Biopoder y arquitectura panóptica digital: una aproximación crítica a la protección de instalaciones militares

Coronel
GUSTAVO ADOLFO NAVARRO CARRASCAL

Artículo para optar al título de:

Magister en Estrategia y Geopolítica

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá, D. C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	CR. GUSTAVO ADOLFO NAVARRO CARRASCAL
Identificación	**:**	18004912
Programa académico	**:**	Maestría en Estrategia y Geopolítica
Tutor metodológico	**:**	Dra. Claudia Garay
Tutor temático	**:**	CR. Aldemar Serrano
Fecha de entrega	**:**	8 de octubre de 2025
Extensión	**:**	13.698 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-No Comercial-Sin Obras Derivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor **autoriza** que este artículo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Biopoder y arquitectura panóptica digital: una aproximación crítica a la protección de instalaciones militares

Biopower and digital panoptic architecture: a critical approach to protection of military installations.

Gustavo Adolfo Navarro Carrascal[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este artículo analiza cómo las nuevas tecnologías contribuyen a la protección de instalaciones militares mediante la articulación de efectos panópticos frente a amenazas híbridas, integrando marcos teóricos de la geopolítica crítica, el biopoder y la guerra cognitiva. Partiendo del concepto foucaultiano de vigilancia y disciplina (Foucault, 1980), se examina cómo el panóptico se transforma en un dispositivo digital capaz de normalizar conductas y generar control en escenarios de alta complejidad estratégica. El biopoder, entendido como gestión de la vida y regulación de poblaciones, encuentra en la tecnología un medio para proyectarse sobre la seguridad de infraestructuras críticas (Valencia & Marín, 2017).

En este marco, se estudian los sistemas de video vigilancia, sensores, inteligencia artificial y plataformas de ciberdefensa que amplían la cobertura y reducen los tiempos de respuesta ante amenazas híbridas, caracterizadas por la fusión de lo militar, lo tecnológico, lo informativo y lo social (Saavedra, 2024). Se plantea que la integración de capacidades para fortalecer la resiliencia operacional.

Asimismo, se evidencia que la protección de instalaciones militares no se limita a la dimensión física, sino que incorpora lo cognitivo y lo simbólico, las tecnologías de control generan un "panóptico mixto", donde la vigilancia algorítmica se combina con actores internos capacitados para la toma de decisiones bajo el ciclo OODA[2], garantizando disuasión, demora y derrota de la amenaza.

Finalmente, se propone una estrategia integral que combina biopoder, control tecnológico y resiliencia, consolidando un marco doctrinal innovador para enfrentar los desafíos contemporáneos de protección de instalaciones militares.

Palabras clave: Biopoder, Panóptico, Panóptico mixto, Conductismo, Protección instalaciones militares.

[1] Coronel de la especialidad de Seguridad y Defensa de bases de la Fuerza Aeroespacial Colombiana. Estudiante de maestría en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.
[2] El ciclo OODA (observación, orientación, decisión, actuar), para John Boyd es un modelo de cómo pensamos y el medio por el cual competimos y colaboramos, el concepto es una metáfora biológica extendida de estímulo y respuesta, pero un modelo orgánico, no mecanicista.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Abstract: This article analyzes how new technologies contribute to the protection of military installations through the articulation of panoptic effects in response to hybrid threats, integrating theoretical frameworks from critical geopolitics, biopower, and cognitive warfare. Drawing on Foucault's concept of surveillance and discipline (Foucault, 1980), it examines how the panopticon is transformed into a digital dispositive capable of normalizing behaviors and exercising control in complex strategic scenarios. Biopower, understood as the management of life and regulation of populations, finds in technology a means to extend itself over the security of critical infrastructures (Valencia & Marín, 2017).

In this context, systems of video surveillance, sensors, artificial intelligence, and cyber-defense platforms are assessed for their ability to expand coverage and reduce response times to hybrid threats, which combine military, technological, informational, and social dimensions (Saavedra, 2024). It is proposed that the integration of capabilities to strengthen operational resilience.

Furthermore, the protection of military installations is shown to extend beyond the physical dimension to incorporate cognitive and symbolic layers. Control technologies generate a "mixed panoptic," in which algorithmic surveillance is combined with trained internal actors making decisions under the OODA loop, ensuring deterrence, delay, and defeat of the threat.

Finally, the article proposes an integrated strategy combining biopower, technological control, and resilience, consolidating an innovative doctrinal framework to address the contemporary Protection of military installations.

Keywords: Biopower, Panoptic, Mixed panoptic, Behaviorism, Protection of military installations.

1. Introducción

La seguridad y defensa en el siglo XXI enfrenta un doble desafío, por un lado, la transformación del sistema internacional a partir de dinámicas de globalización, interdependencia y nuevas tecnologías; por otro, la aparición de amenazas híbridas que desdibujan la frontera entre lo militar, lo político y lo social. En este contexto, la geopolítica crítica ha aportado un marco teórico fundamental para comprender cómo el poder y la seguridad no se reducen a variables materiales, sino que también se constituyen discursivamente a través de representaciones y prácticas espaciales.

Simon Dalby (2002) argumenta que la geopolítica debe analizarse como un discurso que produce territorios y poblaciones como objetivos de intervención, más que como una ciencia neutral de las relaciones internacionales. Esta perspectiva crítica permite replantear la protección de instalaciones militares al entenderlas no solo como activos estratégicos, sino como espacios donde convergen el control territorial, la gestión de poblaciones y la aplicación de tecnologías de vigilancia.

En paralelo, la obra de Barry Buzan (1998) ha sido central para ampliar el concepto de seguridad. Su propuesta de cinco sectores: militar, político, económico, social y ambiental, representa un esfuerzo por superar la visión tradicional centrada en el Estado y la defensa territorial. Para este documento, se retoman de manera particular cuatro de las categorías, militar, política, económico y social, dado que resultan más pertinentes para el análisis de la protección de las instalaciones militares frente a amenazas híbridas.

En el sector militar, las instalaciones son nodos vitales de la soberanía y la capacidad del Estado para ejercer poder; en el sector político, constituyen símbolos de legitimidad institucional cuya vulnerabilidad impacta directamente la percepción de

estabilidad; en el sector económico las instalaciones se configuran como infraestructuras críticas cada vez más dependientes del ciberespacio, de la Inteligencia Artificial (IA) y de sistemas electrónicos de seguridad (SES); y en el sector social, se relacionan con identidades colectivas que las conciben como baluartes de la nación, constituyendo, con el sector político, las bases para ejercer el poder y autoridad dentro de principios lógicos de la buenas relaciones y legitimidad institucional.

La confluencia entre la geopolítica critica de Dalby y los sectores de seguridad de Buzan permite establecer un marco de análisis robusto, según Dalby (2002), la seguridad es producida por narrativas que justifican la militarización de territorios y la vigilancia de poblaciones, naturalizando prácticas de control que en muchas ocasiones refuerzan desigualdades y exclusiones.

Buzan por su parte, muestra que la seguridad se diversifica más allá del ámbito militar, extendiéndose a dimensiones políticas y sociales. Cuando se analizan instalaciones militares bajo estas perspectivas se evidencia que no solo son espacios de defensa física, sino también dispositivos discursivos y materiales que representan, regulan y reproducen formas de poder.

La relevancia de este marco teórico es mayor en un escenario de amenazas híbridas, donde confluyen acciones militares convencionales y no convencionales, ciberataques, desinformación y presión política, el panóptico de Foucault aporta aquí una lente analítica tradicional. Tal como lo expone Foucault en Vigilar y Castigar (2002), el panóptico es una arquitectura de poder que produce disciplina a través de la vigilancia constante y la internalización del control, trasladado al ámbito militar, el panóptico digital describe la capacidad de sensores, cámaras, IA y ciberdefensa para vigilar no solo el espacio físico de

las instalaciones, sino también los flujos de datos y comportamientos asociados a su seguridad. Según Valencia y Marín (2017), de esta manera el biopoder, como gestión de la vida, la salud y la conducta de los individuos se vincula directamente con control tecnológico de las infraestructuras críticas.

La relación entre el biopoder y la geopolítica se encuentra documentada en las doctrinas de seguridad latinoamericanas, según González Hernández (2017), durante la Guerra fría, la geopolítica fue empleada en América Latina para articular discursos de seguridad nacional que combinaban la defensa territorial con el control de la población, uniendo lo bio y lo geopolítico en un mismo entramado.

Esta herencia conceptual es clave para comprender los desafíos contemporáneos; las instalaciones militares no solo se protegen de ataques físicos, sino también ciberataques y amenazas cognitivas que buscan desarticular su legitimidad frente a la sociedad.

En este sentido, la protección de instalaciones ya no puede concebirse como un asunto meramente táctico. Según Saavedra (2024), el ciberespacio y la IA han convertido a las infraestructuras críticas en blanco prioritarios para actores estatales y no estatales, elevando la necesidad de estrategias integrales que contemplen la resiliencia digital, la gestión del riesgo y la capacidad de respuesta multidominio. La geopolítica critica subraya, además, que tales estrategias no son neutrales, implican la normalización de nuevas formas de vigilancia que reconfiguran las relaciones entre Estado, sociedad y tecnología.

Este enfoque resuena con la perspectiva de Dalby, para quien la geopolítica critica debe centrarse en cómo los discursos y prácticas de seguridad afectan territorios y poblaciones concretas, aplicado a Colombia, esto implica analizar cómo la securitización de

instalaciones militares impacta la relación entre las Fuerzas Militares y la sociedad civil, especialmente en un contexto de memoria del conflicto y transición hacia la paz.

La introducción de tecnologías panópticas digitales, si bien incrementa las capacidades de vigilancia y respuesta, también abre dilemas sobre el equilibrio entre la seguridad y libertad, la expansión de dispositivos visuales de control puede producir tanto efectos de protección como de aislamiento, al generar un exceso de visibilidad que transforma a los sujetos en sombras cautivas de la vigilancia. En el ámbito militar, esta paradoja se expresa en la tensión entre la necesidad de un control total del espacio y el riesgo de producir desconfianza o rechazo social frente a la militarización digital.

El presente documento, por tanto, parte de la articulación entre la geopolítica crítica y teorías ampliadas de seguridad para examinar cómo las nuevas tecnologías pueden proteger instalaciones militares mediante efectos panópticos frente a amenazas hibridas.

El objetivo general es desarrollar una estrategia integral con nuevas tecnologías en la protección de instalaciones militares, destacando su relación con el panóptico digital y la gestión de amenazas híbridas. A su vez, se establecen tres objetivos específicos: el primero, explorar la relación entre biopoder y control tecnológico en la protección de instalaciones militares; el segundo, evaluar el uso de sistemas de vigilancia y panópticos en instalaciones militares y su efectividad frente a amenazas hibridas; el tercero, proponer una estrategia integral que articule estos elementos en un modelo panóptico mixto.

La pertinencia de esta investigación se fundamenta en tres aspectos, primero, en la necesidad teórica de vincular las contribuciones de Dalby y Buzan con los conceptos foucaultianos de biopoder y panóptico, generando un marco analítico interdisciplinario; segundo en la urgencia práctica de enfrentar amenazas hibridas que comprometen la

seguridad de instalaciones militares, donde lo físico y lo digital se entrelazan; y tercero, en la relevancia geopolítica para países como Colombia cuya posición estratégica en el hemisferio, sus compromisos internacionales y su proceso de posconflicto demandan una visión integral de la seguridad que trascienda a la defensa convencional.

2. Metodología

De acuerdo con Hernández Sampieri (2023) esta investigación adoptará un enfoque cualitativo, basado en la interpretación y análisis de datos descriptivos, que busca comprender y analizar críticamente las dinámicas del poder, vigilancia y seguridad en entornos de protección de instalaciones militares. Busca comprender los fenómenos explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto, este caso, el interés no recae en medir estadísticamente las amenazas, sino en interpretar el sentido geopolítico y estratégico de la implementación de tecnologías panópticas digitales y su articulación con las nuevas amenazas.

