LAS AMENAZAS MULTIDIMENSIONALES EN UN MUNDO GLOBALIZADO: EL CASO ECUATORIANO

Mayo. de I Stalin Marcelo Barriga Carrera [1]

Resumen

El objetivo central de este estudio es analizar las amenazas multidimensionales, las amenazas híbridas y las amenazas persistentes avanzadas. El estudio hace referencia a su proliferación como consecuencia de la globalización, convirtiendo a Latinoamérica en la región más violenta. Se realiza una recopilación de respuestas ante estas amenazas y por último se estudia de manera específica el caso de Ecuador, demostrando su presencia en el sector político, social y económico del país.

Palabras clave: Amenazas híbridas, multidimensionalidad, cibernética, ciberespacio, seguridad.

Abstract

The central objective of this study was to analyze multidimensional threats, hybrid threats and advanced persistent threats. The study refers to its proliferation as a result of globalization, making Latin America the most violent region. A compilation of responses to these threats is made and finally the case of Ecuador is specifically studied, demonstrating its presence in the political, social and economic sector of the country.

Keywords: Hybrid threats, multidimensionality, cybernetics, cyberspace, security

[1] Academia de Guerra del Ejército
stalingradombc@gmail.com

DOI: https://dx.doi.org/10.24133/age.n15.2022.08
Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 15. Núm. 1 abril 2022. pp. 100 - 133

Introducción

En este trabajo desarrolla el tema de las amenazas multidimensionales, las amenazas híbridas y las Amenazas Persistentes Avanzadas (APT). Estas amenazas se expanden sin limitaciones, llegando al quinto dominio identificado en el espacio. Se han reconocido al narcotráfico, el crimen organizado, el terrorismo y la delincuencia como las amenazas de mayor impacto.

Por otro lado, se amplía su margen de afectación a cinco dimensiones: aire, tierra, mar, espacio y ciberespacio, generando una transformación de las amenazas tradicionales e incluyendo a la cibernética en su dominio, entrando en el contexto las (APT), que sin ser nuevas, han tomado un giro preponderante en los ciberataques y ciberespionajes a nivel mundial.

El análisis realizado demuestra la hipótesis sobre la generalización de las amenazas multidimensionales en Latinoamérica debido a la globalización que ha eclipsado las fronteras para otorgarse el calificativo de amenazas transcontinentales. Esta hipótesis se acopla a otra al confirmar las graves consecuencias económicas, sociales y políticas que estas están trascendiendo en el hemisferio occidental, no solo es un problema de seguridad sino también de gobernabilidad y de afectación a la democracia.

Bajo este contexto, el presente trabajo tiene como objetivo describir el alcance que cada país de la región le ha dado al término "amenazas multidimensionales", realizando un análisis de los Libros de Defensa Nacional de los países de la región latinoamericana. Se hizo un estudio teórico del significado de amenazas híbrida con el fin de relacionar su multidimensionalidad, para finalmente proceder con la investigación de las Amenazas Persistentes Avanzadas, esto permitió comprobar la hipótesis que confirma la relación existente entre los tres tipos de amenazas que afectan a la seguridad nacional.

Para esta investigación se trabajó con una orientación analítico-descriptivo-deductivo, al revisar los Libros Blancos de los países de la región, además se analizaron revistas relacionadas al tema y documentos emitidos por instituciones encargadas de atender la problemática de las amenazas híbridas. El cuerpo del trabajo está dividido en tres partes. La primera describe las amenazas multidimensionales. La segunda detalla la respuesta a las amenazas multidimensionales. Por último, en la tercera parte se hace un análisis de las amenazas multidimensionales en Ecuador.

I. AMENAZA MULTIDIMENSIONALES

Direccionando este concepto a la región latinoamericana, se enuncia en primera instancia el caso de Argentina, en cuyo Libro Blanco de Defensa de 2010 no se conceptualiza de manera explícita a la amenaza multidimensional, más bien; las declaran como nuevas clasificándolas en terrorismo, narcotráfico, crimen organizado, proliferación de armas de destrucción masiva y concesionales y de tecnología militar, el tráfico de armas, el medioambiente y la competencia por los recursos no renovables, es decir, amenazas son todas aquellas que afecten a la integridad de los Estados, a las instituciones y personas por el aumento de la permeabilidad de las fronteras, calificándoles como "fenómenos de comprensión multidimensional que afecta a la problemática de la seguridad" (Ministerio de Defensa - Argentina, 2010, pág. 21).

En la Estrategia Nacional de Defensa de Brasil publicada en 2008, las Fuerzas Armadas no identifican amenazas militares concretas, es su deber estar preparados para la defensa y desempeñar, multiplicidad de misiones en diversas áreas y escenarios. Sin embargo, en el Libro de Defensa Nacional de 2012 señala a las amenazas multidimensionales como un peligro para su seguridad, focalizándolas en el tráfico de armas, narcotráfico, piratería y crimen organizado (Ministerio de Defensa - Brasil, 2012).

Por su parte Chile, en el Libro de la Defensa Nacional de Chile del 2017 manifiesta que "América encara un conjunto multidimensional de riesgos y amenazas, y están presentes una pluralidad de actores estatales y no estatales (…) " (Ministerio de Defensa Nacional - Chile , 2017, pág. 87), al igual que los otros países de la región, Chile identifica al narcotráfico, a la trata de personas y al tráfico de armas, aunque con una intensidad y tratamiento disímil en cada región y Estado. Otro punto fundamental es la globalización, con sus complementos reconocidos en la generalización de las amenazas multidimensionales causadas por la pobreza multidimensional y la corrupción.

Declara a la seguridad humana como principal enfoque de los tres pilares del Sistema de Naciones Unidas cuyo objetivo es proteger a las personas de las amenazas multidimensionales basando sus procesos en la fortaleza y aspiraciones del ser humano a una vida más digna.

En este documento chileno se refina el concepto de multidimensional y se establece que este enfoque "incorpora nuevas dimensiones al análisis de los ámbitos en que el Estado extiende su jurisdicción (…)" (Ministerio de Defensa Nacional - Chile , 2017, pág. 34). Se circunscribe el espacio ultraterrestre relacionado con la dimensión del ciberespacio, donde se generan múltiples formas ilegítimas e ilegales; las zonas fronterizas y las zonas aisladas y extremas son claves para la proliferación de estas amenazas y donde la defensa debe actuar; y, el tercer lugar es el Mar Territorial. La característica multidimensional de las amenazas se encauza a todo el territorio nacional y la visión integral de todas las dimensiones que pueden ser afectadas.

Chile, realiza en un capítulo específico al tema del enfoque multidimensional, al mismo tiempo aclara que, al aceptar el concepto explícito de Naciones Unidas

sobre las amenazas les conjetura con una "perspectiva integrada, multidimensional y amplia, esto no solo contribuye a mitigar el impacto de dichas amenazas, sino que también reduce el riesgo de que se conviertan en crisis de mayor alcance y más difícil solución" (Ministerio de Defensa Nacional - Chile , 2017, pág. 101) .

Colombia editó en 2003 la Política de Defensa y Seguridad Democrática catalogando a las amenazas como "un riesgo inmediato para la nación, instituciones democráticas y la vida de los colombianos" (Ministerio de Defensa Nacional, 2003, pág. 24) enumerando a los siguientes fenómenos: "corrupción, terrorismo, negocio de drogas ilícitas, tráfico de armas, municiones y explosivos, secuestro y extorsión y el homicidio. También destaca la presencia de amenazas de tipo transnacional, siendo estas la existencia de organizaciones armadas ilegales, el contrabando y el narcotráfico" (Ojeda, 2013, pág. 38).

