ESCUELA MILITAR DE CHORRILLOS
"CORONEL FRANCISCO BOLOGNESI"

Propuesta de optimización en el planeamiento y empleo del Batallón de Infantería en la protección de infraestructuras Críticas

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

Autor

Paul Gianfranco Bellido García
(0000-0002-4487-8654)

Asesor

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

Lima – Perú

2021

Dedicatoria

“El presente trabajo lo dedico a mis señores padres quienes siempre velaron por mi bienestar y buena educación y por ello llegue a esta etapa de mi vida profesional”

Agradecimiento

"Agradezco a todos mis docentes quienes me formaron en esta casa de estudios que fueron los cimientos de mi persona y de mi carrera profesional"

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente estudio titulado: *Propuesta de optimización en el planeamiento y empleo del Batallón de Infantería en la protección de infraestructuras Críticas,* establece la revisión conceptual del término de infraestructura crítica, así también se busca dar a conocer el concepto de infraestructura estratégicas desde la perspectiva internacional y especializada en el tema, con el objetivo de comprender la relevancia de resguardar las estructuras en el escenario nacional, proponiendo una forma operativa para optimizar la planificación y uso de un Batallón de Infantería en la ejecución de esta tarea.

El Ejército del Perú ha sido empleado varias veces para asegurar la ejecución de grandes eventos, en paralelo con el mantenimiento de la integridad de las estructuras estratégicas, especialmente en los grandes centros urbanos. Sin embargo, la demanda para la ejecución de estas actividades, especialmente en lo que respecta a la contratación de personal, es muy elevada, superando casi siempre la capacidad de empleo de las fracciones ocupadas.

Los resultados descubiertos en este estudio permitieron comprender de manera adecuada el tema planteado. En este sentido se presenta una propuesta de mejora que plantea la creación de un Departamento de Protección de Infraestructuras, ofreciendo una amplia variedad de Programas de Capacitación. En este sentido sugiere también la optimización de la planificación y empleo en la protección de estructuras estratégicas por parte de un Batallón de Infantería, sirviendo como presupuesto teórico para una mejora en la ejecución práctica de la referida actividad.

Palabras clave: *Optimización, Planeamiento, Batallón de Infantería en Infraestructuras Críticas e Infraestructuras Estratégicas.*

INTRODUCCIÓN

El proceso de crecimiento económico, reconocimiento y proyección internacional que asume el país, requiere una ampliación de la capacidad operativa del Ejército del Perú. Para ello, la Fuerza Terrestre debe ser capaz, volviéndose más eficiente en la misión de preservar sus estructuras estratégicas y en condiciones para ser utilizada para enfrentar posibles amenazas. La importancia de la protección de Estructuras Estratégicas tiene como objetivo garantizar el funcionamiento continuo de los sistemas, bienes, servicios e instalaciones esenciales. En general, pueden clasificarse como aquellas cuya violación o interdicción, destrucción o interrupción del funcionamiento tendría un impacto social, económico, político o ambiental grave, afectando así la seguridad del Estado y la sociedad.

El autor del presente estudio, identificó además que existen vacíos en los procedimientos que se deben tener en cuenta para que las tropas puedan tener el mejor desempeño posible, con el mínimo de efectos secundarios tanto para la población como para las propias tropas, en cumplimiento de los principios establecidos por las normas legales. Conceptualizando lo anterior, el presente estudio se estructura de la siguiente manera:

Primer Capítulo: Presenta la Información General, donde se indica la Dependencia, el Tipo de actividad, lugar, fecha y la Misión y Visión.

Segundo Capítulo: Presenta el Marco Teórico, donde describe los antecedentes nacionales e internacionales, además de la Descripción Teórica y la definición de los términos.

Tercer Capítulo: Presenta el Desarrollo del Tema, donde se describe el Campo y Tipo de Aplicación, el Diagnóstico sobre la problemática actual. Por último, en este capítulo se presenta una Propuesta de Innovación, que busca dar solución al problema observado.

CAPITULO I
INFORMACIÓN GENERAL

1.1. Dependencia (donde se desarrolla el tema)

La dependencia clave para el desarrollo de la Suficiencia Profesional fue el Batallón de Infantería Motorizado Nº 11, acantonada en la Primera Brigada de Infantería, perteneciente a la Primera División del Ejército del Perú.

1.2. Tipo de Actividad (Función y Puesto)

El autor ocupó el cargo Jefe de Patrulla. Con la función de operar misiones militares para la seguridad y control interno del área de responsabilidad a través de diferentes actividades que busquen los intereses comunes de los ciudadanos.

1.3. Lugar y Fecha

El Batallón de Infantería Motorizado N.º 11, se encuentra ubicado en el distrito de Papayal, constituido en la provincia de Zarumilla, departamento de Tumbes, Perú. El autor desempeñó sus funciones el año 2017.

1.4. Visión del BIM N.º 11

Constituir una Brigada de Infantería representante del reconocimiento y respeto de los valores de disciplina, honestidad, respeto y lealtad, cumpliendo con las responsabilidades y principios de la Constitución del Perú, contribuyendo a la construcción de la paz social".

1.5. Misión del BIM N.º 11

La misión del BIM N.º 11, es "defender, velar por la integridad y seguridad de los ciudadanos".

1.6. Actividades del Puesto que Ocupó

Como Jefe de patrulla, el autor ejecutó las funciones de inspeccionar los batallones destinados a operaciones militares para detener las acciones criminales y sus diferentes métodos delincuenciales. Otra función muy importante es la de apoyar a las personas afectadas por estas acciones sediciosas. Por tanto, el mando y control debe estar relacionado con tareas concernientes al plan estratégico establecido.

