SEGURIDAD EN LAS FRONTERAS: UNA REVISIÓN DE LAS TECNOLOGÍAS EMERGENTES APLICADAS A LA SEGURIDAD FÍSICA EN ZONAS FRONTERIZAS

ANA MARÍA HERNANDEZ CARDOZO

CÓDIGO DEL ESTUDIANTE:

D0700313

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE ESTUDIOS A DISTANCIA
PROGRAMA ADMINISTRACIÓN DE LA SEGURIDAD Y SALUD OCUPACIONAL
BOGOTÁ D.C.
2021

SEGURIDAD EN LAS FRONTERAS: UNA REVISIÓN DE LAS TECNOLOGÍAS EMERGENTES APLICADAS A LA SEGURIDAD FÍSICA EN ZONAS FRONTERIZAS

ANA MARÍA HERNANDEZ CARDOZO

CÓDIGO DEL ESTUDIANTE:

D0700313

NOMBRE DEL PROFESOR ASESOR DEL ENSAYO

ASESOR CARLOS ALBERTO ARDILA CASTRO

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE ESTUDIOS A DISTANCIA
PROGRAMA ADMINISTRACIÓN DE LA SEGURIDAD Y SALUD OCUPACIONAL
BOGOTÁ D.C.
2021

SEGURIDAD EN LAS FRONTERAS: UNA REVISIÓN DE LAS TECNOLOGÍAS EMERGENTES APLICADAS A LA SEGURIDAD FÍSICA EN ZONAS FRONTERIZAS

1. INTRODUCCIÓN

Según Zúñiga Rodríguez (2017) algunas fronteras presentan problemas sociales y desafíos que facilitan la prevalencia del delito transnacional mediante actividades como el tráfico de armas, uso y comercialización de explosivos, narcotráfico, contrabando, crimen organizado, secuestro y extorsión por parte de grupos delincuenciales que utilizan pasos clandestinos en áreas donde no existe presencia del Estado o influencia de la Fuerza Pública.

Esta situación ha derivado la necesidad de implementar mecanismos de control para incrementar la seguridad y la protección en las zonas fronterizas (Suárez, 2016a). Más allá de la ubicación de guardas de seguridad privada o contar con cámara de circuito cerrado de televisión o aplicación de técnicas de control de ingreso y salida de personal en la frontera, la tendencia es según plantean Griffiths Spielman & Toro (2020) hacia el desarrollo y uso de nuevas tecnologías para incrementar en nivel de control y de seguridad.

Con esto en mente, y en el marco de las competencias desarrolladas en el programa de Administración de la Seguridad y Salud Ocupacional y complementadas con los contenidos temáticos abordados en el Diplomado en Seguridad y Salud Ocupacional, es posible contar con una visión integral sobre la gestión tecnológica enfocada a la seguridad física; por tanto, se presenta la relevancia de desarrollar una revisión de las tendencias mundiales sobre las aplicaciones tecnológicas orientadas la seguridad en las fronteras, con el fin de aportar al debate académico sobre la importancia de las nuevas tecnologías para la administración de la seguridad en áreas de frontera.

El contexto de inestabilidad y volatilidad que presentan las fronteras ha requerido que los países adopten medidas de seguridad con el fin de garantizar el control en los pasos fronterizos autorizados y la restricción de circulación en zonas que pueden convertirse en pasos clandestinos. Teniendo en cuenta que la gestión de la seguridad en los últimos años ha estado mayormente apoyada en los desarrollos tecnológicos producto de la cuarta revolución industrial, desde este contexto los planteamientos que se pretenden abordar giran en torno a preguntas como ¿Cuáles son las nuevas tecnologías aplicadas a la gestión de la seguridad física en zonas de frontera? ¿Cuáles son los principales riesgos presentes en las fronteras? ¿Qué beneficios se generan en el uso de tecnologías emergentes para la seguridad fronteriza?

Para hacer un acercamiento a la solución de dichos cuestionamientos se establece el objetivo general orientado a realizar una revisión de las tecnologías emergentes aplicadas a la seguridad física en pasos fronterizos. Así mismo, para dar alcance a dichos objetivos, se contemplan los objetivos específicos enfocados a establecer los principales riesgos a la seguridad física en áreas de frontera, seguido de definir las nuevas tendencias tecnológicas más destacadas a nivel mundial y finalizando con la descripción del uso y beneficios de las tecnologías emergentes orientadas a la gestión de la seguridad en las fronteras.

En función de lo anterior se plantea la hipótesis: Existen nuevas tecnologías orientadas y aplicadas a la seguridad física en las fronteras, la cual se abordará de manera argumentativa a partir de los aportes de diversos estudios y autores que han generado conocimiento científico en la materia.

2. DESARROLLO

En este apartado se abordará lo concerniente a los riesgos a la seguridad física en zonas de frontera, así como la definición de las tendencias tecnológicas más destacadas a nivel mundial y se finaliza con el uso y beneficios de las tecnologías emergentes orientadas a la gestión de la seguridad en las fronteras.