Para Perú, la multidimensionalidad de la seguridad se fusiona en el espacio sudamericano con temas tan diversos como: "la pobreza, el terrorismo, el narcotráfico, la corrupción, la delincuencia internacional y otros" (Ojeda, 2013). Estos son factores que pueden debilitar la estructura social y que ahora se están convirtiendo en la principal y más activa "nueva amenaza" para el Estado y la sociedad. El terrorismo, el narcotráfico y el crimen organizado de carácter transnacional, cuyos modos de operación escapan al control del Estado-nación. (Minsiterio de Defensa -Perú, 2006)

En la Política de Defensa Nacional, Libro Blanco editado por el Ministerio de Defensa de Ecuador en 2018, menciona a la Declaración sobre Seguridad en las Américas de octubre de 2003 donde explica que: "la nueva concepción de la seguridad en el hemisferio es de alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupa-ciones y otros desafíos a la seguridad de los Estados del hemisferio" (Ministerio de Defensa Nacional, 2018, pág. 46).

1.1 Amenazas Híbridas

Las amenazas híbridas se caracterizan por el resultado de una cierta combinación de al menos dos amenazas diferentes, que pueden surgir de forma independiente o de al menos una amenaza y fenómeno de la misma categoría (Bartolomé, 2019). Combinan operaciones militares y no militares; actividades convencionales y no convencionales que pueden ser manejadas en concierto por actores estatales o no estatales para lograr objetivos políticos específicos.

Conforme a la proyección de la multidimensionalidad se incluyen las amenazas híbridas encajadas con la particularidad de "ciber", que etimológicamente indica "redes informáticas", que se desarrollan en el ciberespacio, aprovechado especialmente por los actores no estatales. Su proliferación ha ido acorde al desarrollo tecnológico, la competencia geopolítica o la polarización social, son muy disruptivas, están directamente relacionadas con los conflictos armados, el terrorismo, los ciberataques y el espionaje.

El Servicio Europeo de Acción Exterior (2019) considera que las campañas híbridas son multidimensionales e incorporan medidas coercitivas y subversivas, manejando herramientas y tácticas tanto convencionales como no convencionales. Están delineadas para ser difíciles de divisar o definir su estrategia, sobre todo apuntan a vulnerabilidades críticas y buscan causar desorden para dificultar la toma de decisiones rápida y efectiva, llegando a desestabilizar gobiernos.

Haciendo un análisis del concepto, se desglosan cuatro pilares: "los actores (y sus objetivos estratégicos), las herramientas aplicadas por los actores, los dominios que son su objetivo y las fases o actividades que cumplen los actores para completar el panorama de las amenazas híbridas" (Comisión Europea, 2021, pág. 11).

Un actor (estatal o no estatal), que tiene objetivos pero capacidad limitada o posibilidades limitadas para alcanzarlos, puede aplicar una variedad de herramientas a una serie de dominios para realizar un determinado tipo de actividad, con el fin de lograr una serie de objetivos y afectar al objetivo primordial y de su único interés (Comisión Europea, 2021).

El Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas identifica trece dominios objetivos de las amenazas híbridas: Infraestructura, Cibernético, Espacio, Economía, Militar y Defensa, Cultural, Social y la sociedad, Administración Pública, Legal, Inteligencia, Diplomacia, Política e Información.

Las amenazas híbridas pueden variar desde ataques cibernéticos a sistemas de información críticos, pasando por la interrupción de servicios críticos como el suministro de energía o los servicios financieros, hasta el socavamiento de la confianza pública en las instituciones gubernamentales o la profundización de las divisiones sociales (Servicio Europeo de Acción Exterior, 2019).

La cibernética es uno de los dominios en los que ocurren las amenazas híbridas, y el ciberespacio es un habilitador tanto de las operaciones cibernéticas como de las operaciones de información habilitadas por la cibernética. El Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas (2021) identifica tres tendencias actuales de amenazas híbridas en el dominio cibernético: "un aumento en el uso disruptivo de la inteligencia artificial; la expansión del papel del ciber en tiempos de crisis; y el crecimiento de las dependencias entre la política y la tecnología" (pág. 8). Estas tendencias son reconocidas desde el punto de vista de los desarrollos tecnológicos relevantes.

La primera tendencia citada como la inteligencia artificial (IA), identificada como la propensión tecnológica que afecta directamente al dominio cibernético, se vuelve más disruptiva por la accesibilidad

que ofrece, ya sea por la apertura del aprendizaje automático, así como por la cantidad de aplicaciones para solucionar todo tipo de problema, aumentado la productividad y la calidad del desempeño y mejorando la toma de decisiones. Sin embargo, la IA presenta su lado obscuro, con la actuación de irruptores disruptivos, cuyo objetivo es hacer daño, sacar ventajas económicas, espionaje, sabotaje o simplemente infligir daño.

Mientras más avanza la IA, la peligrosidad es mayor, la piratería informática automatizada envenena los datos, centrándose en las infraestructuras críticas de una nación. Se pone en riesgo, centrales eléctricas, sistemas de comunicación, transporte y logística, atención médica y la distribución de agua. El impacto es inmediato a la cotidianidad, a la seguridad social y a la economía.

"La IA habilitará mecanismos de guerra donde el "campo de batalla" se considera global. Simultáneamente, el factor humano en las operaciones disminuirá, lo que dará como resultado menos errores humanos, pero también potencialmente menos decisiones basadas en consideraciones morales" (Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas, 2021, pág. 10).

La IA microfocaliza el "segmento de influencia hiperperzonalizado" (HPIT por su siglas en inglés Hiper-personalized influence targeting) para alcanzar objetivos político, militares y geopolíticos. El ejemplo reciente de IA con un HPIT es el caso de las fuerzas rusas en Ucrania, realizando una combinación de equipos de guerra electrónica, drones comerciales, torres móviles falsas, combinaron las operaciones para sembrar desconfianza y daño psicológico en la población. La recolección de big data, otra herramienta de la IA que admite recolectar datos también permite diseñar y realizar HPTI a gran escala. China es un experto en recopilar datos de infraestructuras de los países occidentales, despliegues militares, opinión pública, así como información de personajes militares, políticos y comerciales influyentes en el mundo.

En la segunda tendencia se enuncia la cibernética en tiempos de crisis, no es difícil imaginar que apoyándose en cualquier crisis ya sea mundial o focalizada, el cibercrimen quiera aprovecharse con la falsa información, estos actores hostiles activan todos sus recursos y microfocalizan el segmento al que maliciosamente atacarán, o mejor dicho se aprovecharán de la situación para conseguir sus réditos.

Es fácil presentar este caso. La pandemia de COVID-19 aumentó cinco veces la posibilidad de ataques cibernéticos a hospitales y centros de investigación, cibersaboteando para extorsionar a través del robo de información. La gran mayoría de los países de la UE y EE.UU fueron el centro de ataque, la misma línea de competencia que involucró a las grandes farmacéuticas por crear la mejor vacuna, les volvió vulnerables para ser un segmento microfocalizado.

El crecimiento de las dependencias entre política y tecnología, es la tercera tendencia. Está demuestra el distanciamiento entre tecnología y política. Mientras que la primera está en una constante innovación, la segunda exige una reducción al ritmo vertiginoso que avanza la tecnología ajustándose primero a las políticas de manera disciplinada. La tecnología 5G implementada por la empresa China Huawei, ha causado la controversia si se puede adquirir esta tecnología y generalizarle, o sería una puerta de entrada para poner en riesgo la seguridad nacional del Estado.

El desarrollo de las tendencias actuales de amenazas híbridas en el dominio cibernético demuestran que la actividad en el dominio de la red por sí sola no constituye una amenaza híbrida, pero se cristaliza en una amenaza cuando un actor utiliza paralelamente varias herramientas y vulnerabilidades en otros dominios para lograr los mismos objetivos. La mayoría de las actividades de amenazas híbridas incluyen elementos de operaciones de seguridad cibernética y de la información.