Por otra parte, el Batallón de Infantería Motorizado N.º 11, cumple con las actividades de efectuar diferentes acciones en la operación estratégica de control interno para brindar seguridad y orden. Delegar actividades de manera objetiva para reducir las actividades del crimen organizado y sus ataques en la localidad, y permitir que los soldados integrantes del Batallón participen activamente en el apoyo a las comunidades que requieren apoyo ciudadano, y monitorear constantemente la seguridad para garantizar el bienestar de sus generales.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Antecedentes Internacionales

Horzella (2019). En su publicación: “Protección de Infraestructura Crítica y Fuerzas Armadas”. En este informe, se ha realizado una revisión conceptual limitada del término Infraestructura Crítica “IC” en las regulaciones internacionales, extranjeras y las profesionales. Asimismo, brevemente se describieron los riesgos y amenazas que se ciernen sobre la infraestructura mencionada, dando paso a la revisión de tres casos, a saber: Ecuador, España y Uruguay, evaluando su modelo de protección de la IC, identificando los roles y sus respectivas Fuerzas Armadas. La infraestructura, ya sea crítica o estratégica, enfrenta una serie de riesgos y amenazas -naturales o artificiales- de tal modo, los países necesitan establecer acuerdos y mecanismos de protección para asignar roles y responsabilidades a las agencias relevantes para proteger a las IC, sean Públicos y/o privados. En cuanto a la protección física de dicha infraestructura por parte de las Fuerzas Armadas, en España esta se limita a la infraestructura del sector de defensa; mientras que en Ecuador y Uruguay la ley autoriza a las Fuerzas Armadas a proteger a los recursos o sectores estratégicos. En conclusión, en términos de acotar la participación de dichas fuerzas a tareas más específicas, requiriendo en el caso de Ecuador de una definición de IC más restringida, que acote a su vez las zonas de despliegue; o como se desprende del caso uruguayo, de una nueva categorización de las situaciones en las cuales estas deben ser utilizadas.

Junta Interamericana de Defensa (2018). En su publicación: “Estudio sobre protección de infraestructura crítica en caso de desastre natural”, manifestaron que, en un entorno cada vez más interdependiente y complejo, la infraestructura proporciona bienes y servicios que se consideran esenciales para las personas. Con el avance de la cuarta revolución industrial, el concepto de infraestructura ha trascendido los activos físicos, y ahora ha agregado sistemas, procesos y organizaciones, así como una infraestructura fundamental para el funcionamiento

de la sociedad. Definir qué servicios se consideran críticos para un país y su población indicará qué infraestructura se considera crítica. Por lo tanto, la interrupción de estos servicios básicos, a través de desastres que afecten traerá graves consecuencias para las personas y los países, y se considera uno de los riesgos globales de hoy. En este contexto, este trabajo analiza el uso de las fuerzas armadas para proteger la infraestructura crítica relacionada con los desastres naturales. En conclusión, conforme a los requisitos específicos, el uso de las fuerzas armadas para proteger la infraestructura crítica en caso de desastres naturales debe verse como una herramienta que complementa los mecanismos de asistencia existentes. La principal medida para proteger la infraestructura crítica en caso de desastre es establecer o mejorar la resistencia a desastres de la infraestructura.

Solís (2019). En su artículo: “La protección de las infraestructuras críticas en la era digital en el contexto de Costa Rica”, indicando que la era digital trae un progreso exponencial en el bienestar humano, pero a su vez también ha traído riesgos y vulnerabilidades en diferentes áreas de la vida (pública y privada). En esta investigación se propone el concepto de infraestructura crítica, basándose en el estudio de las doctrinas que forman parte de la normativa regional para resolver la necesaria relevancia jurídica de este problema, destacando la experiencia de Argentina y Panamá. El concepto de "infraestructura crítica" incluye aquellos elementos materiales y humanos que hacen posible la vida comunitaria al actuar como base de comunicación entre las personas, el comercio, el transporte de valores, la electricidad y los suministros energéticos del petróleo; además, también clasifican ciudades, almacenan información en bases de datos, etc. Actualmente, un eje básico de la infraestructura crítica es Internet. En este sentido, hay retos pendientes que no se pueden postergar: la formación técnica en ética requiere más recursos, las empresas privadas necesitan más participación, compartir experiencia y formación con el sector público; siendo necesario prevenir y sancionar las violaciones de fundamentos clave. Cabe destacar que es de suma importancia la creación de una agencia de seguridad e inteligencia dedicada a supervisar la infraestructura crítica de Costa Rica.

Berdugo (2016). En su investigación: “Importancia de definir la infraestructura critica en Colombia”, cuyo propósito de este trabajo fue demostrar la importancia de una clara legislación colombiana que define la infraestructura crítica, permitiendo el establecimiento de mecanismos de control centralizados y responsabilidades de seguridad, mantenimiento y protección. Una vez que el legislador haya formulado una política, se le dará la seriedad que necesita no solo para poder identificarla, sino también para protegerla de los riesgos comunes y / o externos que puedan derivarse del ir y venir de las actividades estatales. Es importante recordar que el concepto de infraestructura crítica está incluido en todas las instalaciones, redes, servicios y equipos físicos y tecnología de la información, el manejo o destrucción de estos equipos puede tener un impacto en temas de salud, seguridad o económicos en el funcionamiento efectivo de la ciudadanía o del estado y la administración pública, en este sentido, la infraestructura critica puede representar una amenaza para el país en diferentes temas: la ciberguerra, el cibercrimen, el ciberespionaje, y ciberterrorismo ya que permitiría que terroristas cibernéticos se infiltraran en las redes de cualquier país para ejercer sus ataques delictivos poniendo en riesgo la tranquilidad de Colombia.

Miranzo y Del Río (2014). En su investigación, “La protección de infraestructuras críticas”, en el cual describieron cómo el ataque de septiembre de 2001 al World Trade Center puso de relieve las nuevas amenazas y vulnerabilidades que los países deben afrontar al considerar la seguridad de la infraestructura crítica. Dichos ataques pueden causar la pérdida de vidas humanas y económicas y afectar la credibilidad política del gobierno. Además de la creciente demanda de recursos limitados y en declive, así como los antecedentes del cambio climático y el ajuste del equilibrio de poder internacional, esta situación hace que las estrategias de seguridad nacional de muchos países, incluida España, presten más atención a la seguridad de la infraestructura crítica. Sin embargo, aunque las estrategias de seguridad nacional de 2009 y 2013 alinearon a España con las directivas europeas en este sentido, no se ha visto el desarrollo de problemas más allá de la línea general de actuación.