2.1 RIESGOS A LA SEGURIDAD FÍSICA EN ÁREAS DE FRONTERA

Con la llegada de la globalización se genera una transformación de la dinámica mundial, se modifica el comercio, la economía, la cultura y diversos aspectos que alteran el orden nacional y su interacción con otros países. En este contexto se desarrolla un cambio también en el ámbito delictivo, dando lugar al crimen organizado como problema de primer orden, caracterizado en mayor medida por la prevalencia de actividades de los grupos criminales a nivel global. Esta problemática definida como Delito Transnacional es protagonizada por grupos del Crimen Organizado Transnacional (COT) en el cual se llevan a cabo acciones delictivas que constituyen un riesgo a la Seguridad y Defensa de los Estados (Barras, 2013).

Según las pretensiones delictivas procuran asentarse y llevar a cabo las actividades ilícitas en zonas urbanas, especialmente en zonas desreguladas o áreas de conflicto, entre estas áreas de fronteras donde la presencia estatal es débil, con fines de lucro económico para financiación de las organizaciones del COT (Badrán & Palma, 2017). Situación que ha generado la necesidad de incrementar las medidas de control y seguridad para reducir las amenazas emergentes en los pasos de frontera. Si bien, la lucha contra el delito transnacional requiere de un gasto en defensa que no todos los países están dispuestos o en capacidad de incurrir, aquellos económicamente solventes han optado por recurrir a la tecnología para incrementar la ventaja sobre los grupos del COT.

Ahora bien, en las zonas de frontera son evidentes problemas de intereses, percepciones y desafíos que debe asumir cada país de acuerdo con su política exterior y las condiciones de gobernabilidad y soberanía. Esta situación sumada a la poca formulación de políticas conjuntas entre los Estados en el marco de una cooperación regional dificulta la gestión de la seguridad, el comercio y el desarrollo en las fronteras.

De acuerdo con Suárez Piñeros (2017) debido a este entorno complejo las fronteras se han convertido en áreas de interés para la realización de actividades ilícitas del orden de delito transnacional, tales como el tráfico de armas, uso y comercialización de explosivos y precursores químicos, narcotráfico, contrabando, crimen organizado, secuestro y extorsión, para lo cual los grupos terroristas utilizan pasos clandestinos en áreas donde no existe la presencia del Estado y la influencia de la Fuerza Pública es casi nula y además, dadas las condiciones socioeconómicas algunos cuentan con el apoyo de la población civil que reside en estos sectores, bien sea por afinidad o por coacción dadas las pocas de oportunidades de desarrollo social y abandono gubernamental tiene que convivir con esta problemática (Rodríguez, 2007).

En tal sentido, los problemas que se han presentado debido a una seguridad débil y obsoleta en diferentes instalaciones, lo cual se suma a que en las últimas décadas se han incrementado los robos, los asaltos y criminalidad que afectan el bienestar de las familias y de la comunidad aledaña a las fronteras (Bernedo-López & Montes-Valdez, 2020), razón por la cual la seguridad física y tecnológica ha ido avanzando a nivel global y paralelamente con la incursión de las nuevas tecnologías (Pampa Chacchi & Lozano Picaza, 2020).

La seguridad física se asocia con la infraestructura e instalaciones de un espacio en particular. Cada edificio necesita una forma de mantener afuera a los invitados no deseados, y la mayoría de las organizaciones también deben restringir el acceso a ciertas áreas dentro de sus instalaciones, incluso a las personas que ya han sido invitadas a entrar. Debido a esto, debe adoptar un conjunto de medidas de seguridad con las cuales otorgar acceso a los servicios protegidos solo al personal autorizado, aquellos que han sido cuidadosamente (Bernedo-López & Montes-Valdez, 2020a).

En este sentido, las mejores y más viables estrategias de seguridad física utilizan tecnología y hardware especializado para lograr sus objetivos de seguridad. Proteger los activos de intrusos, amenazas internas, ciberataques, accidentes y desastres naturales, a su vez requiere una combinación de tecnología y monitoreo en persona que requiere una planificación cuidadosa y la colocación del personal de seguridad y otras tácticas.

2.2 NUEVAS TENDENCIAS TECNOLÓGICAS MÁS DESTACADAS A NIVEL MUNDIAL

La seguridad física siempre es un componente de una estrategia de seguridad más amplia, pero constituye una parte considerable de esta. Los expertos en seguridad coinciden en que los tres componentes más importantes de un plan de seguridad física son el control de acceso, la vigilancia y las pruebas de seguridad, que trabajan en conjunto para hacer que un espacio sea más seguro (Bernedo-López & Montes-Valdez, 2020a).

En cuanto a los mecanismos de protección de frontera van más allá de la ubicación de guardas de seguridad privada o contar con cámara de circuito cerrado de televisión o aplicación de técnicas de control de ingreso y salida de personal en la frontera, la tendencia es orientada hacia el uso de

tecnologías para incrementar en nivel de control y de seguridad, es recurrir a las herramientas disponibles en desarrollo tecnológico para orientar las labores de manera eficiente y contundente.

Un ejemplo de esto es el caso de la frontera entre Corea del Norte y Corea del Sur, el desarrollo científico y tecnológico desarrollado en Corea ha permitido implementar alternativas de seguridad para esta zona que durante muchos años fue de alta tensión en la Zona Desmilitarizada (DMZ), ahora Corea del Sur utiliza un ejército de drones armados como nueva estrategia para la seguridad de frontera (BBC, 2017).

Por su parte China ha decidido reforzar los niveles de seguridad y vigilancia en la frontera con Corea haciendo de una recién formada brigada de defensa fronteriza, utilizando drones además autos de patrullaje, drones y cámaras de alta tecnología para contar con información precisa, y disponible las 24 horas (CNN, 2017).