Se presentan condiciones profundas que aumentan la importancia del dominio de la red para las amenazas híbridas. Primero, los Estados se desarrollaron sobre la base del rápido avance de la tecnología. Si bien esto ha beneficiado a los países en muchos niveles, también los ha hecho vulnerables a las amenazas en el ciberespacio. En segundo lugar, se ha desarrollado la capacidad de los estados y los delincuentes para operar en el ciberespacio; algunos son muy avanzados, mientras que otros son en su mayoría persistentes. Sin embargo, el número de ciberataques exitosos ha aumentado. En tercer lugar, el ciberespacio es el principal catalizador para la difusión de información a nivel mundial, por tal motivo este se vuelve endeble para las acciones del cibercrimen (Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas, 2021).

El concepto de amenazas híbridas, sin embargo, es el único que plantea el tema de las vulnerabilidades sistémicas de los sistemas democráticos como objetivos particulares y aboga claramente por un enfoque integral con cooperación civil-militar desde el principio.

Vale la pena señalar que la mayoría de los conflictos políticos y militares ahora tienen una dimensión cibernética. Esto enfatiza la creciente importancia del dominio cibernético para las amenazas híbridas no convencionales, ya que es particularmente empoderador para los Estados que no tienen la capacidad militar de las potencias más grandes.

De manera ilustrativa se cita el concepto chino de "Tres Guerras", para simbolizar la forma de pensar china, cuando se trata de la actividad que se ubica en el panorama de las amenazas híbridas en la literatura occidental. "El concepto se compone de Guerra Psicológica, Guerra de Opinión Pública y Guerra Legal, y se hizo oficial por primera vez en las revisiones de las Regulaciones de Trabajo Político del Ejército Popular de Liberación en 2003" (Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas, 2021, pág. 21) .

Las amenazas híbridas proyectan beneficiarse de las "vulnerabilidades de un país y suelen socavar los valores democráticos y las libertades fundamentales" (Comisión Europea, 2016, pág. 3). Lo dicho es muy acertado sobre todo en los países de latinoamericanos, donde el concepto de este tipo de amenaza se hace más palpable y de fácil conjugación entre los diferentes dominios y dimensiones que actúan constituyéndose en un asunto de defensa y seguridad nacional y de mantenimiento del orden público.

El surgimiento de amenazas híbridas presagia un desarrollo peligroso en las capacidades de lo que se denominó fuerza "guerrillera" en conflictos pasados. Pueden combinar fuerzas militares convencionales basadas en el Estado (armas sofisticadas, comando y control y tácticas de armas combinadas) con atributos generalmente asociados con organizaciones insurgentes y criminales.

Las amenazas híbridas se caracterizan por la combinación de fuerzas regulares e irregulares. Las fuerzas regulares se rigen por el derecho internacional, la tradición y las costumbres militares. Las fuerzas irregulares no están reguladas y, como resultado, actúan sin restricciones de violencia ni objetivos para la violencia. La capacidad de combinar y hacer la transición entre fuerzas y operaciones regulares e irregulares para capitalizar las vulnerabilidades percibidas hace que las amenazas híbridas sean particularmente efectivas (Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas, 2021).

Por lo expresado es responsabilidad de cada Estado identificar estos puntos frágiles que también pueden mezclase con redes transfronterizas, cambiando su estructura a niveles transcontinentales. Estos cambios son las características fundamentales de prevalencia lo que le hace a una amenaza híbrida difícil de contrarrestar.

1.2 Amenazas Persistentes Avanzadas

En el desarrollo de las amenazas híbridas, se pudo comprobar que dado el avance tecnológico mundial, estas amenazas se aprovechan de la vulnerabilidad de los países sobre todo en el ciberespacio, dando origen a las Amenazas Persistentes Avanzadas o APT por sus siglas en inglés, pudiendo estas estar presente por largos años sin ser identificadas. Las APT se asocian entre sí y forman grupos para una mayor eficiencia en el ataque.

Están conceptualizadas como:

> Un ciberataque sofisticado que suele lanzar los Estados o ciberdelincuentes avanzados, que obtienen acceso no autorizado a sistemas/redes informáticos y permanecen sin ser detectados durante un período prolongado. Estos grupos de amenazas cuyos ataques no se conciben de forma espontánea. Más bien, se planifican deliberadamente durante períodos de tiempo prolongados con objetivos específicos y consecuencias destructivas (Thales group, 2018).

Estos ataques están dirigidos a instituciones y organizaciones concretas "persiguiendo obtener acceso a largo plazo a una red, filtrando información y propagando el ataque a otros sistemas" (García, 2021). Los principales sectores de interés son: gubernamentales, defensa, infraestructuras críticas, industria armamentística, salud, centros de investigación, energía, telecomunicaciones, financieros, comercio internacional.

Se han podido detectar ataques al Parlamento noruego, a la Agencia de Seguridad Nacional de los Estados Unidos (NSA), contra objetivos militares, gubernamentales y diplomáticos en Ucrania, a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISSA) de EE.UU, Parlamento Finlandés, Parlamento Alemán entre otros.

El ciberdelincuente cuenta con una alta efectividad de sus técnicas de intrusión y de los tipos de ransomware utilizados que han superado las maneras de detección para ser contrarrestados, ni por las altas entidades de países desarrollados como EE.UU, no se ha librado del ataque de los grupos APT. Las acciones primordiales de los grupos APT en el ámbito militar son el ciberespionaje y el ciberataque. Con el fin de extorsionar los ataques provocados por actores estatales y no estatales son disruptivos, aplicando la extorsión a través de la publicación de información confidencial.

Otro accionar de estos grupos APT son la proliferación de noticias falsas y amenazas emergentes recurrentes, la información no contrastada, las advertencias mal interpretadas y las teorías de la conspiración generan confusión en la población facilitando el éxito del ciberataque.

Esta temática se pudo apreciar en los acontecimientos de octubre de 2019, mientras las FF.AA. trataban de mantener el control de la situación, los grupos sociales intervinientes transmitían información falsa que perjudicaba el accionar del Ejército.

El ciberespacio como entorno per se asimétrico es un dominio infinito con puntos inflexibles, con cantidades de actores y amenazas de igual particularidad, con semejanza también al concepto híbrido, Por una parte están los cibercriminales cuyo objetivo es básicamente económico, pero también están los políticos quienes la desestabilización del gobierno es su objetivo, en este grupo se encuentran los ya nombrados ciberespionaje y cibersabotaje con miras a la ciberguerra ocupando un terreno obscuro y con grupos de poder atrás de sus acciones.

Es conveniente referirse al cibercrimen, al ciberterrorismo y a la actividad de los grupos APT que comparten como característica, la inclusión dentro de su inventario de blancos están las infraestructuras críticas, ya mencionadas en párrafos anteriores. La eficacia de estos grupos en 2020 se lleva a pensar por los expertos que los ataques ya no son simples ransomware, sino grupos grandes de APT cada vez más sofisticados con técnicas de hackeo continuas, clandestinas, a través de

múltiples vectores, para accedes a un sistema, dañarlo y permanecer ahí durante un tiempo prolongado.

Para identificar el grupo de APT las empresas de ciberinteligencia les añaden un número o una identificación especial de acuerdo a lo que atañe su tipificación, así por ejemplo:

APT37 - Sospecha atribución: Corea del Norte. Su principal objetivo es Corea del Sur, Japón, Vietnam, Oriente Medio (Securityhacklabs, 2018).

El APT35 -Sospecha de atribución: Irán. Su objetivo, múltiples industrias de EE.UU., Arabia Saudita y Corea del Sur, Europa. Direccionado a personal militar, diplomático, gubernamental (Securityhacklabs, 2018).

