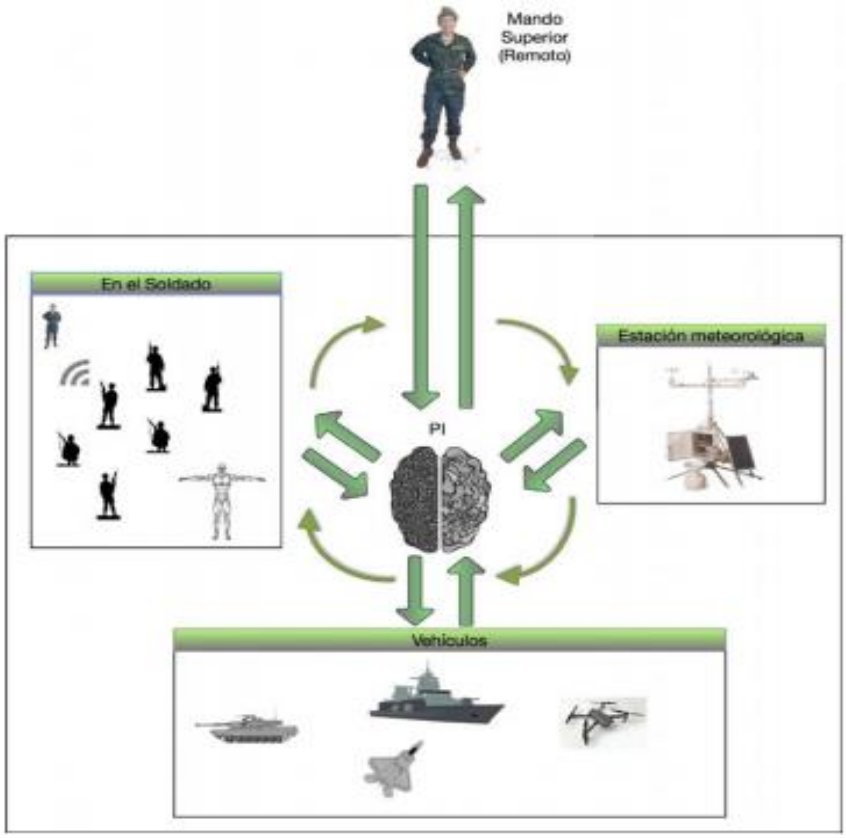


Figura 1. Utilización de sensores en el campo de batalla

Fuente:https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/Usos_militares_inteligencia_artificial.pdf

Big Data: Posible funciones para el Ejército del Perú

- ✓ Incrementa la existencia y la disponibilidad de datos relacionados directamente o indirectamente con actividades criminales.

- ✓ Incremento de la cantidad e importancia de los datos asociados con la seguridad de la información y las tecnologías de la información.

- ✓ Fortalece la Inteligencia militar, a través de la Consciencia situacional, Planeamiento táctico de misiones, Toma de decisión en tiempo real para las operaciones (Defensa/seguridad).

- ✓ Ofrece seguridad ciudadana mediante la vigilancia perimetral a través de la seguridad física de las infraestructuras críticas.

- ✓ Ofrece una mejor Comunicación y redes seguras, mediante el análisis automático de vulnerabilidades de red (máquinas-tráfico de datos), Criminología computacional

- ✓ Mejora la Protección (redes IT) de Infraestructuras críticas, Ciberdefensa / Ciberseguridad.

- ✓ Ayuda en la Infraestructura necesaria para el análisis en tiempo real que sirve para el apoyo en la lucha contraterrorista y contra el crimen organizado.

- ✓ Optimiza el Control y seguridad de los recursos informáticos y datos en organizaciones militares.