El diseño metodológico es tipo descriptivo-propositivo, puesto que combina dos propósitos complementarios, por un lado, describe cómo se manifiestan los procesos de securitización tecnológica y panóptica en instalaciones militares; por otro lado, es propositivo porque plantea un modelo de protección integral que combina la teoría del panóptico, el biopoder foucaultiano y los marcos de geopolítica crítica en un esquema operativo aplicable al contexto colombiano, como advierte Hernández Sampieri, la investigación propositiva se orienta a generar soluciones y modelos que respondan a problemáticas específicas.

El carácter cualitativo de la investigación permite articular diversas fuentes documentales como insumo principal, literatura académica sobre geopolítica crítica, y teorías de seguridad de Dalby y Buzan, Wæver & de Wilde, textos clásicos de biopoder y panóptico de Foucault, estudios contemporáneos sobre infraestructura crítica de Saavedra, así, como documentos doctrinales de la ESDEG y las Fuerzas Militares de Colombia.

En términos operativos, la investigación sigue tres fases metodológicas, la primera consiste en revisión documental y bibliográfica de teorías y doctrinas de seguridad, con énfasis en el biopoder, panóptico digital y amenazas híbridas; la segunda fase se centra en la sistematización crítica de categorías analíticas, lo cual permite evaluar comparativamente el panóptico clásico y el digital; y la tercera fase plantea la propuesta estratégica de un panóptico mixto, sustentado en principios doctrinales disuasión, detección, demorar, negar y derrotar la amenaza y en modelos de toma de decisiones como el ciclo OODA.

Dentro de la investigación se aplica una encuesta a través del instrumento digital de Google Forms que tiene como población objetivo el personal militar de la especialidad de Seguridad y Defensa de bases de la FAC, con la participación del personal en todos los grados para lograr priorizar su experiencia en lo relacionado con la protección de instalaciones.

Esta encuesta está conformada por 5 secciones: 1. Percepción sobre tecnologías de seguridad, 2. Biopoder, vigilancia y conducta, 3. Riesgos percibidos y resiliencia, 4. Acción cognitiva, presión psicológica y toma de decisiones, y 5. Carga operativa, presión psicológica y preparación personal.

Aunque el cuestionario incluye preguntas cerradas, se diseñaron preguntas abiertas que permiten explorar narrativas, percepciones subjetivas y experiencias individuales, esto

se ajusta según lo indicado por Sampieri (2014) que en la investigación cualitativa los instrumentos deben ser flexibles, favoreciendo la expresión libre de los participantes.

3. Relación entre biopoder y control tecnológico en la protección de instalaciones militares

3.1. *Poder y autoridad como paradigma de la protección*

La protección de instalaciones tradicionalmente se ha abordado desde el punto de vista de seguridad física; en este estudio se abordará desde la teoría de poder como principal fuente de autoridad y gobernabilidad.

La autoridad sobre las instalaciones militares y sus áreas de seguridad establece sus fundamentos en el poder ejercido en la soberanía de su territorio y la sociedad que la circunda, para definir el poder que es representado en autoridad, se parte de la definición clásica de poder de Max Weber (1944) que la conceptualiza como la probabilidad de obtener obediencia de otros en una asociación de poder, y la regulación del orden está asegurada mediante la coerción y la amenaza.

También Weber señala el poder como una dominación desde la imposición y la disciplina como la generación de normas para la regulación y acatamiento de la sociedad, estableciendo una jerarquía dentro de la sociedad, que al final se vuelve como la probabilidad de encontrar obediencia.

Esta definición de poder se refleja en la protección tradicional de instalaciones fundamentadas en control de perímetros, barreras físicas, centinelas, patrullas y sensores, para la defensa del territorio y protección del espacio físico, con una lógica de poder de disuasión basada en presencia y el uso de la fuerza, que de acuerdo cont Weber el poder se

ejerce mediante la coerción y amenaza que fundamenta la autoridad bajo dominación y disciplina.

La protección de instalaciones no ha estado alejada de la constante transformación tecnológica del mundo, desde la mitad del siglo XX y con las revoluciones industriales el concepto de vigilancia y seguridad ha avanzado rápidamente, desde sus inicios para la década de los años 50 donde aparecen nuevas tecnologías de video vigilancia, en Alemania con el objetivo de regular los patrones de tráfico, y luego utilizado en situaciones de seguridad en Estados Unidos y Reino Unido, y para finales del siglo XX fue introducido como sistema de seguridad mediante cámaras (Delgado, 2018).

Estos avances tecnológicos conducen a un nuevo modo de ejercer autoridad en una sociedad disciplinada, un nuevo concepto crítico de poder separado del uso de la fuerza y dominación de los individuos disciplinados con otras condiciones regulatorias, por lo anterior, resulta pertinente observar la propuesta contemporánea presentada por Michael Foucault, quien plantea una imagen positiva del poder: "El poder produce. Y produce lo real, a través de una transformación técnica de los individuos en la modernidad, que en nuestra sociedad recibe un nombre: normalización" (Foucault, 2000). Apartándose de la imposición y represión, el poder se vuelve activo, preventivo y con interrelación constante con el individuo, creándose leyes para quienes transgreden las normas.

Este nuevo concepto de poder desplegado con la video vigilancia puede llevar a descartar o replantear la protección clásica, hay que preguntarse ¿es disuasiva la videovigilancia? ¿es real el poder ejercido por la videovigilancia? ¿se deben mantener, reducir o desistir de los centinelas? ¿Qué nuevo rol cumplirían las patrullas para la protección de instalaciones? la presencia del ser humano ejerciendo poder directamente

sobre los individuos genera fricción e incrementa la perspectiva de violencia al ejercer poder, al final debe llevar a dar la respuesta a la pregunta principal de esta investigación ¿Cómo las nuevas tecnologías pueden prestar protección a las instalaciones militares a través de los efectos panópticos, respondiendo efectivamente a los desafíos de las amenazas híbridas?

No es solo vigilar y regular, contar con los archivos de la video vigilancia el poder se ve replanteado en la acción directa de autoridad sobre el individuo disciplinado, Foucault señala que el saber es parte del poder: "todo esto constituye la fábula que occidente se cuenta a sí mismo para enmascarar su sed, su gigantesco apetito, de poder sirviéndose del saber" (Foucault, 1999).

Contar con la información del individuo transfiere el control y ejerce poder de forma sofisticada, utilizándola como instrumento de imposición y autoridad sobre los individuos, no solo es observar en tiempo real para proteger y responder, ejercer poder a través de los datos en custodia que ilustran sobre el evento completo (pre, durante y post), desde múltiples puntos que nos pueden arrojar información para la investigación y en caso de requerirlo replantear los procedimientos de seguridad.

Foucault en su propuesta tiene en cuenta los contextos donde se presentan los conceptos, afirmando que cada época presenta nuevos principios y una nueva forma de discernir de como ver la autoridad del poder "Nuevos mecanismos de poder han evolucionado para lograr que los individuos sean dóciles y disciplinados para que contribuyan a la productividad" (Dávila, 2014). Buscando que el individuo se adapte y acondicione a la nueva forma de vigilancia y autoridad, y no visto como un castigo.

3.2. *Biopoder y comportamiento en la seguridad*

Los nuevos conceptos sobre el poder sobre una sociedad disciplinada y los constantes cambios tecnológicos en la videovigilancia llevado a Michel Foucault a presentar una propuesta para su curso dictado en la clase del 11 de enero de 1978, Foucault (2006) propone una nueva estrategia para ejercer el poder y para analizar sus mecanismos; el biopoder es interpretado por Foucault como una estrategia ejercida directamente sobre la vida, mediante técnicas y dispositivos orientados a administrar, optimizar y más importante aún, disciplinar individuos y a las poblaciones, lo cual resulta pertinente para el estudio de la protección de instalaciones y la gestión de las amenazas.

El biopoder resulta especialmente pertinente como marco interpretativo porque permite examinar las lógicas de control y normalización que aseguran la resiliencia operativa y la respuesta adaptativa frente a los riesgos complejos, integrando las dimensiones física, conductual y cognitiva de la seguridad (Foucault, 2006).

Foucault busca dilucidar el contexto en el que ocurren las cosas, los mecanismos y los individuos involucrados, sus protocolos y sus efectos; propone saber por dónde pasan las cosas y cómo pasan, entre quienes están de acuerdo con qué procedimientos y con qué efectos, cómo se transforman los mecanismos de poder, teniendo en cuenta que el poder se hace, se establece y se ejerce, definiéndolo desde su propia operatividad.

Es así como, para administrar, optimizar y disciplinar los individuos, Foucault señala el surgimiento de dispositivos de seguridad como mecanismo de control social o capaces de modificar el comportamiento del individuo, y plantea que en las sociedades el poder se está reconfigura al orden de la seguridad, buscando el dominio del poder.

El biopoder marca una nueva dimensión dentro de la protección de instalaciones, refuerza la idea que la seguridad no solo es protege físicamente, sino a través de la regulación, conductas y procesos de vida de los individuos, como poder ejercido en la sociedad, dicho lo anterior, está regulación se puede observar con dos actores importantes dentro de la protección de las instalaciones.

El primer actor, el externo, el grupo de individuos que se encuentran fuera del perímetro físico de las instalaciones, actor que de acuerdo a su administración y regulación se vuelve un factor crucial para la seguridad y su comportamiento puede ser ventaja y de cooperación para la protección, o se vuelve el factor más cercano para afectar a seguridad.

El segundo actor es el interno, encargado de la protección, su capacitación, cumplimiento de funciones y conducta sobre los individuos juegan un papel importante en la optimización de la seguridad. Su acción como mecanismo de poder con una incorrecta acción para disciplinar sobre los individuos puede generar fricción y en el contexto actual es visto como una acción violenta contra la sociedad, deteriorando la autoridad legítima de la protección.

Siguiendo a Foucault, la transformación de ambos actores exige generar su transformación para hacerlos productivos, hay que traducirlo en una buena normalización de las acciones de los dos actores con una buena capacitación de las regulaciones y una buena integración de estos dos actores, establecer una observación controlada sin transgredir la soberanía de cada actor y ejercer el poder con legitimidad social que lleve a la cooperación del actor externo para incrementar el rango de la seguridad y ampliar su zona de protección y observar las amenazas distante a los perímetros físicos de seguridad.

Para dar operatividad y articulación dentro del biopoder a través de las nuevas formas de ejercer poder y su normalización, se inserta el concepto de dispositivo de seguridad, que, según Agamben al citar a Foucault, es todo aquello que tiene la capacidad de captar, orientar, determinar, interceptar, modelar, controlar y asegurar los gestos, las conductas, las opiniones y los discursos de los seres vivos (Agamben, 2014). Para desarrollar este concepto de dispositivos de seguridad en la protección de instalaciones se profundiza en espacios de seguridad.

Para esto, Foucault (2006), en su análisis moderno del poder, que es ejercido sobre los individuos y la población, determina una tríada: la soberanía como principal poder ejercido sobre los límites de un territorio; la disciplina, sobre los individuos; y la seguridad, como poder ejercido sobre la población.

La soberanía, desde su enfoque clásico como lo propone Jean Bodin "el poder absoluto y perpetuo de una República" (Bodin, 1997), es una estructura centralizada, que impone orden, justicia y estabilidad institucional, con enfoque jurídico político.

En la genealogía del poder, Foucault (2000) desarrolla un concepto crítico y contemporáneo incluido en el biopoder, reorganiza la soberanía desde la vigilancia como disciplina y seguridad en gestión de la vida del individuo, sin perder el control territorial en espacios excepcionales por el estamento militar, replantea una forma avanzada de gobierno para ejercer el poder para fomentar la vida.