En este punto se puede confirmar la intervención de los servicios de inteligencia de los países para actuar directamente o con la participación de organizaciones criminales que manejan los grupos APT.

Latinoamérica no se ha visto libre de estos grupos, se enuncia los casos de mayor afectación como el de México, atribuido el grupo de malkare Leetmx que afectó a México, Argentina, Costa Rica, El Salvador, Guatemala y Estados Unidos, se centró en el robo de información y espionaje.

En Brasil se descubrió un grupo de APT denominado Poseidón que venía actuando desde 2001, su objetivo estaba encaminado al sector privado y su característica era incluir el uso de conexiones por satélite secuestradas (Sec2crimen, 2021)

Es importante señar que Colombia ha hecho grandes avances en el desarrollo de mecanismos que permitan ejercer una labor eficiente de ciberseguridad y ciberdefensa frente a cualquier amenaza o incidente informático, pero el avance del entorno digital, sobre todo desde el 2019 con la proliferación de la pandemia de COVID 19 y el surgimiento de equipos y dispositivos para la interconexión existe inestabilidad y riesgos inherentes de seguridad digital que son difíciles de combatir, pudiendo resultar la culminación de amenazas y ataques cibernéticos.

Se concreta afirmando que la tecnología ha dado muchos giros en todas las dimensiones y dominios en los que una amenaza pueda actuar y la interoperabilidad de la población aporta con mayor acceso a que estas amenazas ya no sean solo en el campo de batalla sino en cada uno de los dispositivos que se instala, volviéndose una batalla general difícil de intervenir.

Los conceptos descritos pueden dar una sola denominación y decir que las amenazas persistentes avanzadas son las amenazas híbridas del ciberespacio, es decir una ciberamenaza híbrida. La conjunción de los conceptos se direccionan al ciberespacio para aplicar en su denominación el prefijo "ciber".

Con estos antecedentes, el concepto de seguridad deberá llegar a cubrir estas amenazas asumiendo también el rol de multidimensional. En décadas anteriores al avance tecnológico, la seguridad se limitaba a las acciones militares, cumpliendo con enfrentamientos entre Estados. En la actualidad la seguridad no solo se ha expandido a aspectos que no son estrictamente militares, sino que el concepto va hacia la supervivencia plena del individuo dentro de un habitat seguro. En este concepto el Estado debería ser el promotor de esta seguridad, pero también se escapa de sus manos dado el nivel de facilidades para la estructura de una amenaza.

Si se recapitula el concepto de amenaza híbrida, esta es la conjunción de dos o más amenazas, y si se traslada al ciberespacio, está se vuelve incontrolable. Se podría decir que para la seguridad también es necesario una hibridación, una mezcla de estrategias integrales, multidimensionales y cibernéticas.

Esperar de una seguridad total, llámese como se llame, sea esta integral, multidimensional o híbrida es imposible aludiéndose a la especificación de total. Este concepto viene cambiando de manera paulatina a las amenazas que el ser humano enfrenta y a la necesidad de adaptación a un entorno seguro.

II. RESPUESTA A LAS AMENAZAS MULTIDIMENSIONALES

Los atentados del 11 de septiembre de 2001 ocurridos en Estados Unidos, dejaron huellas que marcaron la seguridad mundial, consecuentemente la Organización de Estados Americanos convocó a una Conferencia Especial sobre Seguridad. Gracias a la colaboración de México se realizó el 27 y 28 de octubre de 2003, contando con la participación de 31 delegaciones, encabezada por 18 ministros, 19 delegaciones de países Observadores Permanentes, 24 organismos internacionales y representantes 17 de organizaciones de la sociedad civil (Organización de los Estados Americanos, 2003)

Dados los acontecimientos del 11/9, se establece un alcance multidimensional a las amenazas, explicando que "el concepto y los enfoques tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales" (Organización de los Estados Americanos, 2003, pág. 33).

En la Conferencia, se enuncian las amenazas que están en esta dirección: el crimen organizado, el narcotráfico, el tráfico de armas, entre otros, y se concluye afirmando que "estas amenazas constituyen nuevas y complejas amenazas que rebasan las fronteras nacionales, por lo que requieren de la cooperación de todos para enfrentarlas exitosamente" (Organización de los Estados Americanos, 2003, pág. 13).

Paralelo a esta Conferencia, la Unión Europea realiza una evaluación conjunta de las amenazas que atentan a su seguridad para establecer una Estrategia Europea de Seguridad (EES) adoptada desde diciembre de 2003. Este documento concibe una UE especialmente preparada para responder a situaciones con presencia de amenazas multidimensionales (Consejo de la Unión Europea, 2009).

En este documento, se manifiesta que la propagación de todo tipo de amenazas es consecuencia de "vecinos inmersos en conflictos violentos, los Estados débiles en los que prolifera la delincuencia organizada, las sociedades disfuncionales o las explosiones demográficas en las fronteras europeas, plantean problemas para la región" (Consejo de la Unión Europea, 2009, pág. 35).

Una solución expuesta en la EES recae en los "gobiernos soberanos, responsables de las consecuencias de su actuación y el compromiso compartido de proteger a sus poblaciones del genocidio, los crímenes de guerra, la limpieza étnica y los crimines contra la humanidad" (Consejo de la Unión Europea, 2009, pág. 8).

Un ejemplo perentorio de mencionar comprende los esfuerzos de Estonia desde 2007 para que se incluya a la ciberseguridad en la agenda de las organizaciones internacionales y regionales: UE, OTAN, ONU, OSCE, entre otros. El tema parte cuando el pequeño país báltico, fue víctima de los primeros ciberataques rusos, con características híbridas, alcanzó a bancos, medios de comunicación, organizamos gubernamentales y las redes informáticas colapsaron con mensajes basura e información falsa. El direccionamiento de los IP se ubicaba en Rusia, aunque no se comprobó eficazmente, informantes internacionales sugieren que las prueban confirman que el ataque se originó en el Kremlin y grupos criminales se aprovecharon de la situación para sumarse al ataque contra Estonia (McGuinness, 2017).

A consecuencia de estos ataques, el país incorporó a su política de seguridad nacional, la primera estrategia de ciberseguridad, con el fin de protección de infraestructuras de información crítica, volviendo un experto en ciberdisuación, como eje principal de la política de ciberseguridad (Pernik, 2021)

Para el 2008, la EES refuerza los factores que amenazan la seguridad europea y enumera a la proliferación de armas de destrucción masiva, el terrorismo, la delincuencia organizada, la ciberseguridad, la seguridad energética; y el cambio climático. El rumbo del problema con mayor impacto, radica en los países del Sur y su marcada pobreza y subdesarrollo, la mal nutrición, las pandemias, el fracaso económico, los malos gobiernos, como elementos de inseguridad o amenazas multidimensionales a la seguridad de los países del Norte. Esto se explica por la incapacidad del propio Sur para gestionar o salir de su situación, debido a sus niveles de corrupción que ahondan su situación, llegando a la pobreza multidimensional y un abandono de la población vulnerable (Consejo de la Unión Europea, 2009).

Esto es demostrable al citar el índice Gini cuyo valor demuestra la desigualdad salarial en una región. El de la UE es de 0.308, en comparación con el de Latinoamérica que se ubica en el 0.462, con nueve puntos por encima de los países que pertenecen a la Organización para la Cooperación y el Desarrollo Económico (OCDE) que demuestran el 36.5 del índice en referencia (Zúñiga, 2020).

Relacionando lo expuesto hasta el momento con lo dicho por Ojeda (2013) la noción de amenaza se diversifica e incluye nuevos fenómenos propios del desarrollo, pero también algunos de naturaleza militar. Con este razonamiento lo que surge es que el concepto de Seguridad se vuelva multidimensional" (pág. 17).