En respuesta, los estados occidentales buscarán tecnologías de "salto a adelante". para mantener la ventaja. Esto requerirá una mayor agilidad, y una mayor aceptación de los riesgos del desarrollo por parte de los gobiernos y los sectores de la defensa y la tecnología. Las integraciones de los desarrollos técnicos acelerados en organizaciones de defensa podrían ofrecer capacidades de transformación. Las nuevas tecnologías de tratamiento de la información mejorarán sistemas de seguridad y defensa. De hecho, la velocidad y el alcance de algunos los modernos sistemas de sensores ya superan el procesamiento humano capacidad. Es probable que se haga un mayor uso de la inteligencia artificial y el aprendizaje automático, a medida que los estados tratan de desarrollar (The International Institute for Strategic Studies, 2018).

Por lo tanto, la tendencia es a reemplazar el recurso humano por recursos tecnológicos que brinden mayor nivel de control y atención a las necesidades de seguridad en la frontera en tareas y actividades que representen alto riesgo para la integridad del personal, así mismo implementar los desarrollos tecnológicos al alcance para favorecer el control y monitoreo en las fronteras (The International Institute for Strategic Studies, 2018).

Así mismo, la tendencia es a utilizar nuevas capacidades de procesamiento técnico para aumentar los sistemas de seguridad comprimirán los tiempos de respuesta y pondrán más automatización de las defensas para minimizar el uso de la ventaja del primer golpe del adversario (The International Institute for Strategic Studies, 2018).

En la región, debido a la pluralidad sociopolítica y económica se viven diversas tensiones fronterizas, por tanto, ha llevado a los países de la región a implementar mecanismos de seguridad y control de las amenazas de delitos transnacionales. Un ejemplo de esto es Bolivia, debido a la problemática del narcotráfico planea implementar el uso de cámaras de seguridad y drones de vigilancia de la frontera, los cuales rompen la barrera de espacio y tiempo para aumentar la efectividad en las zonas más vulnerables, sin embargo, estos no reemplazan el componente de control de uniformados, por cuanto continúa teniendo en consideración la ubicación de puestos avanzados de control en zonas fronterizas con Chile y Perú (Hernández, 2019).

De otro lado, como parte de la estrategia tecnológica para la Seguridad Transnacional en la frontera ecuatoriana – venezolana también se ha planteado el uso de drones con tecnología robótica en 3D que permitan ejercer mayor control en dicha frontera, como parte de la cooperación transnacional para evitar la problemática de la insurgencia y grupos al margen de la ley que han usado la frontera como corredor específico para el logro de sus actos delictivos (Suárez, 2016b).

También se observan grandes esfuerzos en la frontera entre Estados Unidos y México debido al sensible conflicto y a las condiciones sociopolíticas en las que el país del norte especialmente durante el mandato de Donald Trump crear una serie de mecanismos para evitar el paso fronterizo no autorizado, además de la construcción del muro en las zonas de mayor vulnerabilidad, el país también ha acudido a la tecnología para la vigilancia y control en la frontera. Entre estos se encuentran el uso de torres, drones y aerostatos dirigibles unidos al suelo que pueden elevarse hasta 1500 metros, helicópteros con poderosos sensores infrarrojos y cámaras de video que también patrullan en las alturas (NY Times, 2017). En México han desarrollado potentes algoritmos de predicción para anticiparse al crimen, cuenta con una plataforma 34.000 bases de datos de más de 250 instituciones de gobierno, que ha contribuido a mejorar la inteligencia operativa criminal(Alvarado, 2018).

En resumen, en la región se hace uso de manera coordinada entre los recursos humanos y los tecnológicos para hacer frente a los delitos transnacionales que se filtran en las fronteras y que la autoridad de cada país ha implementado estrategias para frenar el paso de estos, bien sea de salida o entrada para de manera cooperativa aportar en la lucha contra los delitos transnacionales que afectan la región.

En el ámbito nacional también se destacan esfuerzos del Gobierno Nacional para la lucha contra los delitos transnacionales que enfrenta la región, especialmente en el caso de la frontera con Venezuela, por tanto, ha implementado el uso de vehículo aéreos no tripulados, es decir, drones para la supervisión de la extensa área de la frontera colombo – venezolana. Adicionalmente, ha hecho uso de drones para la seguridad fronteriza terrestre y marítima para operaciones con características de alto riesgo, de cubrimiento de amplias áreas y misiones de reconocimiento,

además utilizados para operaciones de inteligencia y otras como búsqueda y rescate (Sputnik, 2017).

Cabe destacar que en el país ya se han adelantado esfuerzos por desarrollar la tecnología de drones, un ejemplo de esto es el Proyecto Iris, adelantado por un Sargento Primero del Ejército Nacional, como iniciativa para desarrollar productos que se ajusten a las necesidades propias de la nación y la institución. Así mismo como estrategia para la seguridad ciudadana se cuenta con más de 2.700 cámaras de seguridad en ciudades de Barranquilla, Manizales, Bogotá, Armenia, Cali, entre otras (Falck, 2016), y se ha ido más allá, por cuanto se está utilizando la inteligencia artificial para agrupar cientos de denuncias, encontrando en cuestión de minutos, patrones y asociaciones criminales que antes eran imposibles de identificar (Alvarado, 2018).