La disciplina, como segundo eje, disciplina a través del entrenamiento, transformación y el ser observado, emerge con un enfoque de gobierno del individuo como una forma de poder, produciendo individuos útiles y obedientes bajo la lupa de la vigilancia.

El actor interno juega un papel importante dentro de la disciplina, "el soldado se ha convertido en algo que se fabrica… se ha hecho la máquina que se necesitaba; se han corregido poco a poco las posturas… perpetuamente disponible, y se prolonga, en silencio, en el automatismo de los hábitos" (Foucault, 2002). Disciplinar al actor interno para cumplir con el desafío de los avances tecnológicos es el mayor reto para consolidar una protección de instalaciones con videovigilancia.

Este actor interno contribuye a configurar el poder con la acción de disciplinar al individuo y su relacionamiento con el exterior, su evolución dentro del contexto social debe tener una mayor injerencia al interactuar con la población para ejercer poder sin generar fricción, conservando la autoridad que se refleja en la disciplina del individuo en el campo abarcado por la seguridad fuera del territorio asignado para su protección.

La buena interacción con el actor externo facilita su preparación para interiorizar las regulaciones referentes a la protección de las instalaciones a través de videovigilancia; permite ejercer el poder para optimizar la seguridad de la instalación y, al final, proteger la población; el resultado de la disciplina del individuo es la sana convivencia e interacciones relacionadas con la seguridad, la protección de la instalación se vuelve la protección de la población.

Foucault (2006) marca una sucesión, las normas, la disciplina del individuo como fuente principal de la seguridad, sin una buena disciplina o estructuras obsoletas la seguridad se debilita. Es de suma importancia mantener una evaluación constante de las condiciones de los individuos a través de la vigilancia con el fin de conocer la interiorización de las regulaciones y puesta en práctica de los procedimientos de protección.

El tercer eje, la seguridad, aparece como una tecnología del poder que no prohíbe no disciplina directamente, sino que regula a partir de los cálculos de probabilidades y la gestión del riesgo. Foucault describe esta tecnología para la población, como sistema regulador, uso de datos y algoritmos para anticipar amenazas, conocer a la población que interactúa en las fronteras con la instalación es de vital importancia para monitorear comportamientos, gestionar información y datos para anticiparse a la amenaza o mantener el poder efectivo del área externa protegida.

En este punto se articulan los aportes de Barry Buzan, quien concibe la seguridad como un proceso de securitización, Buzan (1998) señala que la seguridad no es una condición estática, es la consecuencia de un discurso que transforma un tema específico en una amenaza, además "el acto de etiquetar algo como una cuestión de seguridad transforma el tema y origina dinámicas de seguridad específicas" (Buzan & Wæver, 2003). Esto implica que los procesos de securitización no son neutrales, sino actos reformativos que definen los objetos referentes, legitiman medidas extraordinarias y justifican el despliegue de tecnologías de vigilancia.

Tras desglosar la tríada de los dispositivos de seguridad del biopoder, se resaltar que esta forma de poder no actúa sobre sujetos jurídicos, sino sobre individuos y su conjunto, no se acepta la fuerza, sino medidas de control técnico y vigilancia. La seguridad ya no consiste solo en contener la amenaza, sino en gobernar la vida, optimizar el rendimiento y regular la población.

La protección de instalaciones puede constituirse como laboratorios del biopoder, se constituyen espacios privilegiados para observar la convergencia de soberanía, disciplina y seguridad como tecnologías del biopoder, el Estado conserva su capacidad soberana, sobre

acciones excepcionales el uso legítimo de la fuerza, mantiene sus sistemas disciplinarios bajo el concepto de entrenamiento y jerarquía y despliega dispositivos de seguridad a través de la videovigilancia para monitorear, clasificar y anticipar la amenaza.

El control de la videovigilancia no es neutral, se configura dispositivo técnico del biopoder que transforma individuos en datos, la vida en información y el riesgo en objetivo de la proyección, de modo que no solo se protegen las instalaciones, sino que gobiernan la vida bajo criterios operacionales.

En este contexto de la autoridad y de poder, puede introducirse un concepto que se relaciona con el biopoder y es acuñado por Roberto Esposito (2002): la inmunización, entendida como un proceso mediante el cual la política protege la vida a través de mecanismos que la limitan parcialmente. De acuerdo con Esposito (2004), no se limita al ámbito biológico, sino que se expande hacia la administración del riesgo tecnológico, cognitivo y social.

Este proceso se traduce en la vigilancia constante que actúa tanto sobre los cuerpos cómo sobre las poblaciones, generando dinámicas de disuasión hacia los actores externos y de normalización de rutinas disciplinarias en el actor interno. Así, la inmunización se convierte en un principio conductual, donde la protección se alcanza no solo mediante la robustez tecnológica, sino también a través de autorregulación y adaptación a la vigilancia.

La convergencia entre Foucault y Esposito abre una nueva comprensión del biopoder en la era digital, el poder deja de ser únicamente disciplinario o regulador para convertirse en una tecnología de gestión de la vida a través de la inmunización, donde la seguridad se convierte en la forma suprema de control. Este enfoque resulta esencial para la protección de instalaciones, pues permite analizar cómo las nuevas tecnologías funcionan

como dispositivos inmunitarios que administran la vida colectiva mediante la vigilancia, la prevención y la disuasión, convergiendo así en un modelo donde el control del riesgo se convierte en el núcleo operativo del poder.

3.3. *Conductismo operativo*

El conductismo, como teoría del comportamiento humano formulada por B. F. Skinner, ofrece una perspectiva operativa clave para comprender el modo en que el biopoder se articula a través de tecnologías de vigilancia y control, desde esta óptica, el comportamiento puede moldearse mediante refuerzos positivos y negativos, sin apelar a nociones de libertad o voluntad. Es así, para la protección de instalaciones, el entorno tecnológico de la videovigilancia actúa como un espacio de condicionamiento conductual, donde el sistema en su conjunto y delimitaciones físicas funcionan como estímulos de refuerzo que anticipan, inhiben o redirigen comportamientos.

Así, el actor externo es inducido a cumplir protocolos sin necesidad de coerción o uso de la fuerza, como señala Skinner (1986), el uso de la fuerza queda relegado cuando los individuos quedan bien programados, contemplado desde su entrenamiento y aplicación de doctrina y las normas regulatorias; lo que permite entender la videovigilancia como un dispositivo del biopoder que opera desde el diseño del entorno.

El actor externo no se administra eficazmente solo mediante coerción, sino mediante arreglos que fabrican conductas de cooperación y cumplimiento; en consecuencia, la videovigilancia debe operar como señal de confianza y no de incertidumbre. Según Rivera-Páez (2019) la legitimidad social caracterizada por el apoyo y aceptación de los

actores externos, estos sistemas de videovigilancia reducen la percepción de seguridad invasiva.

El resultado de la aplicación de estos dispositivos por parte del actor externo y el refuerzo positivo del entorno según Rivera-Páez (2019) favorece la legitimidad, consolida la democracia y fortalece la descentralización en seguridad y desmilitarizando las relaciones sociales, lo que condiciona e incentiva las conductas cívicas de coproducción de seguridad, cooperación de información, respeto a perímetros, haciendo que la videovigilancia funcione como tecnología de confianza y no de intimidación.

Desde una perspectiva conductista en el contexto operativo, el actor interno debe recibir estímulos por parte de la institución representados en la doctrina, procedimientos y distinciones que condicionen el comportamiento observable como un indicador crítico de desempeño, que se refleja en la legitimidad de sus acciones como centro de gravedad de los dispositivos de seguridad y videovigilancia. Rivera-Páez (2019) cualquier arquitectura de vigilancia y control debe diseñarse como un conjunto de refuerzos que mantengan la conducta profesional bajo altos estándares verificables y socialmente aceptables.

Articulado con lo anterior, diferenciar, en la decisión del uso de la fuerza, aquellas actitudes y prácticas que se ganan reconocimiento permiten convertir el biopoder en patrones conductuales definidos que refuercen el uso responsable de las acciones del actor interno reduciendo el riesgo de deslegitimación por abuso o error.

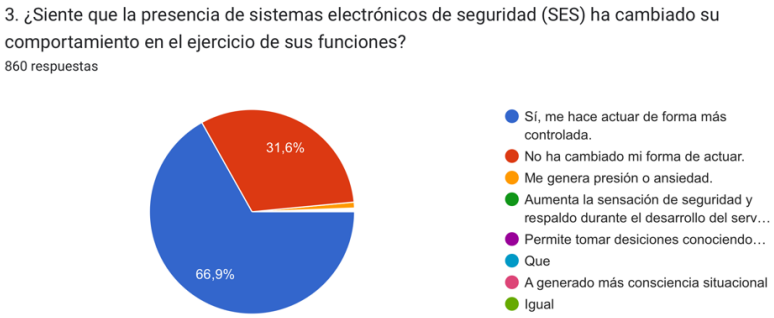
El conductismo permite analizar como los sistemas de entrenamiento y supervisión se convierten en dispositivos de normalización del biopoder; el actor interno no solo es vigilado, sino programado mediante protocolos de reforzamiento sistemático que moldean decisiones, actitudes y reflejos frente a amenazas.

En condiciones de alto estrés o ambigüedad táctica, la toma de decisiones se apoya en aprendizajes operantes previamente interiorizados mediante ejercicios y ensayos, como explica Skinner (1986), cuando se ha interiorizado la forma de proceder ante cualquier situación que se ha ensayado, el resultado no deliberado, consciente de su comportamiento efectivo, en este sentido, el biopoder no actúa solamente sobre cuerpos físicos, sino también sobre el comportamiento automatizado, integrando tecnologías, conducta y racionalidad operativa en el mismo dispositivo.

El conductismo alineado con las tecnologías se manifiesta claramente en la protección de instalaciones contemporáneas, donde el espacio está configurado con una videovigilancia pensada para producir individuos funcionales, a través de sistemas inteligentes de control, el entorno no es solo vigilado, sino también pedagógico, enseña lo que se espera, refuerza lo permitido y corrige lo desviado sin necesidad de presencia física, el sentirse observado genera un cambio conductual de los actores.

Al final, la protección de instalaciones no se limita a neutralizar amenazas, sino que modela anticipadamente la conducta de los individuos es función de su utilidad, previsibilidad y alineación lógica del sistema. Así, el conductismo se convierte en un vector operativo del biopoder, articulado a través de redes tecnológicas que gobiernan la vida, no solo con reglas, sino también mediante estímulos que hacen de la seguridad una práctica de autoridad y poder más que defensa.

Sumado a lo anterior, en la encuesta realizada al personal de Seguridad y Defensa de la FAC encargado de la protección de instalaciones componente físico del Poder Aéreo, Espacial y Ciberespacial se confirma que los SES cumplen una doble función, fortalecer la protección física y actuar como dispositivo de disciplinamiento y normalización de la conducta de los individuos.



En esta respuesta, más del 66.9 % de los encuestados afirma actuar de manera más controlada bajo la presencia de estos sensores digitales, lo que produce la percepción de estar observado permanentemente y reproduce la lógica panóptica, ajustando su comportamiento y confirmar que los SES operan como mecanismos de control conductual que reducen las desviaciones y refuerzan la obediencia institucional.

Este hallazgo evidencia con claridad el funcionamiento de dispositivos de biopoder en el espacio protegido, moldeando el comportamiento de los individuos a través de la visibilidad constante y la interiorización de las regulaciones, desde la mirada de Foucault esta transformación del comportamiento bajo la mirada invisible del poder constituye el núcleo del panóptico, el individuo se convierte en vigilante de sí mismo, en este sentido los

SES no solo controlan, sino que produce cuerpos obedientes sujetos de control y regulados por una norma.