Se aprecia un debilitamiento de las amenazas militares o netamente de la intervención militar, difíciles de reconocer e identificar por su tipología especial, conexa a la globalización , donde las fronteras han desaparecido, "actúan con un alto grado de asociatividad y complementariedad, su grado de presencia deriva más bien de una percepción que de una constancia y; generan un efecto multiplicado en la sensación de inseguridad de la población, definiéndose como amenazas multidimensionales" (Ojeda, 2013, pág. 17).

La situación presente en la región demuestra que la conceptualización dada en la Conferencia de México consolidó el enfoque multidimensional, hoy en día se evidencia que esto no ha resuelto el problema. Banegas (2017) dice que la compleja situación de los países latinos frente al crimen organizado, terrorismo y narcotráfico no se ha resuelto "constatando la falta de una verdadera operatividad pragmática de estrategias y resoluciones, que doten de mecanismos que permitan con agilidad la toma de decisiones conducentes a asegurar la neutralización o combate a las amenazas multidimensionales" (pág. 12).

El periodista de la BBC Lizzardy (2022) explica que Latinoamérica, se ha convertido en la región más conflictiva del planeta, dentro de sus fronteras se han formado los grupos delincuenciales más controversiales, si es verdad que la lucha entre naciones como era el caso del problema limítrofe entre Ecuador y Perú que llevó años solucionar, o el problema de las Islas Malvinas, enfrentando a Inglaterra y Argentina; o Chile y Bolivia por una salida al mar para este última ya no son amenaza, pero todas estas se han transformado en la migración ilegal, la trata de blancas, comercio ilícito y lo peor, el narcotráfico y todas sus derivaciones.

Las llamadas amenazas multidimensionales, alcanzan todas las dimensiones en las que las FF.AA. puedan intervenir. Se complican más cuando estas se transforman en cibers, y peor aun cuando la fuerza de la naturaleza se ensaña y el medio ambiente está más en peligro atrapando al ser humano y llevándole a un mundo fragmentado

Es explícito decir que la seguridad es la base para el desarrollo de las sociedades y por ende, contribuirá en el desarrollo de un Estado. Con esta premisa la seguridad del Estado puede variar, creando una múltiple complexidad de opciones sobre los tipos de seguridad que ya se desarrollaran de acuerdo al incremento de las amenazas y sus diversificaciones.

Al reconocer estas situaciones, necesariamente nace el calificativo que requiera el concepto de seguridad, no solo permitiendo el desarrollo de nuevos tipos de

seguridad enfocados más a la protección del individuo que al Estado.

Con este criterio se aborda la seguridad ciudadana, la seguridad pública, etc. todas dentro de una seguridad integral multidimensional o simplemente seguridad multidimensional, como hace referencia en el Plan Nacional de Seguridad Integral 2019-2030 a las "dimensiones en las cuales se manifiesta las amenazas, peligros y factores de riesgo, dimensiones dentro de las cuales el Estado debe actuar con su estructura por su característica compleja" (Ministerio de Defensa Nacional, 2019, pág. 33). El desafío de esta seguridad es incluir todos los aspectos: políticos, económicos, sociales, de salud y ambientales, de ahí parte el carácter de multidimensionalidad.

Blackweel (2017) quien se ha desempeñado como Secretario de Seguridad Multidimensional desde 2010 dice que:

> El concepto de Seguridad Multidimensional, radica en su capacidad de ofrecer una visión coherente e integral del conjunto de las amenazas a la seguridad que las naciones y los ciudadanos deben enfrentar y la manera igualmente integrada y coherente de hacerlo (pág. 155)

El experto explica que los factores a tomar en cuenta como: las vulnerabilidades sociales, las fragilidades estatales e institucionales y los factores acelerantes del entorno, son determinantes para concretar una seguridad multidimensional.

Deshojando estos factores, las vulnerabilidades sociales en toda la región están intrínsicamente vinculada a los factores económicos, son el origen de la violencia y la delincuencia y son expandibles a regiones enteras.

El segundo factor identificado en la fragilidad estatal e institucional, está representado por instituciones ineficientes, con niveles altos de corrupción que inclusive se han extendido al sector privado. Estos factores refuerzan y empeoran las vulnerabilidades, acrecentando la delincuencia, la desconfianza y la insatisfacción de una democracia fallida originada en políticas poco éticas (Blackwell, 2017).

El incumplimiento del Estado y de Gobiernos sectoriales que dejan de proporcionar los servicios indispensables, la población se ve obligada a recurrir a alternativas ilegales o ilegítimas, acercándose a grupos que le ofrecen dinero, protección y justicia a cambio de estos negocios, formándose pandillas que arrasan con la seguridad de la población más sensible.

En el tercer componente están los factores acelerantes o desencadenantes donde la vulnerabilidad social es testigo de la fragilidad estatal llevando a la región al borde del abismo, influyendo de manera determinante el crecimiento de la delincuencia y sus graves inferencias. Estos factores pueden ser las pandillas, armas de fuego, drogas y bebidas alcohólicas y la economía informal (Blackwell, 2017).

El desarrollo de las capacidades criminales es divergente a las capacidades del Estado, lo que ha obliga a cada uno plantear su propia seguridad dando el enfoque que mejor se acople y que incluye la cooperación de las Fuerzas Armadas en la tarea de contención y represión del crimen y la delincuencia organizada.

Blackweel (2015) asegura que:

> El involucramiento de las Fuerzas Armadas en la represión del crimen ya es, sin embargo, una realidad en muchos países de la región y en algunos de ellos, como México o Colombia, ese involucramiento incluso ha significado cientos de bajas entre las filas de las Fuerzas Armadas, incluidos oficiales de la más alta graduación (pág. 156)

Para Blackwell el rol permanente de las FF.AA. en los temas de seguridad pública no es lo más aconsejable, tampoco se sugiere la militarización de la policía, sustenta su opinión en el criterio de la Comisión Interamericana de Derechos Humanos (CIDH) que diferencia las tareas de cada institución e insta a que no deben ser suplantadas mutuamente (Blackwell, 2015)

Blackwell (2015), argumenta que: "la solución al problema de la inseguridad no es necesariamente más seguridad, más policía, más tropas o una legislación más dura contra el crimen, sino más bien inversiones inteligentes en una seguridad más eficiente" (pág. 10).

Es interesante evidenciar en este trabajo la conclusión que plantea y nombra a la seguridad inteligente con estrategias hacia la prevención del delito, generar nuevos instrumentos de medición del éxito y la eficacia de las fuerzas policiales, al mismo tiempo expone que se debe satisfacer las siguientes condiciones:

- Un enfoque multidimensional e integrado de la seguridad
- Diagnóstico basado en evidencias,
- Políticas públicas basadas en las necesidades y capacidades nacionales y regionales
- La incorporación de las mejores prácticas
- Evaluación de los resultados (Blackwell, 2015, pág. 10)

III. LAS AMENAZAS MULTIDIMENSIONALES EN ECUADOR

Ecuador ha publicado tres Libros de la Defensa Nacional: el del 2002, 2006, dos Agendas Nacionales de Seguridad Interna y Externa del 2011, 2012, 2014 y 2017, hasta establecer la Política de la Defensa Nacional del Ecuador "Libro Blanco" 2018.

Este último tiene congruencia con la Constitución de la República del Ecuador 2008; la Ley Orgánica de la Defensa Nacional y la Ley de Seguridad Pública y del Estado; concibiendo la Política de Defensa Nacional, aprobada por el Consejo de Seguridad Pública y del Estado (COSEPE) y del cual se deriva la Directiva de Defensa Militar, instrumento que se publica el Comando Conjunto de las Fuerzas Armadas (CC.FF.AA.) y con el cual se inicia la Planificación Estratégica Militar e Institucional.