2.3 USO Y BENEFICIOS DE LAS TECNOLOGÍAS EMERGENTES PARA LA SEGURIDAD EN LAS FRONTERAS

Proteger las fronteras del movimiento ilegal de armas, drogas, contrabando y de las personas, a la vez que se promueve la entrada y salida legal, es extremadamente esencial para la seguridad de las naciones. Una seguridad fronteriza efectiva promueve la prosperidad económica, la soberanía nacional y un mundo pacífico, especialmente hoy en día, en un mundo tan marcado por amenazas terroristas y actos criminales. Es así como, ninguna nación puede estar verdaderamente segura sin seguridad en las fronteras, porque las fronteras abiertas fácilmente atraen a los delincuentes con acciones dañinas y potencialmente amenazantes para el orden y la seguridad de los ciudadanos y la gobernabilidad (Raed Al-dhubhani et al., 2017).

Este contexto ha derivado la necesidad de implementar mecanismos de control para incrementar la seguridad y la protección en las zonas fronterizas van más allá de la ubicación de guardas de seguridad privada o contar con cámara de circuito cerrado de televisión o aplicación de técnicas de control de ingreso y salida de personal en la frontera, la tendencia es orientada hacia el uso de tecnologías para incrementar en nivel de control y de seguridad, es recurrir a las herramientas disponibles en desarrollo tecnológico para orientar las labores de manera eficiente y contundente

Así pues, se ha generado la tecnologización y la digitalización de las fronteras (Lalonde, 2019) para contrarrestar el aumento de las actividades terroristas en todo el mundo, a través del control y monitoreo de sus actividades y así ejecutar rápidamente el plan requerido en consecuencia. Con los avances tecnológicos existe cada vez una mayor necesidad de mantenerse a la vanguardia de las nuevas tecnologías a fin de mantener una ventaja frente a las organizaciones del COT.

En tal sentido y de acuerdo con lo expuesto por De Cubber et al. (2017) el uso de la robótica para la seguridad fronteriza se ha visto influenciado por el aumento espectacular de los últimos años en el uso de sistemas aéreos no tripulados o drones por parte de los gobiernos, los consumidores, no obstante y lamentablemente, también por parte de los terroristas y los delincuentes.

Tal es el caso de las aplicaciones en seguridad fronteriza basadas en enjambres de drones miniaturizados (Shaw, 2017), el uso de vehículos aéreos robotizados no tripulados o de drones para operaciones como la observación y la vigilancia ilegales y el tráfico de drogas, o incluso como vector de ataque. Por tanto, se están desarrollando varias modalidades de detección novedosas para hacer frente a la problemática en las fronteras para la detección individual con niveles satisfactorios

de precisión, generalmente se utiliza una combinación de enfoques. Un ejemplo de ello es el proyecto H2020-SafeShore, cuyo principal objetivo es cubrir las lagunas existentes en la vigilancia de las fronteras costeras, aumentando la seguridad interna mediante la prevención de delitos transfronterizos como la trata de seres humanos y el contrabando de drogas (De Cubber et al., 2017).

Así mismo, los robots están cambiando la forma en que los países desarrollan la estrategia de base militar para producir nuevos espacios topológicos de violencia (Shaw, 2017). Entre estos se destaca el sistema robótico de vigilancia espía inteligente basado en GPS usando el Raspberry Pi para la aplicación de seguridad y detección remota ideado por Saha et al. (2017) que consiste en un sistema robótico que está completamente controlado de forma inalámbrica a través de un navegador de Internet y aplicaciones androides. Este cuenta con una cámara se adjunta con una pinza, para que pueda ver el ambiente circundante, adicional un sensor ultrasónico y un módulo GPS, lo que ayuda a medir la distancia y a rastrear la de forma continua. Además, todo el sistema se implementa en frambuesa pi 3 que tiene el sistema operativo Linux y el lenguaje python es usado para escribir un programa de los varios periféricos de este robot sistema.

Otro factor a considerar en la seguridad fronteriza consiste en cómo los robots autónomos producirán sitios de seguridad y simultáneamente situaciones de violencia, lo cual está revolucionando el espacio de batalla (Shaw, 2017). Este es el caso del control distribuido de una red robótica para protección de una región contra los intrusos un algoritmo de control de movimiento descentralizado para el móvil robots para interceptar a un intruso que entre en la región protegida. El algoritmo se desarrolla en base a algunas reglas simples que son computacionalmente eficiente y fácilmente implementable en tiempo real (Savkin & Marzoughi, 2018).

Así mismo, el androide basado en robot inteligente para la seguridad fronteriza de Ramesh et al., (2019), un robot inteligente autónomo basado en Android para la seguridad de las fronteras, que identifica a los intrusos usando el sensor de movimiento PIR, alerta al personal de seguridad por e-mail usando GSM y captura la imagen de los intrusos usando la cámara Raspberry Pi en el dispositivo androide y enviar esta imagen al correo electrónico correspondiente usando androide aplicación basada en la aplicación.

Ahora bien, el crecimiento de los dispositivos de visualización 3D, como hologramas y la realidad virtual, es seguido por el aumento de la demanda de modelos 3D, presentándose una forma económica y directa de crearlos a través de la fotogrametría, un ejemplo de ello es el sistema Multi-robótico de Coordenadas para la toma y visualización de imágenes a través de la fotogrametría desarrollado por De Souza et al. (2017), siendo este un multirobot sistema capaz de tomar múltiples imágenes bidimensionales de un objeto para la posterior generación de una representación 3D de este objeto con beneficios de escalabilidad, aumentando seguridad y fiabilidad en la seguridad territorial.