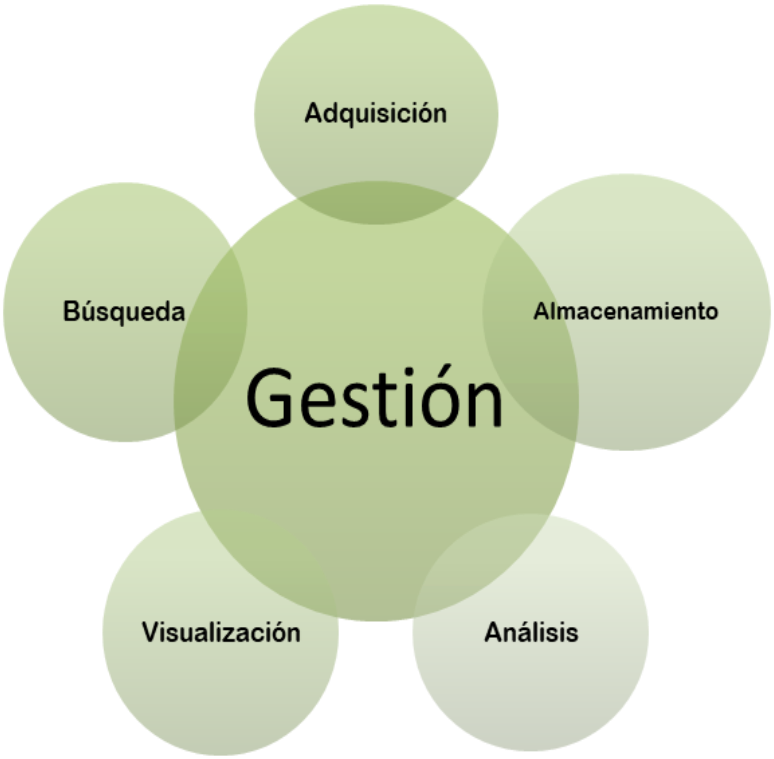


Figura 2. Posibles funciones de la Big Data

Fuente:https://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/174/AplicacionesBigDataDefensaSeguridad.pdf

CONCLUSIONES

Este trabajo comenzó describiendo varios conceptos relevantes para la investigación, entre ellos el concepto de conocimiento, su valor y la importancia de su gestión y aplicación en la toma de decisiones; el concepto de Big Data, sus características, formas de explotación y posibilidades de aplicación en las operaciones militares; el concepto de planificación de las operaciones militares, destacando sus características a nivel político, estratégico, operativo y táctico; el concepto de inteligencia militar, su aplicación, limitaciones y sus características según el nivel en el que se aplique; el concepto de fuentes de información, sus principales vehículos; y por último, los conceptos de inteligencia de fuentes abiertas y medios sociales, describiendo sus características y ventajas.

Se validó el uso de las fuentes cibernéticas en la producción de inteligencia militar, presentando las razones que hacen que los datos de estas fuentes, especialmente los disponibles en los medios sociales, sean fundamentales para la producción de inteligencia en la actualidad. Además, se presentó la evolución de las herramientas y técnicas para la recogida, clasificación, análisis y producción eficiente de inteligencia a partir de grandes cantidades de datos (Big Data). A continuación, para demostrar el uso de la ciberinteligencia en las operaciones militares, se seleccionaron tres ejemplos de uso de la inteligencia a nivel estratégico, operativo y táctico, con el objetivo de apoyar diferentes tipos de operaciones militares en diferentes países, producidos a partir de los medios sociales, utilizando diferentes técnicas y herramientas.

Para finalizar la suficiencia profesional presenta una propuesta de innovación, a partir del análisis de los resultados obtenidos en la investigación, a través del cual se pudo concluir que las técnicas y herramientas para la producción de conocimiento a partir de "Big Data", provenientes de fuentes cibernéticas, ya han alcanzado un nivel de madurez capaz de satisfacer las demandas de inteligencia a nivel estratégico. Otro hecho importante que cabe destacar es la rapidez con la que evolucionan las herramientas, haciéndolas cada vez más especializadas en la producción de inteligencia específica para determinados fines.