4. Uso de sistemas de vigilancia panópticos en instalaciones militares y su efectividad en el control y neutralización de amenazas hibridas

4.1. *El panóptico, vigilancia y disuasión*

El panóptico formulado por Jeremy Bentham, en el siglo XVIII, se refiere originalmente a una estructura arquitectónica penitenciaria circular con una torre central desde donde podía observarse a los internos sin ser visto. Este principio de vigilancia unidireccional generaba una sensación permanente de observación en los internos, este diseño, concebido como un "lugar desde el que se ve todo", implicaba una forma de poder, control y autoridad más eficaz que el castigo físico, ya que introducía en la mente de los observados la posibilidad constante de estar vigilados, desencadenando la autorregulación de la conducta, como señalo Bentham (1980), se trataba de obtener poder de la mente sobre la mente, el ojo que todo lo ve.

Michel Foucault profundizó el concepto de Bentham, sosteniendo que el panóptico no solo organiza el espacio, sino que constituye una perspectiva del poder moderno, caracterizada por una vigilancia continua y sin reciprocidad que convierte al individuo en sujeto disciplinado.

Esta arquitectura moral representa la mutación del poder soberano hacia un poder disciplinado que ya no se castiga, sino que moldea y regula la conducta a través de una vigilancia que es constante y ubicua. Según Foucault (2002), es capaz de producir obediencia al ser sometido a una vigilancia sin ser observado, el actor externo asume por sí

mismo las imposiciones del poder, logrando una autodisciplina del individuo, para el actor interno se traduce en jerarquía y control institucional.

En las instalaciones militares, la lógica panóptica describe un dispositivo que permite ver sin ser visto, para Foucault (1980) es producir conductas predecibles mediante la posibilidad constante de supervisión, esta economía de visibilidad más que coerción física, es la base de su eficacia disuasiva en espacios de alta seguridad.

Desde la perspectiva de Foucault (2006), en su tríada del biopoder los dispositivos de seguridad operan normalizando la conducta, mitigando el riesgo y distinguiendo lo habitual de lo atípico, aplicado a las instalaciones militares, estos dispositivos justifican anillos de seguridad, áreas restringidas y protocolos de respuesta que buscan reducir las situaciones de amenazas, especialmente la de mayor vulnerabilidad, mediante métodos de visibilidad del actor interno y sus regulaciones.

En términos de teoría de la disuasión, la visibilidad del actor interno y la incertidumbre sobre el punto de observación elevan los costos percibidos de las amenazas, desplazando el cálculo del actor hacia la inacción, de acuerdo con Sekulovski (2016), el factor panóptico opera psicológicamente, el poder se ejerce desde la autodisciplina siendo más eficiente administrar el riesgo que contener la conducta.

Las nuevas tecnologías constituyen el punto de partida para un nuevo panóptico, orientado a disuadir, controlar y neutralizar amenazas. El panóptico se ha adaptado al entorno digital mediante SEs, según Wajcman (2010), estos sistemas, definidos como panóptico digital, ya no dependen de estructuras físicas y centinelas, sino en redes descentralizadas de observación continua; el sujeto ya no es simplemente observado, sino

que produce datos constantemente, convirtiéndose en datos, la vigilancia ya no se impone, se integra, lo que permite anticipar y neutralizar potenciales amenazas.

En este marco, la videovigilancia no es un fin en sí mismo sino una pieza de una estrategia de seguridad que se articula en lo jurídico y lo operacional, con control disciplinario para el actor interno y la seguridad para el actor externo, para prevenir, detectar y neutralizar contingencias, su pilar fundamental es su capacidad para hacer creíble la intervención de la autoridad como necesaria y suficiente frente a la amenaza, reduciendo la incertidumbre sobre una acción del actor externo contra la instalación y anticipándose en la toma de decisiones.

El rápido avance de nuevas tecnologías que alimentan el panóptico digital, ligado al afán de las grandes potencias que ejercen el autoritarismo con el individuo, se analiza hoy como "represión digital". Utilizando medidas de vigilancia intensiva para ejercer poder y control representado en la represión y coerción de los individuos, el concepto de represión digital de Steven Feldstein (2021) la define como es el uso de la tecnologías para vigilar, coaccionar o manipular a individuos que desafían al Estado, así que el uso del reconocimiento facial, las llamadas ciudades inteligentes o seguras con transmisión de datos en tiempo real, están siendo utilizadas para ejercer un control coercitivo y manipular a los individuos reintroduciendo lógicas del poder soberano.

Dentro de la construcción del panóptico sin afectar su base fundamental, apararen nuevos análisis y enfoques del ejercicio del poder, autores como Gilles Deleuze (2017) proponen que se pasa de una sociedad disciplinaria a una sociedad de control; ya no opera con individuos, sino que propone el concepto de "dividuos", definido como fragmentos de identidad que se gestionan mediante accesos, códigos y rastreos, a diferencia del poder

foucaultiano, centrado en la visibilidad y el cuerpo, Deleuze propone un poder que actúa por modulación, ya no el cuerpo que se vigila, sino los datos del cuerpo, y el acceso a funciones, privilegios y espacios.

Este nuevo concepto permite comprender y configurar el panóptico digital sin perder el enfoque de poder de Foucault, reforzándolo en las acciones de control, así, el panóptico digital ejerce poder y autoridad sobre los individuos controlados atreves de SES que los vigilan con una distancia cada vez mayor, permitiendo alejarse cada día más de los individuos de forma física y combatir con dividuos o datos como lo presenta Gilles Deleuze.

En relación con lo anterior, el conductismo también robustece el panóptico, el control ejercido desde la vigilancia se refuerza por el principio del condicionamiento operante, Skinner (1971) afirmaba que la conducta se modela por sus consecuencias, así, puede sostenerse que el actor interno y externo tienden a ajustar su comportamiento cuando saben que está siendo observados, interiorizando sus funciones institucionales y sus normas regulatorias. Esta interiorización se convierte en un mecanismo de autorregulación que reduce la necesidad de intervenciones disciplinarias.

Según José Loskyn (2015) el panóptico digital amplía los vectores de disuasión y control, convirtiéndose en una red transversal y horizontal, ya no se centra en la vigilancia ejercida por un solo observador que ejerce el poder a través de la visibilidad de las personas que se sientan observadas y de un resultado que puede ser puesto en duda, gracias a los avances tecnológicos la vigilancia se ha ampliado de forma ilimitada, dejando atrás el concepto que los individuos se sienten observados y pasan a actuar bajo la ilusión de

libertad y autonomía, lo que, en el contexto militar, convierte la vigilancia en mayor campo de observación y control fuera del área asignada y ejercer un efecto disuasivo.

No solo ejerce el control sobre los individuos y previene amenazas físicas, sino que detecta patrones de conductas anómalos y reacciones psicofisiológicas inusuales; ademas, opera en el dominio cognitivo, sirviendo de barrera frente a estas acciones, según la OTAN (2020), las amenazas cognitivas buscan alterar el juicio y la moral de los individuos y erosionar la cohesión organizacional, en este contexto, disponer con un panóptico digital permite contrarrestar estos efectos al articularlos con educación y diseño conductual para maximizar el cumplimiento voluntario y reducir el desgaste coercitivo, también permite mantener la alerta situacional del individuo que no está directamente expuesto a acciones cognitivas, monitoreando alertas de fatiga o patrones de riesgo conductual que afecten la toma de decisiones en el proceso de seguridad.

La protección de instalaciones modernas, especialmente en el ámbito militar, requiere no solo protección clásica, sino también actualizarse tecnológicamente para ejercer control y adelantarse a acciones de amenaza. Según Juan Delgado (2018), los nuevos sistemas de videovigilancia permiten detectar movimientos anómalos y activar protocolos con poca o nada de intervención humana directa, gracias a la amplia observación que cubre no solo del área asignada para la seguridad, sino que amplia su cobertura del área para la observación y ejercer control de los individuos.

El panóptico digital, entonces, no solo presenta una continuidad del modelo clásico, sino una mutación que se adapta a la lógica del biopoder, el poder que se ejerce sobre la vida, sobre las conductas, sobre los cuerpos y los datos. Como lo plantea Foucault, el poder moderno no se ejerce desde la fuerza, sino desde la gestión de la vida, "la seguridad no

refleja el territorio: lo produce" (Foucault, 2006). Así, el panóptico digital produce subjetividades, disciplina, control, autorregulación y, al final también eficiencia.

Desde el concepto del biopoder, el control panóptico de los individuos no es solo una función logística o defensiva, sino una forma de gubernamentalidad, la vigilancia panóptica transforma los espacios militares en espacios de normalización, donde la conducta esperada no es impuesta, sino aprendida, interiorizada y reproducida, esto representa una ventaja operacional frente a las amenazas híbridas y cognitivas, pero exige límites éticos, regulación jurídica y entrenamiento psicológico y conductual adecuado para los actores internos y externos.

5. Estrategia integral con nuevas tecnologías en la protección de instalaciones militares

5.1. *Panóptico clásico*

Para hablar de panóptico clásico se debe definir el concepto de seguridad física: "la parte de la seguridad relacionada con las medidas físicas destinadas a proteger a las personas, para evitar el acceso no autorizado a las instalaciones y protegerlas contra un incidente de seguridad" (ASIS International, 2012).

Dentro de la doctrina de la U.S. Air Force (2023) se establece que, para la protección, deben lograrse la disuasión, detección, demora, negación y derrota de la amenaza, mediante medidas materiales y humanas.

Este concepto de seguridad se alinea con el panóptico clásico de Bentham, quien lo concibe como un edificio circular con celdas periféricas iluminadas y una torre central de inspección, establece un principio arquitectónico de visibilidad total. Según Foucault

(1980), "basta situar un vigilante en la torre central" observar con unos parámetros básicos disciplinan al individuo sin tener contacto entre los dos actores, e invierte la lógica de las mazmorras: la iluminación y el centro de gravedad de los ejes del control físico del espacio y de los individuos.

De este modo, el panóptico se configura como un sistema de vigilancia para proteger los componentes que integran las instalaciones, donde su principal fuente de observación se promueve a través del individuo.

La lógica economía del panóptico reside en maximizar la supervisión en el mínimo de personal, garantizando la línea de visión continua del centinela. Bentham lo concibe domo economía de vigilancia: "el esquema del círculo del panóptico deberá conservar el carácter de economía en la vigilancia, es decir, solo puede agregarse a ese cuadro, un vigilante por esquina" (Valencia & Marín, 2017). Aplicado literalmente, un actor interno controla áreas periféricas fragmentadas, manteniendo el control del actor externo sin interactuar y bajo observación constante, que puede rayar en una acción coercitiva.

Traducido a garitas, anillos de seguridad, zonas despejadas y amplia visibilidad controlados desde puntos elevados, reforzados por barreras y compartimentación, configurando la seguridad física de instalaciones como el conjunto de medidas materiales y presencia humana para disuadir, impedir y responder a intrusiones o agresiones, priorizando al actor interno como eje fundamental de la seguridad, barreras, iluminación y patrullajes en profundidad, sin apelar a SES.

Entre sus beneficios estratégicos, Foucault (1980) señala que este enfoque clásico genera disciplina y regularidad, el control jerárquico, las revistas y el encauzar la disciplina producen conductas y rutinas previsibles que, en una instalación militar, sostienen la

postura y el alistamiento con bajo ruido interno, esta regulación y control facilita órdenes claras, supervisión y control efectivo del individuo en áreas restringidas.

Además, la visibilidad constante del dispositivo proyecta poder: la visibilidad del actor interno en los perímetros refuerza la autoridad, el símbolo del Estado y contribuye a la resiliencia institucional, en tanto los actores internos y externos perciben una respuesta ordenada ante una amenaza. De acuerdo con el Instituto Español de Estudios Estratégicos (2018), orienta simultáneamente la conducta de ambos actores en situaciones de amenaza y mitiga la incertidumbre en la acción táctica.