De igual manera, es preciso resaltar otras opciones que si bien no son nuevos desarrollos, si representan mejoras de los dispositivos y sistemas ya diseñados, tal es el caso de los patrones de especificación de propiedades de las misiones robóticas, desde la ingeniería de software la especificación de la misión permite sintetizar, verificar, simular o guiar la ingeniería de software para robots a través de bloques de especificación reutilizables que pueden ser usados por los ingenieros para crear especificaciones de misiones complejas mientras se reducen los errores de especificación y el lenguaje diseñadores, creando ricos lenguajes de dominio específico para los robots móviles, incorporando nuestros patrones como conceptos de lenguaje (Menghi et al., 2018).

Del mismo modo, se presentan las aplicaciones orientadas a replicar la anatomía de algunos animales, especialmente insectos terrestres y voladores, unos ideados para moverse en entornos complejos evitando obstáculos capaces de detectar individuos, rescatar en situaciones de desastres y reconocimiento militar (Zhang et al., 2017). Así también son observables desarrollo de cyberinsectos pequeños robots de ensamble y robots voladores en el campo de la nanorobótica. Tal es el caso de desarrollo de Lei et al. (2018) cyberinsecto que replica la suave trayectoria 3D del abejorro volador mediante visión estereoscópica empleando *Extended Kalman Filter* (EFK) para lograr electrónica miniaturizada, sensores y cámaras para el monitoreo de grandes áreas. A su vez, otras aplicaciones que imitan la anatomía y capacidad de como el diseñado por Cai et al. (2019) inspirado en el rayo cownose, capaz de realizar movimientos tridimensionales de alta maniobrabilidad y cambiar entre modos de natación de forma rápida y sin inconvenientes, de gran utilidad para aplicaciones militares bajo el agua en entornos estrechos.

Otros aspectos que estas se orientan a la automatización de la toma de decisiones a través de la incorporación de modelos que utilizan complejas estructuras algorítmicas para la adaptación, la adopción de decisiones y la proyección de predicciones.

Así pues, una de las tendencias corresponde al uso de sistemas multiagente autónomos, es decir, con capacidad de decisión propia para actuar de acuerdo con cada amenaza o riesgo. La autonomía se está convirtiendo en un componente omnipresente y no crítico de los sistemas de armas, como el transporte, la navegación o vigilancia, y ya ha tenido un impacto en el uso de la fuerza militar por parte de naciones. Autonomía parcial en la navegación y las capacidades de vigilancia de drones, por ejemplo, ha sido decisivo en el rápido y extenso despliegue (Righetti et al., 2018)

Estos sistemas son ideados con la finalidad de vigilar, controlar y resolver situaciones de amenaza sin la necesidad de la intervención humana para la toma de decisiones en materia de seguridad y defensa. Sus objetivos están orientados a la verificación y validación y las operaciones y vigilancia (Kernchen, 2019). Están basados en una gran cantidad de datos y algoritmos desarrollados de manera tal que establezcan la toma de decisiones y las reglas de acuerdo con los propósitos y circunstancias de funcionamiento, e incluye la interacción humano-robot enmarcando la autonomía como una colaboración continua entre comandantes, soldados y computadoras (Leys, 2018).

Los sistemas de vigilancia pueden comprender unidades móviles que les permiten patrullar zonas o perímetros específicos. Estos robots pueden seguir rutas de patrulla determinadas de antemano por operadores humanos, o se puede dejar que enjambres de unidades móviles se organicen por sí mismos dentro de una zona determinada. En este último caso, las trayectorias de patrulla surgen en función de las interacciones de los robots con el medio ambiente (Brehm, 2017)

Estos sistemas incluyen la detección e identificación de los estados del entorno (mediante sensores), planificación y selección de acciones (en congruencia con la situación problemática), colaboración y negociación (intercambio de información con otros agentes de defensa), ejecución de acciones (incluye monitoreo de la ejecución, vigilancia de los efectos y ajustes de ser necesario) y aprendizaje y mejora del conocimiento (ajuste con respecto a los objetivos de seguridad y defensa)(Theron et al., 2018).

Ya se han desplegado capacidades autónomas de sistemas de seguridad con funciones autónomas, pero ninguno de ellos está actualmente seleccionando y atacando objetivos sin intervención humana directa. Un sistema de este tipo es el "*Super aEgis II de DoDaam*" desplegado en la Zona Desmilitarizada entre Corea del Norte y Corea del Sur. El sistema se

anuncia como capaz de detectar humanos a 2 km de distancia a la luz del día y a 2,2 km de noche. Según el fabricante, puede estar equipado, entre otras opciones, con una ametralladora de 12,2 mm, un lanzagranadas de 40 mm o un lanzador de misiles tierra-aire (Brehm, 2017). Un operador humano puede especificar el perímetro dentro del cual el sistema explora en busca de objetivos y el sistema, según se informa, tiene la capacidad de identificar, rastrear y destruir un objetivo en movimiento y emitir una advertencia a un objetivo antes de un ataque. La versión original tiene un sistema de auto-disparo, que le permite apuntar y atacar sin intervención humana, pero en la práctica actual un operador humano bloquea la capacidad de disparo del sistema.