RECOMENDACIONES

a) Se recomienda al Comando General del Ejército del Perú, optimizar la implementación de los componentes del Sistema de Inteligencia mediante el diseño de nuevas tecnologías y sistemas de información utilizando las instalaciones, los equipos, las comunicaciones, procedimientos, con el personal especializado a fin de viabilizar la interoperabilidad del Sistema de Comando y Control del Ejército para la toma de decisiones que ejerce las atribuciones del Comandante de las Operaciones para alcanzar un determinado objetivo.

b) Se recomienda implementar proyectos de entrenamiento sobre aspectos cibernéticos, Big Data, Inteligencia Militar, Fuentes de información (Open-Source Intelligence, Open-Source Intelligence) empleando las capacidades y recursos suficientes para establecer una eficiente formación al personal militar responsable de estas actividades.

c) Se sugiere como trabajo futuro, realizar una comparación de los resultados obtenidos en este trabajo con la producción de inteligencia a nivel nacional. También se sugiere seleccionar un conjunto de herramientas entre las aquí mencionadas, para su integración y aplicación en un ejemplo práctico para la producción de inteligencia a nivel estratégico, considerando como "teatro de operaciones" las áreas donde se desarrollan las acciones militares debido a la intervención en seguridad pública del Perú.

d) Durante la realización de esta investigación, el principal obstáculo encontrado fue el escaso número de artículos científicos publicados con ejemplos de aplicación práctica de la inteligencia, probablemente porque el tema se trata de forma restringida dentro de las agencias de inteligencia de cada país, por ello se recomienda seguir con nuevas investigaciones relacionadas a este tema para contribuir a un mejor conocimiento.

REFERENCIAS BIBLIOGRÁFICAS

Archer-Brown, C. y Kietzmann, J. (2018). Gestión estratégica del conocimiento y redes sociales empresariales. *Journal of Knowledge Management 2*2(1) DOI: 10.1108 / JKM-08-2017-0359 Recuperado de: https://www.researchgate.net/publication/323467220_Strategic_knowledge_management_and_enterprise_social_media

Baretto J. (2017) "La defensa nacional y la estrategia militar de seguridad cibernética". Maestría en Estrategia y conducción superior de la Escuela Superior de Guerra Conjunta. Ministerio de Defensa – Argentina. http://cefadigital.edu.ar/bitstream/1847939/1061/1/TFM%2004-2018%20BARETTO.pdf

Campos da Rocha, R. (2008) System of Strategic Knowledge Management. https://www.revistaespacios.com/a08v29n02/08290221.html

Campos K. (2021) Importancia de la cibernética en el contexto internacional.

Cifuentes, I. (2008), Inteligencia Estratégica, Perspectiva Militar, https://perspectivamilitar.blogspot.com/2008/02/inteligencia-estratgica.html

De Vergara E. y Trama G. (2017) Operaciones militares cibernéticas. Planeamiento y Ejecución en el nivel operacional. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina. https://esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

Escamilla E. (2018) "La seguridad cibernética en México." Universidad Nacional Autónoma de México.

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/14839/Tesis.pdf?sequence=1

Farfán J., Núñez E. y Torres A. (2016) “Estrategias para la modernización del ejército de Perú.” Escuela de Posgrado de la Universidad del Pacífico. https://repositorio.up.edu.pe/bitstream/handle/11354/1146/Manuel_Tesis_maestria_2016.pdf?sequence=13

Glosario Militar (s.f.). *Glosario Militar.* Recuperado de: http://www.ccffaa.mil.pe/cultura-militar/glosario-militar/

Handel, L. (1990). *Intelligency and Military Operations*. Routledge. Recuperado de: https://www.routledge.com/Intelligence-and-Military-Operations/Handel/p/book/9780714640600

Inoguchi A. y Macha E. (2017) “Gestión de la ciberseguridad y prevención de los ataque cibernéticos en las Pymes del Perú, 2016.” Universidad San Ignacio de Loyola.

http://repositorio.usil.edu.pe/bitstream/USIL/2810/1/2017_Inoguchi_Gestion-de-la-ciberseguridad.pdf