Sin embargo, este panóptico exige un sistema continuo de vigilancia, y un estado de alerta permanente del actor interno que se degrada por la monotonía, la fatiga y la distracción que son limitaciones propias del individuo, y se manifiestan en la seguridad física, lo que abre ventanas de oportunidad al actor externo al caer la alerta situacional en algún sector o durante turnos prologados del centinela.

La simetría del terreno juega un papel importante en este panóptico, según Foucault (1980), fuera de un marco geométrico óptimo, la topografía, edificaciones adyacentes y sombras generan ángulos muertos que niegan la identificación a plena luz y la línea de visión continua que el modelo demanda, allí donde se fractura la visibilidad del individuo, el dispositivo pierde su efecto disciplinario y su economía de personal.

Esta vulnerabilidad se agudiza si se incluye la reducción de personal, algunos informes indican que el pie de fuerza de soldados regulares en las Fuerzas Militares en Colombia se ha reducido en un 46 % aproximadamente en los últimos 15 años, esto erosionando la capacidad operacional para la protección de instalaciones y obliga a desviar un porcentaje de individuos relacionados con otras capacidades a reforzar sus acciones en

apoyo a la protección de instalaciones, con la perdida en algunas ocasiones del control territorial de las áreas asignadas para la protección de instalaciones.

Si se toma como referencia a la Fuerza Aeroespacial Colombiana, la fuerza más pequeña del país, durante años no ha logrado sostener su planta de soldados para la seguridad y defensa del componente físico del poder aéreo, espacial y ciberespacial; su cumplimiento se ha mantenido en un 42 %, lo que dificulta contar con el personal adecuado y de alta rotación para cumplir sus funciones de seguridad.

De igual forma, el estudio de prospectiva y disminución de personal presentado por Juan Díaz (2023) en su investigación a un escenario 2042 identifica una tendencia sostenida a la baja en incorporación (12,6 % anual 2017 a 2021; proyección 14,2 % a 2028) y recomienda reformar el sistema para garantizar el capital humano suficiente y sostener el sistema de protección de instalaciones. La señal estratégica es inequívoca sin corregir la pendiente demográfica y normativa, el panóptico clásico pierde factibilidad operativa.

A ello se suma el riesgo de cooptación del actor interno, una nueva guerra sobre el cerebro humano, según François du Cluzel (2021), la guerra cognitiva describe al celebro humano como dominio operativo, explota sus vulnerabilidades en el procesamiento de información fácil de manipular y engañar, los sesgos cognitivos llevan a una mala toma de decisiones.

Un centinela fatigado, aislado en un puesto de guardia es blanco para cooptación, manipulación, narrativa o presión del actor externo, que puede penetrar al actor interno y provocar acciones desde el interior del sistema de seguridad. No se requiere fuerza física para lograr una acción enemiga, un ejemplo de esto parte desde la presión psicológica que se ejerce al actor interno por las constantes noticias de ataque a las instalaciones, sumado a

esta presión, el observar en varias oportunidades pasar un mismo vehículo, una persona en repetidas ocasiones, consigue llevar a la mente del centinela a ser influenciada por desinformación e impactar sus emociones.

En muchas ocasiones se logra poner en alerta al centinela, la presión a sido tan fuerte que no logra superar sus emociones, dejando un sesgo residual que puede ocasionar un error en la toma de decisiones. Estás acciones cognitivas, de largo aliento desgastan física y mentalmente al centinela y que en el momento menos esperado actúa el enemigo.

La dimensión fisiológica del centinela es importante, su fácil distracción es una gran vulnerabilidad, es estrés, falta de sueño y sobrecarga de atención degradan la atención y su buen juicio. Según François du Cluzel (2021), los conceptos estratégicos y psicosociales subrayan la batalla por la atención y la disputa por la violencia psicológica como vectores que merman el rendimiento y resiliencia de la seguridad basada en individuos. En el panóptico clásico, donde todo descansa en la observación y percepción del individuo, cuando esta falla, falla el sistema de seguridad.

Visto lo anterior, y los actores como centro de gravedad, conviene estimar el costo de operación (OPEX, Operating Expenditures), gastos recurrentes y diarios para la operación de esté panóptico, para un soldado como el actor operativo dentro de la protección de instalaciones, con base en la ley 2384 de 2024 (que modifica la Ley 1861 de 2017), en esta nueva Ley, los gastos de personal de un soldado que ejercen como centinela le cuesta a la institución aproximadamente $31.280.035 para el año 2025 incluyendo instrucción básica; para el año 2026 la bonificación subiría a un salario mínimo mensual legal vigente, más el incremento anual del salario mínimo, esta bonificación aumentaría aproximadamente un 30 %.

Si se realiza un ejercicio de un perímetro lineal de 600 metros donde se parte de la observación en referencia al panóptico clásico, se establecen siete centinelas a lo largo de esta distancia, en un periodo de 24 horas se establecen tres turnos de cuatro horas, lo que lleva a establecer un costo operativo básico aproximado de $656.880.735 por un año de seguridad en esté perímetro.

De este costo anual aproximado deben considerarse gastos que no incluidos, como mantenimiento de instalaciones, servicios públicos, incorporación, exámenes médicos de ingreso y licenciamiento, así como atenciones médicas cuando el soldado es licenciado, pero continúa a cargo del subsistema de salud de las FF. MM.

Otros gastos no calculados no recurrentes, pero de gran impacto para el presupuesto del Estado, los encontramos en dos variables: la primera, por acciones administrativas en contra del Estado ocasionados lesiones o muerte de un actor externo o interno, que son al final causa de fatiga, descuido o mala toma de decisiones del centinela; la segunda, costos por enfermedades de alto valor y accidentes del actor interno que al final representan un gran gasto para el sistema de protección.

De acuerdo con lo anterior y la definición clásica de seguridad de instalaciones, como medidas estructurales y humanas, basadas en barreras, iluminación, centinelas y patrullas que disuaden, impiden y responden a intrusiones y ataques, constituyendo la primera línea de protección.

La efectividad del sistema exige suficiente personal en constante alerta, entrenado y con una alta disponibilidad, lo cual conduce a incrementar los costos variables de este sistema clásico, cada vez que aumentan los centinelas y la disponibilidad del personal por el aumento del riesgo, aumenta el costo del sistema, rompiendo en concepto clásico de

Bentham sobre economía de la vigilancia. Asimismo, cada año aumenta el OPEX de acuerdo con el incremento en gastos de personal, dotación y salud.

A este costo se suman los costos del mantenimiento de las instalaciones (matrices de mantenimiento para barreras de retardo, garitas de seguridad), utilizadas no solo para mantener la observación constante, sino la seguridad del centinela que al final del ejercicio es una de las variables de mayor costo dentro de este sistema de seguridad.

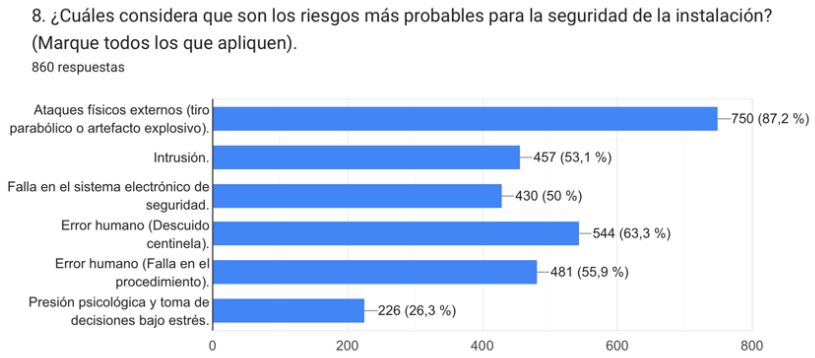
El panóptico clásico presenta varias desventajas. Una es la exigencia de homogeneidad espacial y poblacional: las instalaciones extensas, multizonas o con alto flujo de actores externos que son parte del sistema laboral y logístico para el funcionamiento de una instalación militar, rompen la pureza del diseño e incrementan el ruido organizacional, elevando el riesgo de rutina, habituación y descuido, ello se agrava cuando el recorte de personal obliga a cubrir espacios con individuos sin experiencia en seguridad, conllevando la perdida de competencias críticas.

Otra desventaja, ligada al actor interno (centinela), como se había tratado anteriormente, es el vector crítico, la fatiga, estrés, aislamiento, coerción del contexto en general, o las acciones cognitivas que lo hacen susceptible a cooptación por actores externos. Según du Cluzel (2021), la guerra cognitiva busca corroer la confianza y manipular decisiones individuales con bajo costo; cuando la arquitectura confía todo al ojo humano, un solo fallo puede anular anillos enteros de control.

En síntesis, el panóptico clásico, que establece al individuo como centro de gravedad, que socialmente se está perdiendo su figura para aportar a la seguridad, su costo económico es elevado y creciente, establece un actor interno que de acuerdo a la mutación de las guerras, es de fácil manipulación y cooptar su emociones y respuesta en la toma de

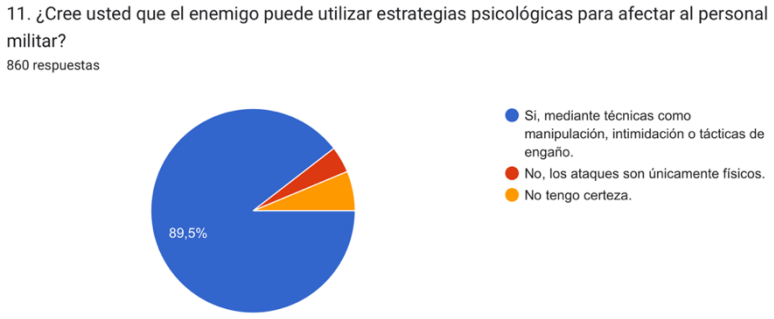
decisiones que pueden ser sesgadas y ponen en riesgo la protección de instalaciones, el poder y la autoridad que se incrementa si se presentan acciones coercitivas por parte de los actores internos en sus patrullas o interacción indirecta con los actores externos.

Entre los hallazgos de la encuesta se observan factores que dejan ver la vulnerabilidad de este panóptico, se reconocen los riesgos más probables para la seguridad como los ataques externos y la intrusión desglosando su limitación estructural, pero es el actor interno con sus acciones el que entra a jugar un papel relevante, teniendo en cuenta que no son las acciones directas del actor externo las que ponen en riesgo la seguridad, y que llevan al fortalecimiento cognitivo del actor interno.



La gráfica permite una lectura crítica del concepto del panóptico clásico, si se analiza las responsabilidades del actor interno como centro de gravedad de este panóptico, un 63,3 % de los encuestados consideran que el error humano (descuido centinela), y un 55,9 % (falla en el procedimiento), riesgos clásicos de este panóptico. De acuerdo con Foucault, está vigilancia busca producir individuos disciplinados, sin embargo, estos datos evidencian que la supervisión no garantiza la autovigilancia perfecta, el error humano persiste.

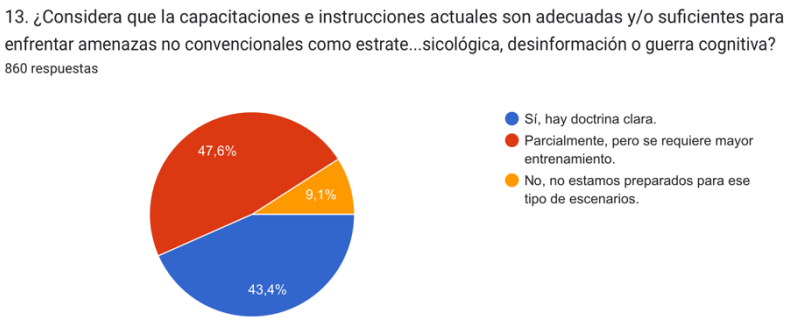
La presión psicológica, aunque baja con un 26,3 %, debe ser conectada con la siguiente pregunta.