Ahora bien, en el marco de la coyuntura actual dada por la emergencia sanitaria por cuenta del brote del denominado COVID-19 cobra especial importancia la orientación hacia la biovigilancia automatizada, esta es muy prometedora tanto para mejorar la respuesta de la salud pública a los brotes de enfermedades naturales como para reducir al mínimo las posibles víctimas de la utilización de armas biológicas. Los sistemas de biovigilancia recogen y analizan grandes cantidades de datos diversos en tiempo real procedentes de muchas fuentes para proporcionar a los gobiernos un aviso previo del brote de una enfermedad o del ataque con armas biológicas (Kernchen, 2019). La capacidad de prever y vigilar cuándo y dónde puede producirse un brote y cómo puede transmitirse un patógeno puede mejorar sustancialmente las estrategias de respuesta a nivel local, nacional e internacional.

Por su parte, el aprendizaje profundo, también conocido como aprendizaje estructurado profundo, es una clase de algoritmos de aprendizaje automático basados en redes neuronales artificiales, que ha dado resultados satisfactorios cuando se utiliza para realizar tareas que son difíciles para los métodos de análisis convencionales. Dentro de los límites impuestos por la disponibilidad de datos, los métodos de aprendizaje en profundidad se han ensayado con éxito para

mejorar la detección de anomalías y el rendimiento de la fusión de datos para subconjuntos de datos particularmente exigentes (Kernchen, 2019).

3. APORTES

El documento se abordó con el fin de estimar las nuevas tecnologías orientadas y aplicadas a la seguridad física en las fronteras a partir de una revisión sistemática de los estudios y autores que han generado conocimiento científico al respecto. Dentro de los principales aportes al campo del conocimiento y en el ejercicio profesional cabe destacar que dentro de los principales riesgos a la seguridad física en las áreas de frontera se destacan las actividades ilícitas relacionadas con los delitos transnacionales tales como el tráfico de armas, uso y comercialización de explosivos y precursores químicos, narcotráfico, contrabando, crimen organizado, secuestro y extorsión, para lo cual los grupos terroristas utilizan pasos clandestinos en zonas de frontera.

Así mismo, es preciso destacar que dentro de las nuevas tecnologías disponibles a nivel mundial que pueden ser implementadas para la gestión de la seguridad física en las áreas de frontera se predominan el uso de sistemas aéreos no tripulados, con enfoques hacia los drones miniaturizados, robots espías inteligentes, integración entre la robótica y el aprendizaje autónomo para el desarrollo de robots capaces de interpretar situaciones de amenaza y tomar acciones de control y seguridad de acuerdo con los algoritmos de programación para gestionar la seguridad física en las fronteras.

Estos desarrollos tecnológicos permiten adelantar actividades de control territorial, vigilancia costera y control de flujo de personas y vehículos en los pasos fronterizos para incrementar la seguridad en estas zonas. Así pues, el uso de sistemas aéreos no tripulados de manera integrada con la robótica autónoma puede ser un sistema de apoyo para reducir riesgos

como el tráfico de armas, el narcotráfico así como el uso y comercialización de explosivos o sustancias ilícitas, toda vez que, se encuentran en la capacidad de monitorear y detectar de manera oportuna los diferentes sistemas de ocultamiento que utilizan las agrupaciones del crimen organizado para el tráfico y contrabando de este tipo de elementos, que ponen en riesgo la seguridad y estabilidad de las naciones, cuyo paso de comercialización se presenta principalmente en las fronteras.

De igual forma, es de destacar el uso de hologramas y realidad virtual que apoyados en la fotogrametría desarrollan robots multisistemas para obtener imágenes bidimensionales y reproducirlas en imágenes 3D. Este tipo de tecnologías pueden ser una herramienta útil para afrontar la criminalidad, asaltos y robos que son actividades que prevalecen en las áreas de frontera, dando lugar a mayor control y supervisión por parte de las autoridades y el Estado.

De otro lado, destacan aplicaciones apoyadas en complejos algoritmos con capacidad de generar toma de decisiones, adaptación al entorno y realizar predicciones a partir de la integración de la información bien sea visual, auditiva o de movimiento. La autonomía de los sistemas incluye capacidades tales como la de vigilar, controlar y resolver situaciones de amenaza sin la necesidad de la intervención humana, incluyendo amenazas biológicas de enfermedades o armas biológicas.

Este tipo de desarrollos tecnológicos generan un importante aporte para el control de los riesgos en la frontera, especialmente los relacionados con el ingreso de personal no autorizado a áreas de alta sensibilidad para la seguridad, al permitir de manera un control 24 horas, 7 días a la semana, en relación con la circulación de personas y vehículos que puedan tener intenciones terroristas o de tráfico de drogas, contrabando o de personas, siendo estas algunas de las amenazas más prevalentes en los pasos de frontera.

A lo largo del documento también se incluyen tecnologías relacionadas con la utilización de imágenes, percepción sensorial y el reconocimiento de voz. Fue posible concretar información de desarrollos tecnológicos que los utilizan como elemento de entrada para apoyo de otras funcionalidades de los sistemas de seguridad, especialmente para aquellos que incluyen la robótica y el aprendizaje autónomo y profundo revisado con anterioridad.