Para la conceptualización de amenazas multidimensionales, el Libro Blanco de 2018 se basa en los compromisos adoptados por la Conferencia Especial sobre Seguridad de México, especificando que "las amenazas, preocupaciones y otros desafíos a la seguridad son de naturaleza diversa y alcance multidimensional, el concepto y los enfoques tradicionales deben ampliarse para abarcar nuevas amenazas no tradicionales, incluyendo aspectos políticos, económicos, sociales, de salud y ambientales" (Ministerio de Defensa Nacional, 2018, pág. 46).

Otros documentos que amplían su perspectiva de las amenazas hacia un enfoque multidimensional para configurar sus estrategias de acción conjunta, se cita el Plan Nacional de Seguridad Integral 2019-2030, en relación a las limitaciones y competencias de las instituciones encargadas de la seguridad y defensa, y dice que:

> Para este propósito es condición sine qua non contar con marco jurídico que garantice el empleo efectivo de las unidades en sus diferentes niveles, y en las distintas dimensiones (tierra, mar, aire, espacio y ciberespacio); toda vez que el accionar de las amenazas surge desde la complejidad, sus técnicas y tácticas sustentadas en redes delincuenciales, con carácter multidimensional; y, que por no existir una delimitación territorial exacta que discrimine entre lo interno y externo, las capacidades y competencias de dichos órganos se verán obligadas a ser redefinidas (Ministerio de Defensa Nacional, 2019, pág. 98).

De este último se desprende dos aspectos importantes. El primero la necesidad de contar con un marco jurídico; y la redefinición de las capacidades y competencias de los órganos de seguridad Fuerzas Armadas y Policía Nacional, situaciones que hasta el momento no se han cumplido pasando a ser un escrito más.

Ecuador identifica al "terrorismo, narcotráfico y sus delitos conexos, crimen organizado, ciberataques, exploración y explotación ilegal de los recursos marítimos, delincuencia organizada transnacional" (Ministerio de Defensa Nacional, 2018, pág. 47)

El crimen organizado está identificado como amenaza a la seguridad nacional y regional, derivándose de este el narcotráfico y tráfico de personas y lavado de activos. Estas amenazas han obligado a establecer acuerdos con sus vecinos Perú y Colombia debido a su extensión transfronteriza. La frontera norte es la zona más vulnerable para el tráfico de drogas, armas y personas, extendiéndose al lavado de dinero e interconexión con cárteles de gran envergadura como el Cártel de Sinaloa (Pichel, 2021)

Uno de los puntos más vulnerables en la frontera norte es la franja de San Lorenzo en la parroquia de Mataje. La inestabilidad se evidencia con el inicio de asesinatos de miembros varias familias que habitaban en las riberas de los ríos San Miguel y Mataje a cargo de los Autodefensas Unidas de Colombia (AUC) y de los paramilitares incrementando el desplazamiento de poblaciones enteras hacia Ecuador. Estos acontecimientos provocaron la expansión del narcotráfico y del terrorismo dentro de territorio ecuatoriano (Villaverde, Ecuador-Colombia: una frotnera caliente y abandonada, 2018).

En esta franja llamada "zona roja" se movilizan los grupos armados, especialmente las disidencias de las FARC, aquí llegan los compradores de coca protegidos por los grupos armados, sin detenerse en fronteras invisibles, por el contrario, la misma rivalidad entre estos transcienden en la violencia y los ajustes de cuenta en Ecuador.

Todo esto ha provocado cambios sociodemográficos, culturales y económicos debido a esta incidencia de factores tanto endógenos como exógenos que repercuten en la seguridad de la parroquia Mataje.

Desde febrero de 2001 se presentaron casos de sicariato como el asesinato del teniente político de la parroquia de Mataje Milton Guerrero Segura, sus hermanos e hija, así como el ocurrido en 2003 a la familia Cortez, al parecer fueron ejecutados por un ajuste de cuentas por drogas o armas (LBE, 2018), lo que implica la escaza justicia que no llega a esta zona ya sea por pánico o por corrupción.

Un acontecimiento que demostró la presencia de una amenaza multidimensional, representada en el narcoterrorismo fue el perpetrado el 28 de enero de 2018 en el cuartel de policía de San Lorenzo, un artefacto explosivo causó su destrucción y el destrozo de 37 casas vecinas. El balance fue de 28 heridos leves y 576 personas tuvieron que abandonar sus viviendas. Este atentado se le atribuyó a Walter Patricio Artizala, alias Guacho, ecuatoriano originario de Limones ligado a las FARC desde 2007, que se supone que es el comandante del Frente Olivier Sinisterra (Castillo, 2021)

Los hechos con particularidades de terrorismo continuaron en la zona hasta el 20 de marzo en el que un explosivo ubicado al lado de la vía Mataje mata a tres infantes de marina y deja heridos a otros once, uno de los cuales fallece a los pocos días. Se trataba de una "bomba trampa" cargada con metralla. Desde el atentado de 1996, cuando las FARC habían emboscado a una patrulla del Ejército ecuatoriano en el río Putumayo, no había habido militares ecuatorianos muertos en ataques de los grupos insurgentes. (Villaverde, 2018)

El 25 de marzo del mismo año un equipo periodístico de El Comercio ingresa a la zona restringida de Mataje, conformado por el reportero Javier Ortega, Paúl Rivas como fotógrafo y el conductor Efraín Segarra se dirigen a Mataje con el fin de investigar un tema relativo al narcotráfico en la frontera entre Ecuador y Colombia. Al siguiente día empieza su labor investigativa, cruzan a Colombia en canoa donde son secuestrados por el Frente Oliver Sinisterra comandado por Walther Arizala, alias "Guacho". Luego de algunos días sin noticias certeras, el 11 de abril el FOS envía un comunicado en el que confirmaba la muerte de los periodistas y del chofer (Castillo, 2021).

Un caso icónico que demuestra la presencia de ciberespionaje es el caso de la Base de Manta. Se inicia como consecuencia del Plan Colombia, Ecuador se vió involucrado en actos provocados por grupos irregulares que afectaban a la población de la frontera norte. Para el pleno cumplimento del plan, Colombia y Estados Unidos negocian recibir el apoyo del ejército americano en acciones de apoyo para combatir al narcotráfico y la guerrilla.

Surge la idea de los Puestos de Operaciones Avanzadas (Forward Operation Location o FOL en inglés), su misión era:

> Brindar una respuesta rápida frente a los nuevos escenarios de guerra que generan las nuevas amenazas como son el narcotráfico, el terrorismo, el crimen organizado, etc. Estos puestos de operaciones avanzadas no requieren de un número significativo de efectivos militares y están conformados por personal altamente especializado (Vallejo, 2013, pág. 38).

Aparecen los detractores ante la presencia del ejército americano, temiendo otro Vietnam e involucrando más a Ecuador en los asuntos colombianos y fue visto como una amenaza en la región andina. "Manta formaba parte de las estrategias de control desarrolladas por el gobierno de los Estados Unidos con el objetivo de proteger sus intereses e inversiones militares y comerciales a nivel mundial" (Machado, 2008). La opinión de altos militares de la época que consideraban a la Base de Manta como los ojos y oídos del Plan Colombia, se contaba con sistemas integrados de inteligencia electrónica y proporcionaba datos de inteligencia en tiempo real.

> El 25 de noviembre de 1999 se publicó en el Registro Oficial No. 325 el Acuerdo de Cooperación entre el Gobierno de la República del Ecuador y el Gobierno de los Estados Unidos de América concerniente al acceso y uso de los Estados Unidos de América de las instalaciones en la base de la Fuerza Aérea Ecuatoriana en Manta para actividades aéreas antinarcóticos (Vallejo, 2013, pág. 55)

Durante diez años la intervención americana fue una realidad, con personal altamente calificado y equipos de alta tecnología para la época, se esperaba un mejor control de la inseguridad sobre todo en Manta, las aspiraciones del pueblo fueron otras, pero el objetivo del ejército americano era otro.