Para el 89,5 % del actor interno, el enemigo puede usar estrategias psicológicas para afectarlo, por ello, la vigilancia física no protege al individuo frente a las manipulaciones cognitivas, configurándolo como el riesgo más latente y se aleja de considerar a la estructura panóptica como eje fundamental de la protección.

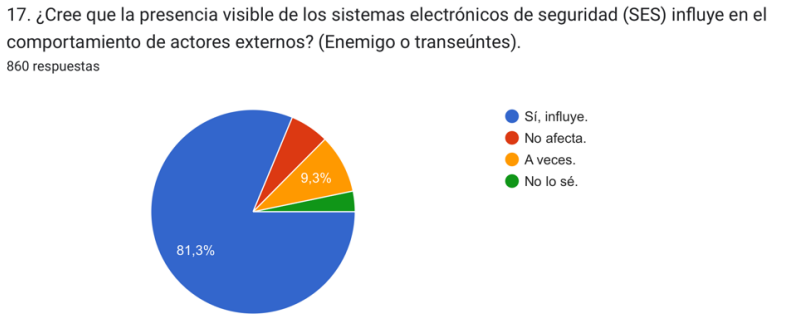
Los efectos subjetivos que genera este panóptico relacionado con la constante vigilancia y el uso del individuo genera un estado de hiperalerta, ansiedad o inhibición de la autonomía, lo que provoca desregulación emocional como vulnerabilidad principal para entornos de amenazas híbridas.

Este análisis integrado establece una brecha muy grande que afecta al actor interno, el cual se encuentra expuesto a la guerra cognitiva, por lo anterior y analizando la siguiente pregunta este panóptico genera una condición doctrinal que se debe tener en cuenta para fortalecer al actor interno.



Los resultados de la pregunta 13 muestran que más del 56 % considera que la preparación actual no es adecuada para afrentar este tipo de amenazas; esta disonancia evidencia una brecha crítica entre la percepción de la amenaza y la capacidad institucional respuesta formativa y doctrinal, para preparar emocionalmente al actor interno en escenarios donde el enemigo ataca su percepción, juicio o estabilidad psicológica.

La vulnerabilidad de este panóptico puede gestionarse con el uso de las nuevas tecnologías, la siguiente pregunta muestra el concepto del actor interno en el uso de los SES.



El 81,3 % considera que la presencia visible de los SES puede influenciar en el comportamiento de los actores externos, esto confirma la eficacia simbólica de la

arquitectura panóptica, el actor externo, al saberse potencialmente observado, ajusta su conducta, ello valida el principio de disuasión, materializando la traducción practica del panóptico en la protección. La visibilidad de la vigilancia produce autocontrol en el actor externo, reduciendo riesgos sin necesidad de intervención directa de la defensa y la resiliencia operativa de estos sistemas contrarrestando las debilidades del individuo.

5.2. *Panóptico digital*

El panóptico digital es la extensión tecnológica del panóptico clásico, según José Valencia (2017) como una herramienta que todo lo ve, gestionando riesgos y generando análisis del contexto; ejerce vigilancia y control de datos, actuando como soporte de una misma racionalidad de control distribuido; en términos de Foucault, sentirse observado, sin ser observado, reconfigura los sistemas electrónicos de seguridad que producen efectos disciplinarios sin contacto físico.

Su naturaleza a diferencia del panóptico clásico es la tecnología, proporciona un esquema de seguridad en profundidad realizando una cobertura total y una evidencia que nos muestra todo lo sucedido después de una acción contra el sistema de protección; con este panóptico se consigue vigilar, detectar, alertar y registrar eventos de seguridad.

El gasto operacional en este panóptico se catalogado como gasto de capital (o CAPEX, Capital Expenditure), que son considerados una inversión a largo plazo para mejorar las operaciones y con una reducción en sus gastos de operación anual. Está inversión puede considerarse alta por la tecnología adquirida, la cual se reduce en el tiempo y su gasto operacional es bajo por la reducción del actor interno que interviene en este panóptico, si bien es un individuo debe ser capacitado y entrenado; el costo de

entrenamiento no es alto pero su resultado operacional es importante para la operación de este panóptico, esta economía se consolida cuando los procesos de detección y registro se automatizan y la vigilancia rutinaria deja de depender exclusivamente de los centinelas.

En un ejercicio técnico realizado por la Subdirección de Sistemas Electrónicos de Seguridad de la Jefatura de Tecnologías de la Información y Comunicaciones para cuantificar el costo de un SES, se simula un perímetro aproximado de 600 metros, que es el alcance qué proporciona este sistema fotovoltaico; se conectó todo el conjunto de sensores para generar un perímetro de seguridad, y se calculó su operación, mantenimiento, cambio de equipos por vida útil por un periodo de cinco años, el CAPEX fue de aproximadamente $2.184.304.200, con valores de el año 2025.

En la creación de un ecosistema de protección de instalaciones la seguridad holística debe considerarse para mantener un ambiente de auto seguridad y aislamiento. Así, en este ejercicio se parte de la base de una estación fotovoltaica, que permite al sistema desconectarse de la red externa; esta independencia eléctrica del SES logra reducir las vulnerabilidades de un ataque del actor externo.

Los avances tecnológicos en este panóptico han permitidos su asociación con la IA para la protección de instalaciones según Boris Saavedra (2024), la IA permite analizar grandes volúmenes de datos para detectar amenazas y activar una respuesta adecuada; incrementa la velocidad y eficiencia del ciclo detectar, decidir y actuar, en términos de estrategia es un multiplicador que reduce ventanas de oportunidad y aporta priorización del riesgo en centros de control.

Para François du Cluzel (2021), en este panóptico el control de la mente humana pasa a un segundo plano, los sistemas electrónicos al producir visibilidad y ser datos en red,

reduce su accionar sobre el sistema de videovigilancia, pero crea nuevos vectores de influencia sobre el actor interno y el externo. Es necesario hacer ver a los actores que la cobertura de este panóptico está más allá del área asignada para protección y están siendo observados en todo momento, generando disuasión efectiva al moldear su comportamiento, imponiendo conductas operacionales y minimizando la fricción con el actor externo, catalogándose como una acción cognitiva que al final puede incluir al actor externo como un agente más dentro del sistema de seguridad, aportando información más allá del perímetro de la instalación.

En la lógica benthamita, según Foucault (1980) basta una mirada para activar el poder, la certeza subjetiva de ser observado reduce la frecuencia de transgresiones y empuja a los sujetos a la conformidad, particularmente cuando la sanción es probable, rápida y proporcional, en entornos militares esto se traduce en menores intrusiones, manipulación de activos y acciones del actor externo.

También, la eficiencia disuasiva no proviene solo del número de cámaras, sino de la percepción de una vigilancia ubicua y de la trazabilidad de conductas: registro, análisis y memoria institucional, Foucault subraya que la supervisión y el archivo convierten a los individuos en objetos describibles y comparables, la trazabilidad ancla la disciplina y disminuye las ventanas de oportunidad del actor externo para configurarse una amenaza para el sistema.

Esa eficiencia exige una evaluación estratégica, que debe ponderar dos variables, certeza de detección y velocidad de respuesta, un panóptico digital bien configurado incrementa ambas al reducir zonas grises y habilitar respuestas en tiempo casi real; a

diferencia de la coerción, la vigilancia constante actúa como poder continuo que previene la materialización del daño.

Además de la evaluación constante, existe una gobernanza jurídica así como en el panóptico clásico, este panóptico cuenta con una regulación jurídica, unos procedimientos internos y al final capacitación de todos los actores. En Colombia, la Ley 1581 de 2012 regula el tratamiento de datos personales, definiendo principios de legalidad, finalidad, libertad, seguridad y confidencialidad; así como excepciones aplicables a bases de datos de seguridad y defensa, y de inteligencia y contrainteligencia. Esto habilita el tratamiento necesario para la protección de instalaciones, sin eximir del cumplimiento de principios y controles.

Asimismo, el concepto 101321 de 2023 del Departamento Administrativo de la Función Pública avala la instalación de cámaras en entidades públicas para fines de funcionamiento institucional, siempre que se respete la dignidad, la intimidad y proporcionalidad, para instalaciones militares este estándar refuerza la necesidad de criterios, avisos y protocolos de acceso a los datos.

En particular, los principios de veracidad, calidad, transparencia, acceso y circulación restringida, y seguridad obligan a diseñar arquitecturas de datos que minimicen el acceso no autorizado, impidan la exposición abierta en Internet y garanticen medidas técnicas, humanas y administrativas robustas, un panóptico militar que descuide estos principios erosiona su legitimidad y, a la larga, su eficacia.

En el plano penal, la Ley 1273 de 2009 tipifica conductas contra la confidencialidad, integridad y disponibilidad de datos y sistemas, en las instalaciones militares dicha cobertura refuerza el componente disuasivo al elevar el costo jurídico de

intentos de intrusión digital vinculados a circuitos de videovigilancia y control, pero también regula al actor interno para mantener una protección adecuada de los datos y sus usos y evitar caer en una represión digital.

Con estas bases jurídicas y afianzando los conceptos de Foucault, Sekulovski (2016) indica que estos dispositivos despliegan dos características, la primera, estos empoderan a las instituciones que operan este modelo de panóptico, y la segunda, constituye una nueva forma de poder sobre los individuos, configurando al panóptico digital, el control disciplinario y las normas regulatorias establecidas para la protección, como la columna vertebral para la seguridad y el control sociopolítico moderno.

Es así que este panóptico constituye una herramienta de gran valor estratégico, integra vigilancia continua, análisis conductual, algoritmos predictivos y cohesión institucional. Sin embargo, su efectividad depende del equilibrio entre vigilancia, libertad y preparación del individuo, de ahí que el diseño de políticas de seguridad deba incorporar tanto tecnologías como pedagogía del control, evitando excesos que pueden convertir al actor interno en víctima de la misma vigilancia que lo protege.

En este análisis de las varias ventajas que ofrece este panóptico solo se observarán dos, la primera tratada anteriormente que permite cobertura y evidencia, generando detección, alerta y registro, con una mejor trazabilidad probatoria; velocidad y estandarización, estableciendo analítica y reglas que reducen tiempo de respuesta y estandarizan procedimientos, también permiten incrementar fácilmente su tamaño tecnológico a un menor costo que instalar un puesto fijo de guardia.

La segunda ventaja, está relacionada con el uso de la IA, que permite analizar grandes cantidades de datos más rápido que el ser humano, reduce falsas alarmas y ayuda a

predecir patrones de intrusión, esta capacidad configura la torre del panóptico digital como un motor analítico más que un simple observador.

Pero también, se describirán dos desventajas, según Saavedra (2024) la primera relacionada con la eficiencia que ofrece este panóptico se vuelve un riesgo sistemático, vulnerable a ciberataques que pueden degenerar sensores y almacenamiento.

Otra desventaja, según el Instituto Español de Estudios Estratégicos (2018), está relacionada con la gobernanza y legitimidad, una vigilancia digital sin controles puede deteriorar esta percepción, debilitando cooperación y cumplimiento, el no tener procedimientos claros sobre cada situación relacionada con el panóptico y no cumplir con las normas establecidas por el Estado deteriora la legitimidad y gobernanza sobre el actor externo llevando a perder hasta su cooperación en seguridad.

Este panóptico presenta un desafío de equilibrio técnico entre visibilidad y privacidad, jurídico y político, aplicando las regulaciones por parte del Estado y las excepciones de seguridad y controles de acceso, las instalaciones pueden sostener este panóptico eficaz sin degradar derechos ni exponer innecesariamente datos sensibles.