Jiménez, R. (2018) Global Strategy

https://global-strategy.org/tipos-de-inteligencia/

Kalden, J. (2018). Análisis de datos dentro de la Guardia Costera de los Países Bajos: mapeo de riesgos, análisis de redes sociales y detección de anomalías. *NL ARMS Netherlands Annual Review of Military Studies* 2018. TMC Asser Press, p. 193-20. Recuperado de: https://www.springerprofessional.de/en/data-analysis-within-the-netherlands-coastguard-risk-mapping-soc/15950044

León, J. (2018) “Aplicación de la ciberinteligencia en el proceso de inteligencia en la dirección de inteligencia del ejército del Perú” http://repositorio.escuelamilitar.edu.pe/handle/EMCH/805

Ministerio de Defensa España.

https://www.defensa.gob.es/defensa/politicadefensa/estrategiaseguridad/

Mohamed, N. y Al-Jaroodi, J. (2014). *Real-Time Big Data Analytics: Applications and Challenges.* Proceedings of the 2014 International Conference on High Performance Computing and Simulation, HPCS 2014. 10.1109/HPCSim.2014.6903700. Recuperado de: https://www.researchgate.net/publication/283212652_Real-Time_Big_Data_Analytics_Applications_and_Challenges

Noguera, Vargas y Collante (2010) Innovación Tecnológica

https://www.google.com/search?q=innovaci%C3%B3n+tecnol%C3%B3gica+definici%C3%B3n&client=firefox-b-d&sxsrf=AOaemvLwiV1ipzgkpotMVjYH0O-iq79Z0w:1631915474008&tbm=isch&source=iu&ictx=1&fir=h76WQIQ6fwTrwM%252CjjTbHB_8aoAhVM%252C_&vet=1&usg=AI4_-kRRT_JjSOwoOyE_HwP-mLXUXiYlw&sa=X&ved=2ahUKEwjJo4bx_obzAhVbHbkGHZyuBjEQ_h16BAhEEAE#imgrc=edWOWRHVEqD1-M&imgdii=Rgc9yvIJruUmIM

Omand, D., Bartlett, J. y Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security. 27*. 10.1080/02684527.2012.716965. Recuperado de: https://www.researchgate.net/publication/262869934_Introducing_social_media_intelligence_SOCMINT

Prieto del Val, T. (2014) La Inteligencia Militar, una constante histórica.

http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO79-2014_InteligenciaMilitar_PrietodelVal.pdf

Quick, D. y Choo, K. (2018). Inteligencia forense digital: subconjuntos de datos e inteligencia de código abierto (DFINT + OSINT): una combinación coherente y oportuna. Future Gener. Computación. Syst., 78 , 558-567. Recuperado de: https://www.semanticscholar.org/paper/Digital-forensic-intelligence%3A-Data-subsets-and-A-Quick-Choo/49d3c6c0b058df491ddbbd5eb1a324ad87bf5319

Real Academia Española (RAE) 2021. Recuperado de: https://dle.rae.es

Revista Actualidad (2021) Ondas electromagnéticas.

https://www.redeweb.com/actualidad/ondas-electromagneticas/

Romero Mier, S. (2020). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista De La Escuela Superior De Guerra Naval, 16*(1), 51-70, Ecuador. Recuperado de: https://doi.org/10.35628/resup.v16i1.67

Sanchez, J. (2018). *"Sistema de información geográfica militar y su uso en el sistema comando y control del Ejército en el CE-VRAEM año 2017",* Instituto Científico Tecnológico del Ejército – ICTE, Lima. Recuperado de: http://repositorio.icte.ejercito.mil.pe/handle/ICTE/69

SHERMAN KENT, (1948) Inteligencia estratégica para la política mundial norteamericana.

https://www.economiapersonal.com.ar/wp-content/uploads/2018/07/Inteligencia-Estrategica-_-Sherman-Kent.pdf

Symon, P. y Tarapore, A. (2015). Análisis de inteligencia de defensa en la era del Big Data. *Joint Forces Quarterly — JFQ, 79*, pág. 4-11. Recuperado de: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_4-11_Symon-Tarapore.pdf