El 1 de marzo de 2008, el gobierno colombiano planea la Operación Fénix, incursionando el espacio aéreo ecuatoriano y bombardeando Angostura, causando la muerte de 22 guerrilleros y el segundo comandante de las FARC, Raúl Reyes, alias "tiro fijo", demostrando la inseguridad que afronta la vigilancia del espacio aéreo, marítimo y terrestre, así como la falta de capacidad de reacción de las entidades a cargo de la seguridad y defensa del país.

Las investigaciones realizadas por una Comisión determinó que la información de inteligencia estratégica fue procesada en el FOL de Manta. En informes de periódico internacionales se afirma que según el Washington Post las bombas inteligentes eran de fabricación estadunidense, el periódico de investigación afirmó que la Agencia de Inteligencia de Estados Unidos fue quién asesoró las acciones con un programa encubierto con el gobierno colombiano (Priest, 2013) .

A manera de conclusión se podría establecer la siguiente interrogante: ¿Por qué EE.UU no iba a realizar lo que hoy se llama ciberespionaje para alcanzar sus objetivos? siendo los productores de la mejor tecnología, Ecuador no iba a ser la excepción, para incursionar en el ciberespacio nacional y realizar el ataque en Angustura, según su conveniencia. En definitiva, el caso redactado hace alusión a la presencia de APT 14 años atrás.

Este fue el detonante para que el acuerdo de renovación del contrato con el FOL no se renovó. Opiniones como las de Mario Pazmiño, ex director de Inteligencia del Ejército aseguró que "la inseguridad, con la salida de la base, va a afectar a todo el proceso que se venía siguiendo por parte de EE.UU. en la región con relación al combate al narcotráfico" (Benitez, 2019). Para el experto, la salida del FOL venía de otros detractores de origen izquierdista y por las mismas FARC, al buscar beneficiarse con la salida de los americanos de territorio sudamericano para manejar el narcotráfico bajo su control.

Esto se puede comprobar en la escalada del narcotráfico en la región de la frontera norte, debido a las falencias de la policía colombiana y la DEA. El caso de Édison Washington Prado Álava alias "Gerald", detenido en 2017, habría montado una red internacional del crimen organizado, transportaba droga usando lanchas rápidas "go fast" con contenedores que la embarcaban en barcos nodrizas. En este caso, se involucró a miembros desde bajos niveles como guardias, conductores, servidores públicos, así como a políticos que incluían a personajes cercanos al expresidente Rafael Correa.

El avance de las amenazas es tan agresivo como una amenaza híbrida multidimensional. Así se podría calificar al ataque con drones al Centro de Privación de Libertad Zonal 8 donde están recluidos dos de los líderes del grupo delictivo Los Choneros. El conflicto híbrido por sus características trató de desestabilizar la seguridad del penal por un enfrentamiento entre carteles internacionales: los mexicanos Jalisco Nueva Generación y el de Sinaloa. El ex jefe de Inteligencia militar afirmó que los dos carteles tienen una estructura muy fuerte en el país (Voz de América, 2021), al punto que se ha vuelto una híbrida multidimensional extrema, peor aún al ser Ecuador atractivo para la logística y el tránsito de los estupefacientes (Voz de América, 2021). Este escenario no es aislado a los acontecimientos que han venido sucediendo en las cárceles del país causando más de 300 personas privadas de la libertad muertas de una manera extremadamente violenta.

Los casos presentados demuestran que Ecuador no esta libre de ningún tipo de amenaza multidimensional,

al contrario, su incidencia ha aumentado, así lo reporta el informe de la Policía al revelar que los niveles de violencia e inseguridad entre 2016 y 2021 duplicó su porcentaje. Para 2016 fue de 5,81 por cada 100.000 habitantes, y para el 2021 subió a 10.62 (El Comercio, 2021).

El Estado no va a poder combatir solo a este tipo de amenazas por tratarse de organizaciones complejas y trasfronterizas y esto requiere la colaboración de otro Estado fuerte y experimentado, que aporte con tecnología y capacitación al personal militar. A pesar de esto, el FOL no fue la solución, porque se extralimitaron sus capacidades que no estaban contempladas en el convenio, como fue el espionaje y su intervención para dar respuesta más a sus intereses que a los del país de acogida.

Conclusiones

El ataque a las Torres Gemelas marco una ruptura a la seguridad internacional, dándole el enfoque multidimensional a las nuevas amenazas y como respuesta a estas amenazas se reflejó la acogida de las naciones latinoamericanas a través de sus Políticas de Defensa Nacional con la publicación de sus respectivos "Libros Blancos"

El concepto de amenazas hibridas son comprendidas dentro de las amenazas multidimensionales y las amenazas persistentes avanzadas, son intrínsicamente ciber y por lo tanto deben ser tratadas como tales.

Las FF.AA. como responsables de la defensa y las instituciones encargadas de la seguridad en general, deben innovarse para responder eficiente y eficazmente a las situaciones cambiantes que se están presentando en los nuevos escenarios.

El concepto de multidimensionalidad está plenamente relacionado con la globalización y las amenazas tradicionales han pasado a ser integrantes de un grupo mayor, por lo que las FF.AA. en su rol protagónico como parte de la seguridad integral necesita de un rediseño de fuerza que permita potenciar sus capacidades hacia un escenario multinacional y cada vez más complejo de detectar.

El Estado debe revertir las vulnerabilidades sociales luchando por un cambio ético y libre de corrupción, trabajar por disminuir la delincuencia y violencia a través de un enfoque de equidad e igualdad social.

Como reflexión final, se debe conocer conceptual y estadísticamente la realidad de las amenazas multidimensionales, su conjunción con las híbridas y las APT, con el fin de articular políticas regionales y nacionales que ayuden a una colaboración conjunta para hacer frente a estas amenazas, solo una correcta evaluación permitirá su alcance dimensional.

Referencias

Consejo de la Unión Europea. (2009). *Estrategia Europea de Seguridad*. Bruselas, Bélgica.

Banegas, A. (2017). *Estrategias para combatir las amenazas multidimensionales en la región. Santiago*: Academia Nacional de Estudios Políticos y Estratégicos .

Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *Revista Latinoamericana de Estudios de Seguridad*(25), 8-23.

Benitez, S. (2019). ¿Ecuador HUB de las Drogas?: Cosntrucciones semánticas sobre el valor geoestratégico del Ecuador en la dinámica delictiva transnacional desde el 2009 hasta el 2016. Recuperado el 24 de enero de 2022, de https://repositorio.iaen.edu.ec/bitstream/handle/24000/5117/Tesis%20Silvia%20Ben%C3%ADtez.pdf?sequence=1&isAllowed=y

Blackwell, A. (2015). *La Policía que merecemos: Una Discusión para el futuro*. Wilson Center, 1-12.

Blackwell, A. (2015). Seguridad Multidimensional: Enfrentamiento nueva amenazas. *Seguridad, ciencia y defensa*, 153-158.

Blackwell, A. (2017). Enfoques stuacionales de la delincuencia y la violencia: *El caso de América Latina.* Wilson Center, 1-7.

Castillo, C. (2021). *El ataque al cuarte policial de San Lorenzo y el cambio estratégico del centro de gravedad a la frotnera norte ecuatoriana. Consecuencias en la seguridad de la frontera norte*. Recuperado el 14 de febrero de 2022, de https://repositorio.flacsoandes.edu.ec/xmlui/bitstream/handle/10469/17317/TFLACSO-2021CACL.pdf?sequence=2&isAllowed=y

Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas. (2021). *El futuro del ciberespacio y las amenazas híbridas*. Luxemburgo: Publications Office of the European Unin.