Entre estas aplicaciones se destacan los sistemas biométricos, reconocimiento de voz, duplicidad auditiva, uso de sensores inteligentes, los cuales se incorporan como parte de sistemas de vigilancia para complementar desde diferentes fuentes de información los datos que muestran las condiciones del entorno y la caracterización de los individuos que se encuentran en este en el marco de la gestión de la seguridad física en las fronteras.

Dichos desarrollos tecnológicos resultan ser una fuente clave para la seguridad física en las fronteras, en especial para el control de ingreso y salida de migrantes, toda vez que, a partir de sistemas inteligentes de biometría, reconocimiento de voz e integración de imágenes será posible la identificación oportuna de individuos que sean buscados por las autoridades. Esto permite la alerta temprana de situaciones de riesgo en las que se involucren grupos terroristas, u organizaciones del crimen organizado dedicados al secuestro, extorsión u otras actividades ilícitas en las áreas de frontera.

4. CONCLUSIONES

A la luz de la información consolidada en el desarrollo del ensayo fue posible aceptar la hipótesis planteada: Existen nuevas tecnologías orientadas y aplicadas a la seguridad física en las fronteras, toda vez que fue posible hacer una revisión sistemática sobre los desarrollos

tecnológicos disponibles a nivel mundial que son susceptibles de implementar para la gestión de la seguridad física en las fronteras.

A su vez fue posible concluir que las principales amenazas a la seguridad física en las fronteras se encuentran directamente relacionadas con el delito transnacional a través de actividades tales como el tráfico de armas, uso y comercialización de explosivos y precursores químicos, narcotráfico, contrabando, crimen organizado, secuestro y extorsión que sumados a condiciones de seguridad débiles u obsoletas incrementan la vulnerabilidad en las fronteras.

Por último, fue posible concluir que la mayoría de los desarrollos tecnológicos incluyen de manera integrada las aplicaciones en cuanto a la robótica, la utilización de imágenes, percepción sensorial y reconocimiento de voz, junto con algoritmos de programación para el aprendizaje autónomo y aprendizaje de dichos sistemas. De manera diferenciada, las aplicaciones a nivel de robótica incluyen el uso masivo de sistemas aéreos no tripulados, algunos de estos replicando aspectos de la naturaleza como los enjambres con la finalidad de realizar reconocimiento de áreas o el control territorial en zonas de frontera. Así mismo, desarrollos basados en el uso de hologramas y realidad virtual que apoyados en la fotogrametría desarrollan robots multisistemas para obtener imágenes bidimensionales y reproducirlas en imágenes 3D.

También fueron evidentes desarrollos tecnológicos orientados integración de la información bien sea visual, auditiva o de movimiento para procesarla a través de algoritmos que ofrecen la capacidad de identificación de amenazas, predicción de riesgos y adopción de decisiones en función de la programación.

REFERENCIAS BIBLIOGRÁFICAS

Alvarado, N. (2018). *Tecnología contra el crimen: Entusiasmo con cautela y criterio*.

Barras, R. (2013). El crimen organziado transnacional: Mecanismos de lucha previstos en las estrategias de seguridad nacional. *UNISCI Discussion Papers, 35*.

BBC. (2017). *¿Por qué Corea del Sur usará un ejército de drones armados para enfrentar la amenaza bélica de Corea del Norte? - BBC News Mundo*.

Bernedo-López, J. N., & Montes-Valdez, A. U. (2020). *Empleo de la tecnología en la seguridad de la Escuela Militar de Chorrillos CFB - 2020*. Escuela Militar De Chorrillos “Coronel Francisco Bolognesi.”

Brehm, M. (2017). Defending the Boundary: Constraints and Requirements on the Use of Autonomous Weapon Systems Under International Humanitarian and Human Rights Law. *SSRN Electronic Journal*, *MAy*. https://doi.org/10.2139/ssrn.2972071

Cai, Y., Bi, S., Li, G., Hildre, H. P., & Zhang, H. (2019). From Natural Complexity to Biomimetic Simplification: The Realization of Bionic Fish Inspired by the Cownose Ray. *IEEE Robotics and Automation Magazine*, *26*(3), 27–38. https://doi.org/10.1109/MRA.2018.2861985

CNN. (2017). *China está reforzando su vigilancia en la frontera con Corea del Norte | CNN*.

De Cubber, G., Shalom, R., Coluccia, A., Borcan, O., Chamrád, R., Radulescu, T., Izquierdo, E., & Gagov, Z. (2017). The SafeShore system for the detection of threat agents in a maritime border environment. *IARP Workshop on Risky Interventions and Environmental Surveillance*, 6–9.

De Souza, A. R., Raad, R., Batista, M. R., & Romero, R. A. F. (2017). Coordinate multi-robotic system for image taking and visualization via photogrammetry. *Proceedings - 2017 LARS 14th Latin American Robotics Symposium and 2017 5th SBR Brazilian Symposium on Robotics, LARS-SBR 2017 - Part of the Robotics Conference 2017*, *2017-Decem*, 1–6. https://doi.org/10.1109/SBR-LARS-R.2017.8215328

Falck, F. (2016). *Cámaras versus drones: Las políticas públicas Latinoamericanas en la encrucijada. El caso de honduras y Colombia*.

Griffiths Spielman, J., & Toro, J. P. (2020). *Desafíos para la seguridad y la defensa en el continente americano 2020-2030*. Athenalab.

Hernández, C. (2019). *Bolivia empleará drones en la vigilancia de fronteras - Noticias Infodefensa América*. Infordefensa.