Páez (2020). En su investigación: “Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la política nacional de ciberseguridad del Ecuador”. El propósito de este estudio estuvo basado en describir una serie de pautas para ayudar a determinar la infraestructura crítica estratégica de un país. En vista de que Ecuador ha sufrido múltiples ataques a nivel de seguridad de la información. El caso más reciente fue un ataque a una plataforma de red con dominios.gov.ec y .ec. La seguridad de la información y las comunicaciones se ha convertido en una parte importante de la vida de las personas, los países y sus actividades. Como parte de la protección y seguridad de la información, el gobierno ecuatoriano ha aprobado un decreto para establecer una entidad para supervisar todas las infraestructuras que se consideran esenciales para el normal desarrollo de las actividades financieras, civiles, militares y otras. La identificación de infraestructura crítica se ha convertido en una parte importante e indispensable de la formulación e implementación de políticas nacionales de ciberseguridad. Fue recomendable considerar diferentes métodos utilizados para identificar infraestructura como ENISA y NIST.

El análisis realizado por el autor de la investigación descrita, permitió encontrar las diferencias entre los procedimientos realizados a nivel mundial para la selección de servicios e infraestructuras criticas tomando en cuenta la realidad situacional del estado o país que lo quiera aplicar. Existe una organización, en el Ecuador, encargada del desarrollo de un catálogo de infraestructuras críticas. Sin embargo, hasta el momento no se ha encontrado un modelo similar a los desarrollados en otros países, que cumpla con las características para su efectividad. El proceso metodológico utilizado para este trabajo, permitió encontrar y clasificar las metodologías que han sido analizadas de acuerdo a las características planteadas, el proceso de selección y clasificación de las mismas fue evaluado, cuyos resultados fueron de gran ayuda para los resultados de esta investigación.

2.1.2 Antecedentes Nacionales

En vista de que la suficiencia profesional plantea un tema de investigación novedoso, no fue posible encontrar fuentes a nivel nacional de acuerdo con la temática del estudio.

2.2 Descripción teórica

2.2.1. Concepto de Infraestructura crítica

La comprensión de la infraestructura crítica (en lo sucesivo denominada IC) tiene amplias definiciones en las normativas internacionales y en las bibliografías profesionales. Por ejemplo, la Comisión Europea propuso el siguiente enfoque para este concepto en 2004:

> Este es el nombre de aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información, cuya interrupción o destrucción tendría un mayor impacto en la salud, seguridad o bienestar económico de los ciudadanos o en el funcionamiento efectivo de los gobiernos miembros. La infraestructura crítica abarca muchos sectores de la economía, incluidos la banca y las finanzas, el transporte y la distribución, la energía, los servicios públicos, la atención médica, el suministro de alimentos y las comunicaciones, y los servicios gubernamentales clave. Estrictamente hablando, algunos de los elementos clave en estos sectores no constituyen "infraestructura", sino redes o cadenas de suministro que apoyan la entrega de productos o servicios básicos. Por ejemplo, el suministro de alimentos o agua en nuestras principales áreas urbanas depende de algunas instalaciones clave, pero también depende de una compleja red de productores, procesadores, fabricantes, distribuidores y minoristas. (Comisión Europea, 2004).

En definiciones posteriores, el Consejo Europeo afirmó en su Directiva 2008/114 / CE que Infraestructura Crítica se entenderá como:

> Elementos, sistemas o partes de ellos ubicados en los Estados miembros son vitales para el mantenimiento de importantes funciones sociales, la salud, la integridad física, la seguridad y el bienestar social y económico de la población. Su destrucción o destrucción afectará gravemente a los estados miembros. incapacidad para mantener estas funciones (Consejo Europeo, 2008).

Por su parte, el gobierno de Estados Unidos fue pionero en este campo, y expuso su posición al respecto a mediados de la década de los noventa:

> La infraestructura de ciertos países es muy importante. Si se inhabilita o se destruye, tendrá un impacto debilitante en la defensa nacional o la seguridad económica de los Estados Unidos. Esta infraestructura crítica incluye telecomunicaciones, sistemas de energía, almacenamiento y transporte de gas natural y combustible, banca y finanzas, transporte, sistemas de suministro de agua, servicios de emergencia (incluidos los servicios médicos, policiales, de bomberos y de rescate) y la continuidad del gobierno. Dado que la mayor parte de la infraestructura crítica pertenece y es operada por el sector privado, el gobierno y el sector privado deben desarrollar estrategias conjuntas para protegerla y asegurar su operación continua (Clinton, 1996).

Por el contrario, la estrategia del Reino Unido proporciona un análisis detallado y una priorización de los riesgos y amenazas que enfrenta cada sector de las actividades de infraestructura crítica mediante el desarrollo de sus propios métodos de prevención de riesgos. El papel de la seguridad de la red también es una prioridad de la estrategia, y la conclusión es que la mejora del binomio tecnología-capital humano será de importancia decisiva para garantizar la seguridad nacional (Moteff, 2015).

2.2.3. Estructuras Estratégicas

Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información que ejecutan los servicios básicos. Como ejemplo de estructuras, podemos mencionar plantas hidroeléctricas, aeropuertos, ferrocarriles, líneas de transmisión eléctrica, puertos, entre otros, que deben ser blancos de extrema cautela por parte del Estado Nacional (Moreira, 2019).

Estas estructuras son conocidas como Estructuras Estratégicas, por su importancia en el escenario nacional, cuya interrupción del servicio puede ocasionar serios daños al Estado y a la Sociedad, incluso imposibilitando la realización de un gran evento, reduciendo el país anfitrión. Credibilidad (Moreira, 2019).

