EJÉRCITO DE CHILE
DIVISIÓN EDUCACIÓN
Academia de Guerra

PROCESO DE "PREPARACIÓN DE INTELIGENCIA PARA LAS OPERACIONES" (IPO) Y SU PERTINENCIA DE SER EMPLEADA COMO UNA HERRAMIENTA DE INTELIGENCIA EN EL CONTEXTO DE AMENAZAS HÍBRIDAS".

Memoria para obtener el título de Oficial de Estado Mayor del Ejército de Chile

MAYOR MARCELO JAVIER FLORES MOLINA

PROFESOR GUÍA:
TENIENTE CORONEL ALEJANDRO ERNESTO RUBILAR GAETE
Oficial de Estado Mayor

MAGISTER EN CIENCIAS MILITARES CON MENCIÓN EN PLANIFICACIÓN Y GESTIÓN ESTRATÉGICA DE LA ACADEMIA DE GUERRA

Santiago de Chile
2023

AGRADECIMIENTOS

A mi esposa Carolina, cuyo apoyo ha sido fundamental durante mi carrera militar. A mi hijo Gabriel Ignacio, quien es el motor que impulsa mi trabajo y mis ganas de superarme día a día.

ÍNDICE

Lista de Abreviaturas …….....		v
Tablas ……..		viii
Imágenes …….....		ix
Resumen …….		1
Abstract ……...		2
Introducción		3
Capítulo I: Problema de Investigación ……		6
1.	Planteamiento del problema ……	6
1.1	Antecedentes del Problema ……	6
1.2	Preguntas de investigación …….	8
1.2.1	Pregunta general ……..	8
1.2.2	Preguntas específicas ……..	8
1.3	Objetivos …….	9
1.3.1	Objetivo general ……	9
1.3.2	Objetivos específicos …….....	9
1.4	Justificación de la investigación …….	9
1.5	Delimitación de la investigación …….	10
1.6	Marco Teórico-Conceptual Referencial …….	11
1.6.1	Conflicto / Guerra Híbrida …….....	11
1.6.2	Amenaza ……	13
1.6.3	Amenaza Híbrida ……..	14
1.6.4	Intelligence Preparation for Operations IPO …….	15
1.6.5	Intelligence Preparation of the Battlefield / battlespace IPB ……..	16
1.6.6	Joint Intelligence Preparations Operational Environment JIPOE ……..	17
1.7	Marco Metodológico …….	17
1.7.1	Paradigma de investigación, nivel de conocimiento, método investigativo ….	17
1.7.2	Selección de fuentes de información …….	19
1.7.3	Técnicas e instrumentos para la recolección de datos e información ……..	20
1.7.4	Técnica(s) y procedimientos de análisis de los datos recopilados ……..	20
Capítulo II: Amenaza Híbrida ……...		22
2.1	Metodología del capítulo ……..	22
2.2	Amenaza híbrida y su fundamentación a base de la teoría y análisis	23

	académico …….....	
2.3	Amenaza híbrida y su fundamentación a base de la Directiva Política en el Sector Defensa y Doctrina Nacional y Extranjera ……	34
2.3.1	Directivas Políticas para el Sector Defensa …….	34
2.3.2	Doctrina Nacional …….	37
2.3.3	Doctrina Extranjera ……...	38
2.4	Identificación de cualidades equivalentes sobre la amenaza híbrida ……..	43
2.5	Caso de Estudio “Guerra del Líbano 2006 y relación actual con “Guerra de Ucrania” ……..	44
2.6	Síntesis del capítulo...…….....	53
Capítulo III: “Preparación de Inteligencia para las Operaciones” IPO ……..		56
3.1	Metodología del capítulo……...	56
3.2	Revisión de la fundamentación y su relación bibliográfica con el contexto híbrido ……	56
3.3	“Preparación de Inteligencia para las Operaciones” IPO ……...	57
3.3.1	Antecedentes Generales ……	57
3.3.2	Conceptualización, propósitos y fundamentación ……...	58
3.3.3	Operaciones en red ……..	61
3.3.4	IPO como herramienta de preparación de inteligencia ……..	66
3.3.5	Cuadro descriptivo de IPO y su pertinencia en el análisis de amenazas híbridas ……...	73
3.4	Síntesis del capítulo ……	78
Capítulo IV: IPB y JIPOE y su pertinencia de ser empleados en el análisis de amenazas híbridas ……		81
4.1	Metodología del capítulo……...	81
4.2	Revisión de fundamentos y su relación con el contexto híbrido ……...	81
4.3	Análisis comparativo de procesos de inteligencia empleados en apoyo a nuestros procesos de planificación de operaciones ……	82
4.4	IPB Complejo ……	93
4.5	IPB ATP 2-01.3 ……	95
4.6	Síntesis capitular ……...	98
Capítulo V: Conclusiones y propuestas ……		102
5.1	Conclusiones ……	102
5.2	Síntesis ……...	102