En suma operacional y sin caer en triunfalismos, un panóptico digital bien gobernado disuade al elevar la certeza de disuasión, controla al estandarizar la conducta mediante la interiorización de la mirada y neutraliza al acortar el ciclo sensor y tomador de decisiones con la analítica e IA enlazada. En términos del objetivo, la evidencia teórica de Bentham y Foucault y la regulación colombiana y doctrinal, sustenta que bajo esos condicionantes esos sistemas son efectivos en el control y la neutralización de amenazas en instalaciones militares.

En una de las preguntas realizadas, relacionada con este panóptico arroja que el 79,4 % considera que los SES refuerzan la capacidad para actuar frente a una amenaza, lo que refuerza que la aplicación de estos sistemas no solo contribuye a la protección, sino que actúan como un apoyo en caso de ser requeridos en la defensa de la instalación ante una amenaza.

5.3. *Panóptico mixto*

La presente propuesta de un panóptico mixto reúne las nuevas tecnologías enmarcadas en la perspectiva del biopoder, el conductismo y la geopolítica, y se presenta una propuesta como un ecosistema de seguridad integral, sustentado en articulación doctrinal, principios estratégicos y tecnologías emergentes. Si bien en otros países el panóptico digital ha sido aplicado con énfasis en la integración de IA, big data y sistemas biométricos.

En Israel, por ejemplo, se han desplegado sistemas de vigilancia digital en torno a instalaciones militares y fronterizas, que combinan cámaras de alta resolución con algoritmos predictivos para anticipar intrusiones; China ha implementado un modelo panóptico digital en el que la vigilancia masiva, apoyada en redes 5G y reconocimiento facial, no solo protege infraestructuras críticas, sino que también se utiliza como herramienta de control poblacional; en Estados Unidos el Departamento de Defensa emplea tecnologías panópticas digitales en instalaciones militares, integrando sistemas de sensores, drones y satélites con la doctrina de Force Protection Effects para responder a amenazas híbridas y cibernéticas.

Estas experiencias muestran que el panóptico digital amplía significativamente la capacidad de vigilancia y reacción, pero también plantea retos en términos de dependencia

tecnológica, legitimidad social y vulnerabilidad cibernética; el caso chino evidencia los riesgos de convertir el panóptico digital en un sistema de control excesivo sobre la ciudadanía. Para Colombia, estas lecciones refuerzan la pertinencia del panóptico mixto, que, según Rivera-Páez (2019), aprovecha las ventajas digitales sin sacrificar la centralidad del ser humano ni la legitimidad democrática en la protección de instalaciones militares.

Este nuevo modelo representa un avance estratégico para la protección de instalaciones enfocado en la protección del componente físico del poder aéreo, espacial y ciberespacial de la FAC. Este enfoque responde a la necesidad de modernizar las capacidades de videovigilancia, control y respuesta ante amenazas en un entorno operacional cada vez más complejo y tecnológicamente desafiante.

Por lo anterior, se recurrirá al panóptico digital como eje principal del modelo y optimizando algunas funciones del panóptico clásico. Esta integración en proporciones donde la tecnología marca la seguridad y el ser humano la defensa, se busca obtener una seguridad basada en SES con equipos dotados de IA desde el sensor óptico para lograr abarcar un mayor control del área asignada y vencer las zonas grises que se pueden llegar a presentar con un panóptico clásico.

En la búsqueda de una mejor integración con los medios tecnológicos, se debe partir interpretando el concepto de biopoder introducido por Foucault, el cual redefine la forma en que un Estado ejerce control, ya no mediante la violencia física directa, sino a través de mecanismos que administran la vida y regulan las conductas colectivas, en la protección de instalaciones militares, este concepto crítico es indispensable porque desplaza la seguridad de una lógica reactiva hacia una lógica preventiva. En el panóptico mixto, el biopoder se expresa en protocolos que normalizan la cooperación social, en la capacidad de moldear

hábitos de vigilancia y en la legitimidad proyectada por la Fuerza Pública al articular su presencia con la comunidad.

Al biopoder se suma el complemento operativo como el conductismo de Skinner, al explicar cómo los comportamientos pueden ser moldeados por estímulos, en el ámbito militar, esto se traduce en entrenar al actor interno mediante refuerzos positivos, reconocimiento y confianza institucional, al actor externo con incentivos simbólicos, participación y reconocimiento social para fortalecer el flujo de información y cooperación. Este marco permite entender la seguridad no como coerción, sino como un proceso de aprendizaje colectivo que se integra al panóptico mixto.

Para ejercer el poder y la autoridad bajo el biopoder Foucault presenta su tríada de soberanía, disciplina y seguridad, soberanía expresada en la autoridad política; la disciplina, en la acción militar organizada; y la seguridad, en la gestión de riesgos con participación ciudadana.

Esta tríada vista desde el enfoque de la guerra de Clausewitz ofrece una integración con el contexto actual donde la política representa la dirección estratégica y la legitimidad del poder, las Fuerzas Militares constituyen el instrumento disciplinario y operativa y la ciudadanía simboliza la dimensión de legitimidad social y cooperación. Está tríada lejos de ser abstracta, se materializa en la gestión del espacio militar y en la necesidad de articular los distintos niveles del poder. La síntesis de ambas triadas ofrece una base conceptual sólida de un panóptico mixto que no solo vigila, sino que regula, disuade y legitima la acción militar frente a amenazas.

Para lograr este ecosistema hay que hablar del panóptico clásico y digital, el primero históricamente ha sido asociado con torres de vigilancia, centinelas y mallas de

seguridad, garantizando control directo pero con altos costos operacionales, el panóptico digital, en cambio despliega la tecnología, IA, drones y sistemas que amplían la cobertura con menores costos operativos a largo plazo, así, el panóptico mixto que se propone surge de la necesidad de fusionar lo físico con lo digital, equilibrando la inmediatez humana con la precisión tecnológica.

La organización espacial de este panóptico se estructura en tres anillos de seguridad, un anillo interior concentrado en la defensa inmediata, con barreras, sistemas de negación y una defensa capacitada y rápida, el intermedio incorpora sensores, IA y cámaras que aseguran la detección y demora, para un anillo exterior integrado por patrullas, drones, conectividad operativa, agentes de inteligencia, que generan disuasión y anticipación, ademas de cooperación ciudadana. Estos tres anillos articulados aseguran profundidad estratégica y redundancia en la defensa, así como una acción adecuada sobre el actor externo que nos proporciona el principal insumo para la seguridad materializado en la cooperación como resultado de la autoridad y legitimidad de la institución.

Como resultado del conductismo social, que este panóptico refuerza al moldear los comportamientos del actor externo próximo al perímetro de la instalación, este actor es invitado a participar en redes de información y vigilancia, reforzándose con capacitaciones sobre regulaciones y deberes, el refuerzo positivo consiste en la seguridad percibida, mientras que las Fuerzas Militares obtienen legitimidad y acceso a información valiosa, convirtiendo a este panóptico en un sistema de seguridad compartido.

Una decisión clave de esta propuesta es la no utilización de centinelas fijos en el perímetro, pues estos son vulnerables a ataques directos en respuesta a sus patrones previsibles, y también a los ataques cognitivos qué afectan al individuo indirectamente, en

su lugar se emplean sensores, patrullas equipadas y apoyadas con drones. Estas patrullas dinámicas garantizan la flexibilidad, reducen el riesgo de infiltración y evitan el desgaste de la vigilancia estática, reservando al personal para tareas de control y defensa.

La integración de nuevas tecnologías busca reducir el error humano mitigando los riesgos asociados a fatiga y toma de decisiones; favorece una respuesta rápida y coordinada en la búsqueda de mejores tiempos de respuesta y economía de fuerza, al permitir respuesta con los actores más cercanos a la situación de riesgo, interoperabilidad facilitando compatibilidad con sistemas aliados y optimización del talento humano, en búsqueda de un actor interno más capacitado y cualificado para fortalecer sus capacidades técnicas.

El componente digital por la acelerada evolución de tecnologías emergentes aplicadas a la seguridad y defensa; esta transformación no solo permite alinear las capacidades de la FAC con estándares internacionales, sino que impulsa la optimización de recursos y fortalecimiento de su infraestructura, así como la disponibilidad de soluciones duales adaptables al ámbito militar y civil.

Este panóptico mixto refuerza la cobertura mediante cámaras con IA, sensores térmicos y sistemas de análisis de patrones, y altavoces de red. A ello debe sumarse la integración con redes de videovigilancia de entidades públicas y privadas que, a través de un espejo de imágenes compartidas, permita ampliar la cobertura de la soberanía de la protección en un ecosistema urbano y territorial inmediato logrando una mejor seguridad en profundidad y ejerciendo la autoridad sobre el actor externo, logrando una innovación tecnológica con un monitoreo constante con trazabilidad y evidencia digital.

Todo esto ofrece un marco operativo para esta panóptico, articulado con la doctrina de la U.S. Air Force que aplica cinco efectos para la protección, disuasión mediante

visibilidad de patrullas, drones y una regulación clara, detección con sensores, sistemas anti drones, e IA y el sistema de altavoz de red, demora con obstáculos físicos y electrónicos, negación mediante controles de acceso y protocolos digitales, y demora con la intervención del actor interno capacitado para la defensa, estos efectos no son meramente técnicos, sino que aseguran la coherencia táctica y estratégica de la defensa.

La aplicación de esta doctrina evita la dependencia ciega de la tecnología, aunque los algoritmos pueden detectar patrones, la última decisión recae en el actor interno capacitado, que actúa con base en experiencia, doctrina, normatividad y procedimientos. Esta centralidad del factor humano en la derrota de la amenaza reafirma la soberanía estatal y preserva la legitimidad en el uso de la fuerza, elementos esenciales en un contexto democrático, incluida la derrota en la dimensión aérea mediante sistemas antidrones.

Para conectar este panóptico con el actor interno y la toma de decisiones dentro del proceso, de acuerdo con John Boyd (1996), se establece el modelo OODA (Observar, Orientar, Decidir Actuar) convirtiéndolo en el motor decisional del ser humano, los sensores, drones y patrullas alimentan la observación, la orientación se construye con análisis de IA y agentes de inteligencia, la decisión corresponde al centro de comando y control, comandado con un actor interno capacitado, con regulación y procedimientos, y con la suficiente experiencia para la toma de decisiones, el actuar se ejecuta con patrullas y unidades entrenadas para la defensa, este ciclo otorga rapidez, flexibilidad y capacidad de adaptación frente a amenazas híbridas.

Alineado con la doctrina de la Fuerza Aeroespacial Colombiana (2020), los principios de la guerra que se reflejan en este panóptico, la economía de fuerzas se alcanza al sustituir centinelas con patrullas, drones e información, la unidad de mando se asegura en

el centro de comando y control, con comunicaciones, red de información y toma de decisiones integradas; la seguridad se garantiza con vigilancia en capas; la sorpresa se materializa en respuestas imprevistas partiendo del ser observado sin ser observado, y la flexibilidad en la capacidad de adaptarse a amenazas hibridas, esto lo convierte en un sistema doctrinariamente sólido y estratégicamente adaptable.

Dentro de los principios del Poder Aéreo aplicado con el control centralizado y ejecución descentralizada, el mantener el control de los SES y todas las operaciones de seguridad y defensa permite explotar la velocidad y flexibilidad en la respuesta a las amenazas y defensa de la instalación, la sinergia como integración de los panópticos, contribuye a un resultado superior; la persistencia presentada dentro de la continuidad, adaptado al modelo OODA manteniéndose siempre observándose y orientado al dispositivo, la legalidad y legitimidad obtenida en el cumplimiento de la ley, normas y los procedimientos establecidos por la FAC para las actividades de video vigilancia y protección de instalaciones.