Los principales actos que pueden suponer riesgos para estas estructuras son los atentados terroristas, provocados por grupos extremistas que pretenden provocar el pánico en la población, con el fin de imponer su ideología o religión, como podemos describir a continuación:

> La protección de Estructuras Estratégicas tiene como objetivo garantizar el funcionamiento continuo de los sistemas, bienes, servicios e instalaciones esenciales. En general, las Estructuras Estratégicas pueden clasificarse como aquellas cuya violación o interdicción, destrucción o interrupción del funcionamiento tendría un impacto social, económico, político o ambiental grave, afectando así la seguridad del Estado y la sociedad (Moreira, 2019).

2.2.3. Diferencia entre infraestructura crítica y estratégica

La discusión teórica presentada en el presente trabajo no se limita a la infraestructura crítica, también existe un concepto estrechamente relacionado que contiene matices de sus características, el de infraestructura estratégica. Por ello para ayudar a conceptualizarlo mejor, Henry Mintzberg (1993, citado por Moreira, 2019) señaló:

> La infraestructura estratégica está relacionada con la sostenibilidad o existencia de una organización; desde la perspectiva de la estrategia nacional, si la infraestructura está relacionada con la operación normal de restablecimiento de los servicios básicos, será considerada como "infraestructura estratégica", pero si estos se relacionan con servicios básicos, una vez que se producen interferencias o daños, no hay alternativa, se habla de "infraestructura crítica".

Infraestructura estratégica: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información de los que dependen las operaciones de servicios básicos (Moreira, 2019).

Infraestructura crítica: Infraestructura estratégica, donde su desempeño es fundamental para la operación y no permite soluciones alternativas, por lo que su interferencia o daño tendrá un impacto grave en los servicios básicos (Moreira, 2019).

La infraestructura, ya sea crítica o estratégica, enfrenta muchos riesgos y amenazas. Según Moteff (2015), la interrupción operativa de la infraestructura crítica puede ser causada por múltiples factores: mal diseño, error del operador, daño físico causado por desastres naturales (terremotos, tormentas eléctricas, etc.), daño físico deliberado o acciones humanas (robo, incendio premeditado, atentados terroristas, etc.). De manera similar, el Forld Economic Forum en el año 2018, clasificó estas amenazas de la siguiente manera:

Figura 1

Tipos de Amenazas que enfrenta la IC.

EVE NTOS NATURALES	**ACCIÓN HUMANA**	
	FALLA TÉCNICA ERROR HU-MANO	TERRORISMO, CRÍMEN, GUERRA
Peligros Hidrometereológicos	Fallas de sistema	Terrorismo
Peligros Geológicos	Negligencia	Sabotaje
Epidemias y Pandemias	Accidente o Emergencias	Otras formas de crimen
Eventos Cósmicos	Fallas en la Institución	Guerras/Conflictos

Fuente: World Economic Forum (2018 citado por Recalde y Racines, 2018).

Una vez identificada la amenaza, es necesario tomar medidas para proteger esta infraestructura y poder responder rápidamente ante cualquier situación que pueda ocurrir. Cada una de estas infraestructuras tiene sus propias vulnerabilidades. Por tanto, es necesario determinar el nivel de riesgo asociado a cada una de estas amenazas, para luego determinar y priorizar una serie de medidas que se pueden tomar para minimizar estos riesgos (Moteff, 2015).

Por lo tanto, los países necesitan establecer acuerdos y mecanismos de protección para asignar roles y responsabilidades a las instituciones (públicas y privadas) relacionadas con la protección de la IC para reducir las vulnerabilidades antes mencionadas.

2.2.4. Perspectivas de las infraestructuras críticas en otros países

En los últimos años, varios países han prestado cada vez más atención a garantizar la seguridad y reducir la vulnerabilidad de importantes infraestructuras nacionales frente a amenazas y riesgos de diversa índole.

Las últimas estrategias de seguridad nacional aprobadas por Finlandia, Japón, Reino Unido, Estados Unidos, Australia y Francia lo demuestran.

Finlandia: La estrategia de seguridad de Finlandia se centra en proteger la infraestructura crítica de manera integral, enfatizando la importancia de mantener un enfoque de seguridad general. En particular, enfatiza la seguridad de la cadena de suministro y la promoción de mecanismos elásticos para mantener las importantes funciones básicas del país. Además, considerando los nuevos desafíos que plantea la crisis económica y el mayor grado de interdependencia en una sociedad globalizada, incluida la posibilidad de trasladar la infraestructura necesaria a otros países (Miranzo y Del Río, 2014).

Japón: La estrategia de seguridad de Japón se centra principalmente en prevenir los ciberataques a la infraestructura de sus intereses nacionales como una amenaza importante. Específicamente menciona la posibilidad de que el país sea responsable de estas acciones, y busca como fin último, mejorar la base intelectual del país para mejorar las capacidades técnicas, especialmente las de comunicación, que son el motor del poder económico y económico. Seguridad en Japón (Miranzo y Del Río, 2014).

Francia: Un enfoque similar aclara el Libro Blanco de Defensa francés, que se centra en los esfuerzos para proteger el potencial científico y tecnológico del país como una forma prioritaria de prevenir ataques a su infraestructura. La estrategia enumera 12 Departamentos de actividad que se consideran esenciales para la continuidad de las funciones básicas del país, con un enfoque en el combate a los ciberataques, especialmente los ciberataques a los sistemas de información nacionales. Para garantizar su seguridad, Francia cree que debe mantener su capacidad de producir dispositivos de seguridad autónomos para detectar ataques y mejorar sus capacidades en las comunicaciones electrónicas, especialmente en la fabricación de dispositivos y componentes (Miranzo y Del Río, 2014).

En cuanto a las estrategias de seguridad del mundo anglosajón (Australia, Reino Unido y Estados Unidos), existen diferencias significativas (Miranzo y Del Río, 2014).

Australia: La estrategia de Australia es la más dura en este tema, y se centra en la importancia de fortalecer la capacidad de recuperación de la población, los activos, la infraestructura y las instituciones, para lo cual establecieron un foro de debate con expertos en la materia (Miranzo y Del Río, 2014).