Vilcarromero L. y Vílchez E. (2021) "Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones." Universidad Peruana de Ciencias Aplicadas. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624832/VilcarromeroZ_L.pdf?sequence=11&isAllowed=y

Wilson, E., Gahan, M., Lennard C. y Robertson J. (2018). El continuo de la inteligencia forense en el contexto military. *Australian Journal of Forensic Sciences*, p. 1-13. Recuperado de: https://www.tandfonline.com/doi/abs/10.1080/00450618.2018.1459839

ANEXOS

ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI

"Alma Mater del Ejército del Perú"

ANEXO 01: INFORME PROFESIONAL PARA OPTAR
EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES

1. DATOS PERSONALES:

1.01	Apellidos y Nombres	CASTRO GONZÁLEZ LUIS GUSTAVO
1.02	Grado y Arma / Servicio	CRL INF
1.03	Situación Militar	ACTIVIDAD
1.04	CIP	118373700
1.05	DNI	44218930
1.06	Celular y/o RPM	944972203
1.07	Correo Electrónico	LUIZCAZTRO.G@GMAIL.COM

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	27 MARZO 1993
2.02	Fecha_ egreso EMCH	01 ENERO 1997
2.04	Fecha de alta como Oficial	01 ENERO 1997
2.05	Años_ experiencia de Oficial	24
2.06	Idiomas	PORTUGUES -ESPAÑOL

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

Nº	Año	Lugar	Unidad / Dependencia	Puesto Desempeñado
3.01	2006	TOCACHE	BIM 15	JEFE CIA

3.02	2008	LIMA	SIE	ANALISTA
3.03	2014	PICHARI	EM 2DA BRIG INF	G-2
3.04	2017	MOQUEGUA	EM 3RA BRIG BLIN	G-3
3.05	2020	PICHARI	CEVRAEM	C-2

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

Nº	Año	Dependencia y Período	Denominación	Diploma / Certificación
4.01	2008	ESCUELA DE INTELIGENCIA DEL EJERCITO	CURSO BASICO DE INTG	CURSO BASICO DE INTELIGENCIA
4.02	2011	ESCUELA DE GUERRA DEL EJERCITO	EMPLEO DE GRANDES UNIDADES DE COMBATE	MAGISTER EN CIENCIAS MILIATRES
4.03	2012	ESCUELA CONJUNTA DE LAS FFAA	CURSO EM CONJUNTO	PROGRAMA DE ESTADO MAYOR CONJUNTO
4.04	2018	ESCUELA CONJUNTA DE LAS FFAA	CURSO SUPERIOR DE INTG CONJUNTO	CURSO SUPERIOR CONJUNTO

5. ESTUDIOS DE NIVEL UNIVERSITARIO

Nº	Año	Universidad y Período	Bachiller - Licenciado
5.01	2009	ESCUELA MILITAR DE CHORRILLOS	BACHILLER EN CIENCIAS MILITARES

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

Nº	Año	Universidad y Período	Grado Académico (Maestro – Doctor)
6.01	2015	ESCUELA SUPERIOR DE GUERRA	MAESTRO EN CIENCIAS MILIATRES
6.02	2019	ENRIQUE GUZMAN Y VALLE	MAESTRO EN CIENCIAS DE LA EDUCACION

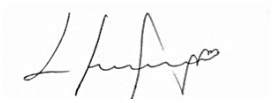
7. ESTUDIOS DE ESPECIALIZACIÓN

Nº	Año	Dependencia y Período	Diploma o Certificado
7.01	2009	UNIVERSIDAD CATOLICA DEL PERU	RESOLUCION DE CONFLICTOS SOCIO

			AMBIENTALES
7.02	2011	CAEN	INTELIGENCIA ESTRATEGICA

8. ESTUDIOS EN EL EXTRANJERO

N°	**Año**	**País**	**Institución Educativa**	**Grado / Título /**
8.01				



CRL LUIS CASTRO GONZALEZ