Comisión Europea. (2016). *Comunicación conjunta sobre la lucha contra las amenazas híbridas: Una respuesta de la Unión Europea.* Bruselas.

Comisión Europea. (2021). *El paisaje de las amenazas híbridas. Un modelo conceptual*. Luxemburgo: Publications Office of the European Union.

Dalby, C. (2021). Muchos comentarios y pocas pruebas: ¿carteles de México causan violencia en Ecuador? *Insight Crime*. Recuperado el 14 de febrero de 2022, de https://es.insightcrime.org/noticias/muchos-comentarios-pocas-pruebas-carteles-mexico-causan-violencia-ecuador/

El Comercio. (2021). La tasa de homicidios en Ecuador se duplicó en los últimos seis años. págs. https://www.elcomercio.com/actualidad/seguridad/homicidios-ecuador-muertes-crimen-asesinatos.html#:~:text=Un%20informe%20de%20la%20

Polic%C3%ADa,en%20el%20pa%C3%ADs%20se%20duplic%C3%B3. Recuperado el 24 de enero de 2022

Forbidden Stories. (2018). *Frontera Cautiva. La Linea de Fuego.* Recuperado el 2 de diciembre de 2019, de https://lalineadefuego.info/2018/10/24/cuatro-historias-relatan-la-situacion-de-la-frontera-norte-y-el-asesinato-de-los-periodistas/

García, J. (2021). *Amenazas Persistentes Avanzadas.* Recuperado el 22 de enero de 2022, de https://ciberseguridad.oesia.com/amenazas-persistentes-avanzadas/

LBE. (2018). El desangre blanco en el río Mataje. *La Barrera Espaciadora.* Recuperado el 14 de febrero de 2022

Lissardy, G. (2022). Por qué América Latina es la región más violenta del mundo (y que lecciones puede tomar de la historia de Europa). *BBC New Mundo.* Recuperado el 14 de febrero de 2022, de https://www.bbc.com/mundo/noticias-america-latina-48960255

Machado, D. (2008). *La Base de Manta y la estrategia de militarización en América Latin*a. Recuperado el 23 de enero de 2022, de https://rebelion.org/la-base-de-manta-y-la-estrategia-de-militarizacion-en-america-latina/

McGuinness, D. (2017). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. *BBC New*. Recuperado el 14 de febrero de 2022, de https://www.bbc.com/mundo/noticias-39800133

Ministerio de Defensa - Argentina. (2010). *Libro Banco de la Defensa.* Ciudad Autónoma de Buenos Aires: Minsiterio de Defensa.

Ministerio de Defensa - Brasil. (2012). *Libro Blanco de Defensa Nacional*. Brasilia: Ministerio de Defensa.

Ministerio de Defensa Nacional - Chile . (2017). *Libro De la Defensa Nacional de Chile*. Santiago de Chile: Ministerio de Defensa Nacional.

Ministerio de Defensa Nacional. (2003). *Política de Defensa y Seguridad Democrática*. Recuperado el 22 de enero de 2022, de https://www.oas.org/csh/spanish/documentos/colombia.pdf

Ministerio de Defensa Nacional. (2018). *Política de la Defensa Nacional del Ecuador "Libro Blanco".* Quito: Instituto Geográfico Militar.

Ministerio de Defensa Nacional. (2019). *Plan Nacional de Seguridad Integral 2019-2030*. Recuperado el 8 de julio de 2021, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-matriz-web.pdf

Minsiterio de Defensa de la República de Bolivia. (2004). *Libro Blanco de Defensa 2004*. La Paz: Instituto Geográfico Militar.

Minsiterio de Defensa -Perú. (2006). *Libro Blanco de la Defensa Nacional*. Recuperado el 22 de enero de 2022, de https://cdn.www.gob.pe/uploads/document/file/397073/Libro_blanco.pdf

Ojeda, C. (2013). *Amenazas Multidimensionales: Una realidad en Suramérica.* Chile: Academia Nacional de Estudios Políticos y Estratégicos.

Organización de los Estados Americanos. (21 de noviembre de 2003). Conferencia Especial sobre Seguridad. México.

Pernik, P. (2021). *Disuación cibernética: Un estudio de caso sobre políticas y prácticas de Estonia.* Centro Europeo de Excelencia para Contrarrestar las Amenazas Híbridas, 1-28.

Pichel, M. (2021). *Cómo Ecuador pasó de ser país de tránsito a un centro de distribución de la droga en América Latina (y qué papel tienen los carteles mexicanos).* Recuperado el 14 de febrero de 2022, de https://www.bbc.com/mundo/noticias-america-latina-58829554

Priest, D. (2013). Acción encubierta en Colombia. Washigton Post, págs. https://www.washingtonpost.com/sf/investigative/2013/12/21/covert-action-in-colombia/?hpid=z1. Recuperado el 14 de febrero de 2022

Restrepo, J. (24 de abril de 2018). *Terror en la frotnera norte de Ecuador: ¿Qué hay detrás de estos sucesos?* Recuperado el 2 de diciembre de 2019, de https://actualidad.rt.com/actualidad/269472-ecuador-narcotrafico-terrorismo-frontera-colombia

Sec2crimen. (2021). *Amenazas Persistentes Avanzadas. Análsiis de grupso APT. Obejtivos: Estados Unidos y Latinoamérica*. Recuperado el 22 de enero de 2022, de https://www.sec2crime.com/2021/06/27/amenazas-persistentes-avanzadas-analisis-de-grupos-apt-objetivo-eeuu-y-latam/

Securityhacklabs. (2018). *Grupos avanzados de amenazas persistentes "APT Groups"*. Recuperado el 22 de enero de 2022, de https://securityhacklabs.net/articulo/grupos-avanzados-de-amenazas-persistentes-apt-groups

Servicio Europeo de Acción Exterior. (2019). *Una Europa que protege: Contrarrestar las amenazas híbridas.* Recuperado el 22 de enero de 2022, de https://eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf

Thales group. (2018). *Amenazas persistentes avanzadas.* Recuperado el 22 de enero de 2022, de https://cpl.thalesgroup.com/es/encryption/advanced-persistent-threats-apts

Ulrich, B. (1998). ¿Qué es la globalización? Falacias del globalismo respuestas a la globalización. *Reseña*s. 118-123.

Vallejo, M. (2013). *Análisis constructivista de la Base de Manta y la percepción del gobierno y la sociedad civil.* Recuperado el 22 de enero de 2022, de https://repositorio.flacsoandes.edu.ec/bitstream/10469/5709/2/TFLACSO-2013MGVJ.pdf

Villaverde, X. (10 de septiembre de 2018). Ecuador-Colombia: una frontera caliente y abandonada. Recuperado el 2 de diciembre de 2019, de https://

www.opendemocracy.net/es/ecuador-colombia-una-frontera-caliente-y-abandonada/

Villaverde, X. (10 de septiembre de 2018). *Ecuador-Colombia: una frotnera caliente y abandonada*. Recuperado el 2 de diciembre de 2019, de https://www.opendemocracy.net/es/ecuador-colombia-una-frontera-caliente-y-abandonada/

Voz de América. (2021). Drones atacan penal de máxima seguridad de Ecuador. Recuperado el 24 de enero de 2022, de https://www.vozdeamerica.com/a/drones-atacan-penal-maxima-seguridad-ecuador/6225705.html#:~:text=Un%20ataque%20con%20drones%20y,encerrados%20altos%20jefes%20del%20narcotr%C3%A1fico.&text=El%20gobierno%20de%20Ecuador%20atribuye,entre%20carteles%20internaci

Zuniga, J. (2020). La desigualdad en América Latina. Recuperado el 22 de enero de 2022, de *Panorámica:* https://www.panoramical.eu/columnas/la-desigualdad-en-america-latina/