Estados Unidos: El enfoque estadounidense se enfoca en reducir la vulnerabilidad de ataques y ciberataques en áreas específicas que se consideran prioritarias: redes de transporte, redes eléctricas y la economía, estas últimas consideradas particularmente vulnerables a los ciberataques, haciendo del ciberespacio un área clave de acción nacional (Miranzo y Del Río, 2014).

Reino Unido: Por el contrario, la estrategia del Reino Unido proporciona un análisis detallado y una priorización de los riesgos y amenazas que enfrenta cada sector de las actividades de infraestructura crítica mediante el desarrollo de sus propios métodos de prevención de riesgos. El papel de la seguridad de la red también es una prioridad de la estrategia, y la conclusión es que la mejora del binomio tecnología-capital humano será de importancia decisiva para garantizar la seguridad nacional (Miranzo y Del Río, 2014).

3.2.5. Infraestructura Crítica: ¿Defensa o Seguridad Pública?

Ante la interrogante, ¿quién es el responsable de proteger la Infraestructura Crítica (IC)? La experiencia comparativa no está clara. En este sentido, y con base en la diferencia antes mencionada entre infraestructura crítica e infraestructura estratégica, Mario Moreira elaboró la clasificación basada en propósitos y métodos de protección:

Figura 2.

Clasificación de los propósitos y métodos de protección

Tipo de Infraestructura	Finalidad de la Protección	Medios a emplearse
Estratégica	Asegurar la sustentabilidad del Estado, en cuanto a brindar a la población la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.	Seguridad Pública Cuando se comienza a afectar las condiciones de bienestar social presente y futuro de la población, pasa a ser un problema de Defensa Nacional.
Crítica	Aquella que afecta la existencia del Estado como tal; o que ante daño o deterioro no exista alternativa	Defensa Nacional
Relacionada con los recursos estratégicos (Agua, alimenticios, minerales, energéticos y biodiversidad)	Proteger el recurso como tal, la infraestructura de explotación, traslado, industrialización y distribución.	Defensa Nacional

Fuente: Moreira (2019).

El modelo descrito anteriormente proporciona un papel de liderazgo para el Departamento de Defensa. Sin embargo, la revisión del caso muestra que el paradigma de la protección de la IC es diferente al rol mayor de la seguridad pública, como es el caso español; el rol principal de la defensa en el caso de Uruguay; el caso de Ecuador se encuentra en algún punto intermedio, y la responsabilidad en este sentido compartida por las dos carteras de inversión (Moreira, 2019).

Específicamente, en lo que respecta a la protección física de CI por parte de las Fuerzas Armadas, podemos señalar que en el caso español esta se limita a la infraestructura de los sectores de defensa y aeroespacial; mientras que en Ecuador y Uruguay la ley autoriza a las Fuerzas Armadas. para proteger el llamado recurso o Toda la infraestructura relacionada con el sector estratégico (Moreira, 2019).

2.3. Definición de términos

OPTIMIZACIÓN

Es la “acción de desarrollar una actividad lo más eficientemente posible, es decir, con la menor cantidad de recursos y en el menor tiempo posible” (Westreicher, 2020).

BATALLÓN DE INFANTERÍA

“El batallón suele ser parte de un regimiento, grupo o brigada, dependiendo del modelo organizativo usado por ese servicio. Los batallones son ordinariamente homogéneos con respecto al tipo” (Berdugo, 2016).

PLANEAMIENTO

Es el “proceso metódico que se diseña con la misión de lograr un objetivo” (Ucha, 2014).

PROTECCIÓN

La protección es “un cuidado preventivo ante un eventual riesgo o problema” (Pérez y Merino, 2010).

INFRAESTRUCTURAS CRÍTICAS

Su desempeño es “fundamental para la operación y no permite soluciones alternativas, por lo que su interferencia o daño tendrá un impacto grave en los servicios básicos” (Moreira, 2019).

INFRAESTRUCTURAS ESTRATÉGICAS

Son “instalaciones, sistemas, equipos físicos y tecnología de la información de los que dependen las operaciones de servicios básicos” (Moreira, 2019).

AMENAZA

Se refiere al “dicho o hecho que anticipa un daño” (Pérez y Gardey, 2010).

SEGURIDAD

“Certeza, donde no se registran peligros, daños ni riesgos” (Ucha, 2014).

CAPÍTULO III
DESARROLLO DEL TEMA

3.1. Campos de Aplicación

El área de investigación es el Batallón de Infantería Motorizado Nº 11, acantonada en la Primera Brigada de Infantería, perteneciente a la Primera División del Ejército del Perú. Las líneas de investigación son: Método de Instrucción Militar, Rol de las misiones individuales del combatiente. Capacitación y Constructivismo.

3.2. Tipos de aplicación

El surgimiento de la Era del Conocimiento, el surgimiento del Perú como nación de gran importancia en el escenario internacional y la notable imprevisibilidad de los conflictos en el siglo XXI, caracterizados por diferentes tipos de amenazas, catalizaron la percepción de la necesidad de transformación del Ejército Perú (EP). Esta necesidad tiene como objetivo brindar al país el apoyo necesario para enfrentar los nuevos desafíos de hoy, entre ellos el resguardo de nuestras infraestructuras críticas.

El proceso de crecimiento económico, reconocimiento y proyección internacional que asume el país, requiere una ampliación de la capacidad operativa del Ejército del Perú. Para ello, la Fuerza Terrestre debe ser capaz, volviéndose más eficiente en la misión de preservar sus estructuras estratégicas y en condiciones para ser utilizada para enfrentar posibles amenazas. En ese sentido se plantea el tema y sea aplicado al nivel operativo.

La protección de Estructuras Estratégicas tiene como objetivo garantizar el funcionamiento continuo de los sistemas, bienes, servicios e instalaciones esenciales. En general, las Estructuras Estratégicas pueden clasificarse como aquellas cuya violación o interdicción, destrucción o interrupción del funcionamiento tendría un impacto social, económico, político o ambiental grave, afectando así la seguridad del Estado y la sociedad.