Kernchen, R. (2019). Artificial Intelligence and Big Data Analytics for Biodefence: Implications for Threat Assessment and Biosurveillance By Roman Kernchen 06 Dec Artificial …. *Schriftenreihe Des Eyvor Instituts*, *3*, 1–6. https://doi.org/10.34764/b5s2-f048

Lalonde, P. C. (2019). *Canadian Border Security: Examining Border Services Officer and Traveller Knowledge Concerning Interaction Narratives and Technologization Within the Windsor Borderland*. https://doi.org/10.1017/CBO9781107415324.004

Lei, Z., Zheng, N., & Ma, Q. (2018). Smooth 3D trayectory segmentation for flying insects. *Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*, 739–745. https://doi.org/DOI 10.1109/Cybermatics_2018.2018.00147

Leys, N. (2018). Autonomous Weapon Systems and International Crises. *Strategic Studies Quarterly, 12*(1), 48–73. https://doi.org/10.2307/26333877

Menghi, C., Tsigkanos, C., Berger, T., Pelliccione, P., & Ghezzi, C. (2018). Poster: Property specification patterns for robotic missions. *Proceedings - International Conference on Software Engineering*, 434–435. https://doi.org/10.1145/3183440.3195044

NY Times. (2017). *Más drones y cámaras en la frontera, mejor que el muro de Trump – Español*.

Pampa Chacchi, J., & Lozano Picaza, Á. (2020). *La tecnología de seguridad física y el sistema de seguridad en la Escuela Militar De Chorrillos "Coronel Francisco Bolognesi", 2020*. Escuela Militar De Chorrillos "Coronel Francisco Bolognesi."

Raed Al-dhubhani, Shehri, W. Al, Mehmood, R., Iyad Katib, A., Altowaijri, A., & Saleh, A. (2017). Smarter Border Security: A Technology Perspective. In *Border Security and Safety*.

Ramesh, B., Yuvaraj, ;, Shankarnag, ;, Pavan, ;, & Satwik, ; (2019). An Android based intelligent robot for border security. *International Journal of Computer Science and Mobile Computing*, *8*(2), 123–129. www.ijcsmc.com

Righetti, L., Pham, Q. C., Madhavan, R., & Chatila, R. (2018). Lethal Autonomous Weapon Systems [Ethical, Legal, and Societal Issues]. *IEEE Robotics and Automation Magazine*, *25*(1), 123–126. https://doi.org/10.1109/MRA.2017.2787267

Rodríguez, G. (2007). Futuros Desafíos de la Política de Seguridad Democrática en las Fronteras. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, *2*(1), 193–210.

Saha, S., Singh, A., Bera, P., Kamal, M. N., Dutta, S., Gorian, U., Pramanik, S., Khan, A., & Sur,

S. (2017). GPS based smart spy surveillance robotic system using Raspberry Pi for security application and remote sensing. *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2017*, 705–709. https://doi.org/10.1109/IEMCON.2017.8117239

Savkin, A. V., & Marzoughi, A. (2018). Distributed control of a robotic network for protection of a region from intruders. *IEEE International Conference on Robotics and Biomimetics, ROBIO 2017*, *1*, 1–5. https://doi.org/10.1109/ROBIO.2017.8324516

Shaw, I. G. R. (2017). Robot Wars: US Empire and geopolitics in the robotic age. *Security Dialogue*, *48*(5), 451–470. https://doi.org/10.1177/0967010617713157

Sputnik. (2017). *Narcos, militares y políticos todos subidos al boom de los drones en Latinoamérica - Sputnik Mundo*.

Suárez, L. (2016a). *Seguridad transnacional por medio de drones de última tecnología en las fronteras ecuatorianas y venezolanas*. https://repository.unimilitar.edu.co/bitstream/handle/10654/16022/SuarezPi%F1erosLeonardo2017.pdf?sequence=1

Suárez, L. (2016b). *Seguridad transnacional por medio de drones de última tecnología en las fronteras ecuatorianas y venezolandas*. https://repository.unimilitar.edu.co/bitstream/handle/10654/16022/SuarezPi%F1erosLeonardo2017.pdf?sequence=1

Suárez Piñeros, L. (2017). Seguridad trasnacional por medio de drones de última tecnología en las fronteras ecuatorianas y venezolanas. In *Blanco, Moleiro, Crisis Institucionales y Apoyo Militar 2000. p.87, p -256*. Universidad Militar Nueva Granada.

The International Institute for Strategic Studies. (2018). *The Military Balance 2018*.

Theron, P., Kott, A., Drasar, M., Rzadca, K., Leblanc, B., Pihelgas, M., Mancini, L., & Panico, A. (2018). Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. *International Conference on Military Communications and Information Systems*, 1–9. https://doi.org/10.1109/ICMCIS.2018.8398730

Zhang, Z., Zhao, J., Chen, H., & Chen, D. (2017). A Survey of Bioinspired Jumping Robot: Takeoff, Air Posture Adjustment, and Landing Buffer. *Applied Bionics and Biomechanics*, *2017*, 1–22. https://doi.org/10.1155/2017/4780160

Zúñiga Rodríguez, L. (2017). El concepto de criminalidad organizada transnacional: problemas y propuestas. *Revista Nuevo Foro Penal*, *12*(86), 62–114. https://doi.org/https://doi.org/10.17230/nfp.12.86.2