Al agregar un componente humano para inteligencia perimetral, se fortalece la seguridad en profundidad, su función es anticipar movimientos sospechosos, recopilar información y alimentar el OODA; estos agentes integrados con la tecnología convierten este panóptico en un dispositivo resiliente.

En el plano de costos, el panóptico clásico depende de OPEX elevado, mientras que el digital requiere CAPEX significativo; el mixto equilibra ambas dimensiones, invierte en tecnología para reducir carga operativa, pero mantiene presencia humana en patrullas, toma de decisiones y defensa, este equilibrio asegura sostenibilidad financiera y operativa, a la vez que garantiza legitimidad al preservar la centralidad del factor humano.

La incorporación de drones autónomos para la seguridad amplía el radio de acción de la seguridad, estos no solo patrullan y disuaden, sino que también pueden portar cargas útiles no letales como sistemas de iluminación, sirenas o interferencia electrónica. Su despliegue, combinado con patrullas, aumenta la capacidad de reacción y reducir el riesgo para el actor interno.

Su conexión debe estar orientada a un sistema de red interna y no depender de sistemas de internet o nubes que pueden llevar al sistema hacer vulnerables a ciberataques, debe contar con una infraestructura robusta e independiente que permita su interconexión, aprovechando una de las ventajas que nos ofrece el panóptico digital como es adicionar equipos y ampliar su operatividad con una reducción de costos.

Se debe lograr flexibilidad con su operación para que sea interoperable con sistemas ya existentes, en busca de una reducción de costos e inversión, pero sin perder su fin de brindar detección, alerta y archivo de la información.

Su dependencia a la red eléctrica, en un alto porcentaje es el talón de Aquiles de este panóptico digital. Esta vulnerabilidad es muy bien conocida por el actor externo que al lograr sabotear el sistema permitir incomunicarlo con el dispositivo, contar con sistemas de energía alternativas como estaciones fotovoltaicas otorga independencia y autonomía para su operación, lo cual también reduce el costo operativo de este panóptico.

Esta propuesta de panóptico mixto se encaminada a la protección de instalaciones militares enfocado en su soberanía territorial. Con esta propuesta se debe articular el sistema de control acceso a la unidad, controles a áreas restringidas y los demás sistemas con los que se cuenten internamente para lograr robustecer la protección de la instalación militar dentro y fuera de su perímetro.

6. Conclusiones

Las nuevas tecnologías de vigilancia digital representan una manifestación contemporánea del biopoder en escenarios estratégicos, donde la población es gestionada a través de sistemas de observación, algoritmos de predicción y mecanismos de regulación de conductas, en este sentido, el uso de las nuevas tecnologías permite de que las infraestructuras críticas en especial las instalaciones militares no solo sean protegidas físicamente, sino también reguladas simbólicamente mediante la construcción de conductas, percepciones y lealtades.

A partir de este enfoque, puede afirmarse que el biopoder se articula con el control tecnológico no solo en administración del individuo, sino también en la gestión de las acciones subjetivas; el control uno se ejerce desde las amenazas directas, sino desde la prevención y la trazabilidad patrones, en consecuencia, se verifica una mutación del poder disciplinario hacia un poder biotecnológico, donde el espacio geopolítico de la seguridad se configura desde la vida gestionada en tiempo real, habilitando nuevas formas de vigilancia preventiva, tal como se evidencia en los sistemas de ciberdefensa y videovigilancia integrados en zonas estratégicas.

Los sistemas panópticos aplicados a entornos militares han evolucionado hacia estructuras de vigilancia digital qué funcionan con lógica, amplia observación y análisis predictivo, en este marco, el panóptico digital, a diferencia del clásico de Bentham ya no necesita de un vigilante visible, sino qué se configura como una red distribuida de observación y registro autónomo qué permite detectar comportamientos atípicos, patrones de riesgo y vectores de amenazas en tiempo real.

Los resultados del análisis empírico (encuestas y doctrina) muestran que esta arquitectura digital se vuelve efectiva en la medida que logra integrar nueva tecnologías y protocolos de respuesta descentralizada, esto permite establecer efectos disuasivos, tiempos de respuesta reducidos, y una mayor resiliencia frente a ataques híbridos, tanto cibernéticos cómo físicos. A su vez, se evidencia qué la percepción de seguridad y control conductual mejora significativamente cuando los sistemas digitales son complementados con presencia humana en tareas de supervisión e intervención operativa puntual.

En contraste, el panóptico digital permite ampliar cobertura, reducir el OPEX y mejorar la decisión mediante algoritmos de la IA y drones, aunque su dependencia tecnológica puede generar riesgos en escenarios de ciberataques. La evolución confirma que la mayor efectividad surge de un modelo híbrido o mixto, donde lo humano y lo tecnológico se complementan, patrullas reemplazan centinelas fijos, drones amplían el perímetro de seguridad y la integración publico privada multiplica la capacidad de observación y respuesta.

De acuerdo con los hallazgos teóricos y empíricos se propone una estrategia integral de protección basada en un modelo de panóptico mixto, que articula nuevas tecnologías, análisis conductual y una toma de decisiones basada en el ciclo OODA, garantizando que el factor humano sea quien tome la decisión final, bajo el marco de disuadir, detectar, demorar, negar y derrotar. Este modelo debe considerar principios doctrinales claves como: disuasión inteligente, control descentralizado y resiliencia operacional adaptativa, alineados con la doctrina Force Protection Effects de la USAF.

Esta estrategia propone que la toma de decisiones este en manos de un actor interno capacitado y con experiencia, que actúe en un centro de comando digitalizado, con

autonomía para activar mecanismos de defensa escalonada. Esta arquitectura deberá incorporar protocolos de interacción con actores externos en una lógica de seguridad colaborativa, a su vez, se enfatiza la necesidad de diseñar entornos normativos y éticos qué regulen el uso de tecnologías emergentes.

Las anteriores conclusiones permiten afirmar que el uso estratégico de nuevas tecnologías en la protección de instalaciones militares no puede entenderse fuera de una lógica de biopoder y geoestratégica, donde la vigilancia, el control conductual y la respuesta adaptativa conforman un ecosistema de seguridad panóptica. El modelo propuesto de panóptico mixto, con efectos disuasivos y control digital descentralizado, responde directamente a los desafíos contemporáneos de las amenazas híbridas, al integrar mecanismos preventivos, respuesta ágil y una gobernanza basada en IA y humana coordinada. Esta estrategia permite alcanzar una superioridad situacional en el espacio de protección, sin recurrir exclusivamente al despliegue masivo del actor interno, sino activando un ecosistema estratégico inteligente, efectivo y sostenible.

7. Referencias

Agamben, G. (2014). *¿Qué es in dispositivo?* Buenos Aires.
ASIS International. (2012). *Protección de activos Seguridad Física.* ASIS International.
Bentham, J. (1980). *El panóptico.* Madrid: Ediciones la Piqueta.
Bodin, J. (1997). *Los seis libros de la República.* Madrid: Tecnos S.A.
Boyd, J. (1996). *The Essence of Winning and Losing.* U.S. Air Force.
Buzan, B., Wæver, O., & Wilde, J. D. (1998). *Security: A new framework for analysis.* Colorado: Lynne Rienner Publishers.
Buzan, B., & Wæver, O. (2003). *Regions and Powers The Structure of International Security.* New York: Cambridge University Press.
Congreso de Colombia. (2009). *Ley 1273 de 2009.* Bogotá D.C.: Departamento Administrativo de la Función Pública.
Congreso de Colombia. (2012). *Ley 1581 de 2012.* Bogotá: Departamento Administrativo de la Función Pública.

Congreso de Colombia. (2024). *Ley 2384 de 2024.* Bogotá: Departamento Administrativo de la Función Pública.

Cluzel, F. d. (2021). *Cognitive Warfare.* Obtenido de https://www.comciencia.br/wp-content/uploads/2022/11/Guerra_Cognitiva_Cluzel_OTAN.pdf

Dalby, S. (2002). *Environmental Security.* University of Minnesota.

Díaz, J. (2023). *Estudio prospectivo del reclutamiento de conscriptos para el sostenimiento efectivo, operacional y estratégico del Ejército Nacional de Colombia sobre el escenario 2042.* Bogotá: Tesis de Maestría Universidad Externado de Colombia.

Dávila, J. (2014). *El concepto de poder en las organizaciones: bases analíticas.* Obtenido de https://repository.eafit.edu.co/bitstream/handle/10784/2953/juanmanuel_davilaocampo_2014.pdf?sequence=1

Delgado, J. (2018). Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia. Murcia, España: Universidad Católica de Murcia.

Esposito, R. (2002). *Immunitas: Protección y negación de la vida.* Madrid: Amorrortu editores.

Esposito, R. (2004). *Bíos. Biopolítica e Filosofía.* Madrid: Amorrortu Editores.

FAC. (2020). *Manual-FAC-0-B- Público Doctrina Básica Aérea, Espacial y Ciberespacial -DBAEC- Quinta Edición 2020.* Bogota: FAC.

Feldstein, S. (2021). *The rise of digital repression.* New York: Orford University Press.

Foucault, M. (1980). El ojo del poder (Entrevista). En J. Bentham, El panóptico. La Piqueta.

Foucault, M. (1999). *Estrategias de poder.* Argentina: Ediciones Paidós Ibérica S.A.

Foucault, M. (2000). *Un diálogo sobre el poder y otras conversaciones.* Madrid: Alianza Editorial S.A.

Foucault, M. (2000). *Defender la sociedad.* Buenos Aires: Fondo de cultura económica de Argentina S.A.

Foucault, M. (2002). *Vigilar y castigar: nacimiento de la prisión.* Buenos Aires: Siglo XXI editores.

Foucault, M. (2006). *Seguridad, Territorio, Población.* Buenos Aires: Fondo de Cultura Económica.

Galic, M., T. T., & B.-j. K. (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, 9-37.

Hernández, B. G. (2017). La construcción bio/geopolítica de las Doctrinas de Seguridad Nacional. *Cadernos do CIM*, 61-69.

Instituto Español de Estudios Estratégicos. (2018). *Resiliencia: del individuo al Estado y del Estado al individuo.* Madrid: Ministerio de Defensa de España.

Loskyn, J. (2015). El panóptico digital. *Virtualia #30.*

Rivera-Páez, S. (2019). Oportunidades de mejora en la legitimidad de las Fuerzas Militares: análisis y propuestas. En F. K. Adenauer, *Fuerzas Militares de Colombia: nuevos roles y desafíos nacionales e internacionales* (págs. 209-237). Bogotá: En E. Pastrana Buelvas & H. Gehring (Eds.). Obtenido de ResearchGate: https://www.researchgate.net/publication/332447960

Saavedra, B. (2024). Infraestructuras críticas: Amenazas, retos y oportunidades de la Inteligencia Artificial y el Aprendizaje Automático. *National Defense University, Perry Center Occasional Paper*.

Sampieri, R. H., Collado, C. F., & Lucio, M. B. (2023). *Metodología de la Investigación (6ª ed.)*. México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Sekulovski, J. (2016). *The Panopticon Factor: Privacy and Surveillance in the Digital Age.* Obtenido de https://philpapers.org/archive/SEKTPF.pdf

Skinner, B. F. (1986). *Mas allá de la libertad y la dignidad.* Barcelona: Ediciones Martínez Roca S.A.

U.S. Air Force. (2023). *Air Force Doctrine Publication 3-10, Force Protection.* U.S. Air Force.

Valencia, J., & Marín, M. (2017). El panóptico más allá de vigilar y castigar. *Kavilando*, 511-529.

Wajcman, G. (2010). *El ojo absoluto.* Buenos Aires: Manantial.