Los principales actos que pueden suponer riesgos para estas estructuras son los atentados terroristas, provocados por grupos extremistas que pretenden provocar el pánico en la población, con el fin de imponer su ideología o religión, como podemos ver a continuación.

El Ejército del Perú ha sido empleado en diversas operaciones de seguridad de estructuras estratégicas, especialmente enmarcadas en grandes eventos. Estos lugares abordan a un gran número de personas, siendo su protección de suma importancia. Un aspecto relevante de estas operaciones, que buscan mantener el orden durante la ejecución de eventos de gran escala, es el trato con el público externo. De esta forma, la preparación constante y preventiva por parte de la Fuerza es sumamente necesaria, de manera que se eviten daños colaterales a la población.

El autor del presente estudio, además identificó que existen vacíos en los procedimientos que se deben tener en cuenta para que las tropas puedan tener el mejor desempeño posible, con el mínimo de efectos secundarios tanto para la población como para las propias tropas, en cumplimiento de los principios establecidos por las normas legales.

Con base en la cita anterior, se puede verificar la relevancia del tema en cuestión, en el que se comprueba la necesidad de preservar la integridad de estas infraestructuras, que pueden influir directamente en el Estado y la Sociedad.

3.3. Diagnóstico

La evolución de los medios tecnológicos y la creciente globalización han ido transformando la forma en que interactúa toda la sociedad mundial. La facilidad de acceso a los medios de comunicación y transporte, países cada vez más interconectados, ha provocado una mayor unión entre los pueblos. Sin embargo, también han provocado puntos negativos, principalmente relacionados con el aspecto de seguridad.

Con la intensa migración de tropas de países a otros, por una variedad de razones, es esencial tener un mayor control sobre las estructuras más grandes. Son las centrales eléctricas, puertos, aeropuertos, ferrocarriles, entre otros, que son de vital importancia en el escenario nacional, por lo que se denominan Estructuras Estratégicas. Para cumplir con su rol institucional, junto con las Agencias de Seguridad Pública, el Ejército del Perú busca acompañar la evolución del combate que imponen los escenarios modernos, preparándose adecuadamente para enfrentar cualquier situación, en caso de empleo real.

El Ejército del Perú ha sido empleado varias veces para asegurar la ejecución de grandes eventos, en paralelo con el mantenimiento de la integridad de las estructuras estratégicas, especialmente en los grandes centros urbanos. Sin embargo, la demanda para la ejecución de estas actividades, especialmente en lo que respecta a la contratación de personal, es muy elevada, superando casi siempre la capacidad de empleo de las fracciones ocupadas. Además, existe cierta dificultad para llevar a cabo la planificación, ya que aún no existe un conjunto de técnicas, tácticas y procedimientos que permitan el establecimiento del dispositivo de seguridad en estos lugares.

Así, con el fin de verificar cuál es la mejor manera de asegurar la integridad de las estructuras estratégicas, especialmente durante la ejecución de grandes eventos, se formuló el siguiente problema: ¿Cómo optimizar la ejecución y planificación de seguridad de estructuras estratégicas, particularmente enmarcadas en grandes eventos?

3.4 Propuesta de innovación

Los resultados descubiertos en este estudio mediante la revisión de la bibliografía permitieron comprender de manera adecuada el tema planteado. El estudio sobre infraestructura mencionada aquí, ya sea crítica o estratégica, enfrenta una serie de riesgos y amenazas naturales o artificiales. Por ello se necesita establecer acuerdos y mecanismos de protección para asignar roles y responsabilidades a los órganos relevantes para proteger las infraestructuras críticas Pública y privada y reducir estas lagunas.

Se propone la creación de un Departamento de Protección de Infraestructuras, ofreciendo una amplia variedad de Programas de Capacitación. En este sentido se sugiere además la optimización de la planificación y empleo en la protección de infraestructuras estratégicas por parte de un Batallón de Infantería, sirviendo como presupuesto teórico para una mejora en la ejecución práctica de la referida actividad.

3.4.1. Descripción de la propuesta

La propuesta planteada no pretende reunir procedimientos, sino más bien ser una guía que puede dar al comandante la dirección de su planificación y, en consecuencia, una buena ejecución por parte de la tropa.

El punto básico y necesario del nuevo enfoque del Perú sobre la protección de infraestructuras críticas debe ser corregir las brechas más importantes frente al enfoque actual, como una definición clara del tema, que incluya no solo la necesidad de protección, sino también los riesgos y amenazas a las que se enfrenta, así como los riesgos y amenazas previsibles en un futuro próximo, y un marco claro para el establecimiento de metas prioritarias. La seguridad y resiliencia de la infraestructura crítica son vitales no solo para la confianza pública, sino también para la seguridad, prosperidad y bienestar de la nación.

Dado el contexto anterior, la importancia para la presentación de la propuesta planteada, donde se impulsen programas de capacitación para este propósito. La creación de un Departamento de Protección de Infraestructuras debe ofrecer una amplia variedad de programas de capacitación gratuitos para socios gubernamentales y del sector privado. Estos cursos de estudio independiente basados en la web, cursos dirigidos por instructores y materiales de capacitación asociados brindan a los funcionarios gubernamentales y a los propietarios y operadores de infraestructura crítica el conocimiento y las habilidades necesarias para implementar actividades de resiliencia y seguridad de la infraestructura crítica.

En este sentido, la propuesta de innovación promueve una reflexión sobre un tema sumamente importante y fundamental para el éxito de las probables acciones futuras de la Fuerza Terrestre. Por ello es importante establecer Estrategias de Seguridad Nacional, líneas de actuación estratégicas con el propósito de fortalecer la seguridad de las infraestructuras críticas:

- Responsabilidades compartidas y cooperación público-privada
- Planeamiento escalonado
- Equilibrio y eficiencia
- Resiliencia
- Coordinación
- Cooperación internacional.

3.4.2. Desarrollo de la propuesta

Tabla 1.
Preparación y uso en protección de estructuras estratégicas y seguridad en grandes eventos

PREPARACIÓN Y USO EN PROTECCIÓN DE ESTRUCTURAS ESTRATÉGICAS Y SEGURIDAD EN GRANDES EVENTOS
1. Misión Preliminar 1. <u>Recibimiento de la misión.</u> ▪ Despeje de dudas ▪ Cuadro de horario (hasta empleo) ▪ 1/5 para organización ▪ 1/5 para recibir material

- 3/5 instrucciones y agradecimientos
- Orientaciones iniciales para Estado Mayor y Comandante de Sub Unidad
- Composición de las tropas S1 / S3
- S3 / S4 (preliminar) necesidad de materiales
- Orden de preparación de S3
- S2 Medidas iniciales de Inteligencia y Contrainteligencia

2. Estado Misión

- Misión
- Intención de Comandante
- Estado final deseado
- Reconocimiento inicial

2. Planeamiento

- Nueva declaración
- Cronograma de trabajo
- Planeamiento detallado del Estado Mayor y Comandante de Sub Unidad
- Necesidad de apoyo educativo
- Necesidad de apoyo logístico

3. Sitio de Logística

- Necesidades / Verificación
- Equipamiento Independiente

- Armamento y munición letal
- Armamento y munición menos letales
- Vehículos
- Equipo específico / esencial: Rayos X, Scanner, ropa de civil, detectores radiológicos
- Estimación logística
- Finalización de clases

4. Instrucciones

a) Instrucciones preparatorias

- Conciencia situacional
- Ambiente operacional
- Acciones a realizar
- Condiciones de ejecución

b) Instrucciones en las fuerzas especializadas Organizaciones Militares y Órganos de Seguridad Pública.

- Garantizar la Ley y el Orden
- Módulos de tiro letal y menos letal
- Reglas legales y de compromiso
- Realizar acciones antiterroristas y contra grandes adversidades
- Técnicas, Taticas e Procedimientos

- Tareas esenciales y específicas: revisión del personal, trato con extranjeros, operar un detector de rayos X y radiación, control de equipos de obra civil

c) Simulación de trabajo

5. Empleo

a) Reconocimiento final

b) Reglas de participación

c) Técnicas, Taticas y Procedimientos

Nota: Elaboración propia, 2021.

3.4.3. Objetivo de la propuesta

- El objetivo en general será establecer una mayor cooperación y comunicación entre el sector privado y el gobierno. El sector privado posee y opera gran parte de la infraestructura crítica de la nación. Según lo visto por la Comisión, la función principal del gobierno (además de proteger sus propias infraestructuras) es recopilar y difundir la información más reciente sobre técnicas de intrusión, análisis de amenazas y formas de defenderse de los piratas informáticos.

- Establecer una estrategia de acción para facilitar una mayor cooperación y comunicación entre el sector privado y las agencias gubernamentales apropiadas mediante: el establecimiento de una oficina de formulación de políticas de alto nivel en la Casa Blanca; establecer un consejo que incluya ejecutivos corporativos, funcionarios del gobierno local y estatal y secretarios del gabinete; y establecimiento de cámaras de compensación de información.

- Desarrollar una capacidad de alerta de ataques en tiempo real.

- Establecer y promover un programa integral de sensibilización y educación.

- Simplificar y aclarar los elementos de la estructura legal para respaldar las medidas de garantía (incluida la eliminación de las barreras jurisdiccionales para perseguir a los piratas informáticos por medios electrónicos).

- Ampliar la investigación y el desarrollo de tecnologías y técnicas, especialmente tecnologías que permitan una mayor detección de intrusiones.

- Capacitación conjunta con las Agencias de Seguridad Pública y unidades especializadas dentro del Ejército del Perú, para un mejor entrenamiento de las tropas.

CONCLUSIONES

En cuanto a las preguntas de estudio y objetivos propuestos al inicio de este trabajo, se concluye que la presente investigación cumplió con el propósito pretendido, ampliar el entendimiento de la planificación y empleo de un Batallón de Infantería en una operación de Protección de Estructuras Estratégicas. La revisión de la literatura permitió concluir que existe la necesidad de una mejor adecuación de los Batallones de Infantería en cuanto a su desempeño en la seguridad de las estructuras estratégicas. Esta necesidad se manifiesta en elementos específicos y fáciles de realizar, que deben ser observados por los planificadores, para que las tropas puedan actuar de la mejor manera posible.

La Infraestructura estratégica son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información de los que dependen las operaciones de servicios básicos. Infraestructura crítica: Infraestructura estratégica, donde su desempeño es fundamental para la operación y no permite soluciones alternativas, por lo que su interferencia o daño tendrá un impacto grave en los servicios básicos. Ante la duda de ¿quién es el responsable de su protección, la seguridad pública o la defensa nacional? La experiencia comparativa no es clara.

De acuerdo a la experiencia del autor se permitió identificar que existen vacíos en los procedimientos que se deben tener en cuenta para que las tropas puedan tener el mejor desempeño posible, con el mínimo de efectos secundarios tanto para la población como para las propias tropas, en cumplimiento de los principios establecidos por las normas legales.

Así, para contribuir a la planificación y ejecución de este tipo de operaciones, se propone la creación de un Departamento de Protección de Infraestructuras, ofreciendo una amplia variedad de Programas de Capacitación. En este sentido sugiere además la optimización de la planificación y empleo en la protección de estructuras estratégicas por parte de un Batallón de Infantería, sirviendo como presupuesto teórico para una mejora en la ejecución práctica de la referida actividad.

RECOMENDACIONES

1 Debido a la presentación del tema propuesta se pudo evidenciar su importancia, por ello se recomienda al Gobierno adoptar el tema de infraestructura crítica en la legislación, al ser una ley, se convertirá inmediatamente en norma de obligado cumplimiento, si se viola la norma habrá que tomar medidas judiciales.

2 Se recomienda revisar la experiencia internacional sobre el tema de infraestructura crítica que lo describe como una amenaza para el país en diferentes ámbitos. La finalidad debe ser adoptar los modelos ejecutados con éxito.

3 Se recomienda ejecutar un análisis estratégico por sectores y formular un modelo nacional de elección de infraestructura crítica para reflejar la protección y gestión de la información del servicio.

4 Se recomienda realizar un análisis exhaustivo del estado actual de seguridad de la información y ciberdefensa del Perú para gestionar los procesos que pueden incluirse en el modelo de selección de infraestructura crítica.

5 Se recomienda implementar el modelo de selección de infraestructura crítica que defina en el futuro, combinando las características propuestas en este estudio, porque han sido analizadas y probadas en el modelo de selección implementado con éxito en otros países con destacado desarrollo en la seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Berdugo, H. (2016). *Importancia de definir la infraestructura critica en Colombia*. Universidad Militar Nueva Granada. https://repository.unimilitar.edu.co/bitstream/handle/10654/14342/BerdugoSierraHelber%20Alirio2016.pdf?sequence=1&isAllowed=y

Clinton, W. (1996). *Executive Order EO 13010 Critical Infrastructure Protection.* Fas.org. https://irp.fas.org/offdocs/eo13010.htm

Comisión Europea (2004). *Critical Infrastructure Protection in the fight against terrorism*. COM (2004). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

Consejo de la Unión Europea (2008). Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. https://www.ccncert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Horzella, B. (2019). *Protección de Infraestructura Crítica y Fuerzas Armadas.* Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28141/1/BCN_Proteccion_IC_Conceptualizacion_y_experiencia_comparada.pdf

Junta Interamericana de Defensa (2018). *Estudio sobre protección de infraestructura crítica en caso de desastre natural.* http://scm.oas.org/pdfs/2018/CP39205SINFORME.pdf

Miranzo, M. y Del Río, C. (2014). La protección de infraestructuras críticas. *UNISCI Discussion Papers,* (35):339-352. Universidad Complutense de Madrid. https://www.redalyc.org/pdf/767/76731410018.pdf

Moreira, M. (2019). La Protección de Infraestructuras Críticas o Estratégicas, ¿Responsabilidad de Seguridad Pública o de Defensa Nacional? Revista Estrategia (6): 41-53. República Oriental del Uruguay. https://issuu.com/calen_uy/docs/revista_estrategia_n_6__2019_

Moteff, D. (2015). *"Critical Infraestrutures: Background, Policy, and Implementation".* Congressional Research Service. https://fas.org/sgp/crs/homesec/RL30153.pdf

Páez, J. (2020). Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la política nacional de ciberseguridad del Ecuador. Carrera de Ingeniería en Sistemas e Informática. Universidad de las Fuerzas Armadas ESPE. http://repositorio.espe.edu.ec/handle/21000/23641

Pérez, J. y Gardey, A. (2010). Definición de riesgo. https://definicion.de/riesgo/

Pérez, J. y Merino, M. (2010). Definición de protección. https://definicion.de/proteccion/

Recalde, F. y Racines, P. (2018). La Protección de las Infraestructuras críticas en el ámbito de las Fuerzas Armadas. *Revista de Ciencias de Seguridad y Defensa IV* (5). http://geo1.espe.edu.ec/wpcontent/uploads//2018/12/5art1.pdf

Solís, J. (2019). La protección de las infraestructuras críticas en la era digital en el contexto de Costa Rica. *Revista de la Facultad de Derecho de México 69*(463). https://www.researchgate.net/publication/334105770_La_proteccion_de_las_infraestructuras_criticas_en_la_era_digital_en_el_contexto_de_Costa_Rica

Ucha, F. (2014). Planeamiento. Definición ABC. https://www.definicionabc.com/general/planeamiento.php

Westreicher, G. (2020). Optimización - Economipedia. Economipedia. https://economipedia.com/definiciones/optimizacion.html

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	BELLIDO GARCÍA PAUL GIANFRANCO
1.02	Grado y Arma / Servicio	TENIENTE / INFANTERÍA
1.03	Situación Militar	ACTIVIDAD
1.04	CIP	124149400
1.05	DNI	45769432
1.06	Celular y/o RPM	
1.07	Correo Electrónico	

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	01 ABRIL DEL 2009
2.02	Fecha_ egreso EMCH	31 DICIEMBRE DEL 2012
2.04	Fecha de alta como Oficial	01 ENERO DEL 2013
2.05	Años_ experiencia de Oficial	8 AÑOS
2.06	Idiomas	ESPAÑOL

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

Nº	Año	Lugar	Unidad / Dependencia	Puesto Desempeñado
3.01	2015	CANAYRE	BCT N°42	JEFE PATRULLA

3.02	2016	SATIPO	BCT N°79	JEFE PATRULLA
3.03	2017	PAPAYAL	BIM N°11	CMDTE SECC
3.04	2018	TUMBES	BING COMB N°1	CMDTE SECC
3.05	2021	CORRALES	BIB N°211	CMDTE SECC

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

Nº	Año	Dependencia y Período	Denominación	Diploma / Certificación
4.01	2021	6 MESES	CURSO BÁSICO	DIPLOMADO
4.02				
4.03				
4.04				
4.05				

5. ESTUDIOS DE NIVEL UNIVERSITARIO

Nº	Año	Universidad y Período	Bachiller - Licenciado
5.01			
5.02			

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

Nº	Año	Universidad y Período	Grado Académico (Maestro – Doctor)
6.01			
6.02			

7. ESTUDIOS DE ESPECIALIZACIÓN

Nº	Año	Dependencia y Período	Diploma o Certificado
7.01			
7.02			

8. ESTUDIOS EN EL EXTRANJERO

N°	Año	País	Institución Educativa	Grado / Título / Diploma / Certificado
8.01				
8.02				

FIRMA _____
POSTFIRMA