5.3	Valoración ……..	108
5.4	Propuestas …….	110
	Referencias bibliográficas …….....	112
	Anexo Nº1 “Pasos de Metodología IPO” ……...	117
	Anexo Nº2 “Proceso IPO” Desarrollo de modelo de inteligencia ……..	119
	Anexo Nº3 Paso Nº1 “Definir el Espacio de Operaciones” ……	120
	Anexo Nº4 Paso Nº2 “Describir los efectos en el espacio de Operaciones” ……..	124
	Anexo Nº5 Paso Nº3 “Evaluar fuerzas adversarias, amenazas y elementos de potenciales amenazas ……	133
	Anexo Nº6 Paso Nº4 “Determinar posibilidades” …….	146
	Anexo Nº7 Entrevistas a especialistas en inteligencia ……	150
	Anexo Nº8 Procesamiento de encuestas ……..	153

LISTA DE ABREVIATURAS

Abreviaturas	Definición
AII	Área of Intelligence Interest / Área de Interés de Inteligencia
AO	Ambiente Operacional
AOR	Area of Operations / Área de Operaciones
ASCOPE	Áreas, Estructuras, Capacidades, Organizaciones, Personas, Eventos
A/S	Analysis / Synthesis, Análisis / Síntesis
ATGM	Anti-Tank Guided Missile / Misil Guiado Anti-Tanque
CBRNE	Chemical, Biological, Radiological, Nuclear or Large Explosive / Químico, Biológico, Radiológico, Nuclear o Alto explosivo
CEEAG	Centro de Estudios Estratégicos de la Academia de Guerra
CESIM	Centro de Estudios e Investigaciones militares del Ejército de Chile
C/I	Capabilities, Intentions / Capacidades e Intenciones
COG	Center of Gravity / Centro de Gravedad
COA	Course of Action / Curso de Acción
CULTINT	Cultural Intelligence / Inteligencia cultural
CYBERINT	Ciber Intelligence / Ciberinteligencia
DIPLINE	Dirección de Planificación e Informaciones del Ejército.
DIRECTEMAR	Dirección General del Territorio Marítimo y de Marina
DP	Decision Point / Punto Decisivo
ECOA	Enemy Course of Action / Curso de Acción del Enemigo
EEC	Estado de Excepción Constitucional
EE.UU.	Estados Unidos
EFD	Estado Final Deseado
EUA	Estados Unidos de América
FDI	Israel Force Defense / Fuerzas de Defensa de Israel
GEOINT	Geospatial Intelligence / Inteligencia Geoespacial
GZ	Gray Zone / Zona Gris
HIT	High Impact Threat / Amenazas de Alto Impacto
HPT	High-Payoff Targets / Objetivo de Alto Rendimiento

Abreviaturas	Definición
HUMINT	Human Intelligence / Inteligencia humana
HVT	High Value Target / Objetivos del Alto Valor
IC	Critical Infraestructure / Infraestructura Crítica
IED	Improvised Explosive Device /Artefacto Explosivo Improvisado
IIA	Influence Interest Área / Área de Influencia de Inteligencia
ILO	Infraestructure Liaison Officers / Oficiales de Enlace de infraestructura
INFOOPS	Informations Operations / Operaciones de Información
IPB	Intelligence Preparation of the Battlefield/Battlespace**”** / Proceso de Integración del Campo de Batalla
IPO	Intelligence Preparation for Operations / Preparación de inteligencia para las Operaciones
ISR	Intelligence, Surveillance, Reconnaissance / Inteligencia, Vigilancia, Reconocimiento
I&W	Indications and Warning / Indicaciones y Advertencias
JFC	Joint Force Commander / Comandante de la Fuerza conjunta.
JIPOE	Joint Intelligence Preparation Operational Environment / Preparación de Inteligencia del Ambiente Operacional Conjunto
LDN	Libro de Defensa Nacional
MANPADS	Man-portable air-defense systems / Sistema de Defensa Antiaérea Portátil
MD	Most Dangerous / Más Peligroso
ML	Most Likely / Más probable
MOOTW	Operaciones Militares Distintas a la Guerra
MOUT	Military Operations in Urban Terrain / Operaciones Militares en Terrenos Urbanos
NAI	Named Areas of Interest / Áreas de Interés Nombradas
NORA	Non-obvious relationship awareness or analysis / Conocimiento o análisis de Relaciones No Obvias
OAKOC	Observación y Campo de Tiro, Avenidas de Aproximación, Terrenos Críticos, Obstáculos, Cubierta y Protección
OE	Operational Environment / Ambiente Operacional
ONA	Operational Net Assesment / Evaluación de Red Operativa
OOB	Order of Battle / Orden de Batalla

Abreviaturas	Definición
OODA	Observar, Orientar, Decidir, Actuar
OPFOR	Opposing Force / Fuerza Opositora
OPSEC	Operational Security / Operaciones de Seguridad
ORBAT	Order of Batlle / Orden de Batalla
OSINT	Open Source Intelligence / Inteligencia de Fuentes Abiertas
OTAN	North Atlantic Treaty Organization / Organización del Tratado del Atlántico Norte
PAO	Proceso de Adquisición de Objetivos
PDN	Política de Defensa Nacional
PMESII	Político, Militar, Económico, Social, Información, Infraestructura
PMESII-PT	Político, Militar, Económico, Social, Información, Infraestructura, Entorno Físico, Tiempo
PTE	Potential Threat Elements / Elementos de Amenazas Potenciales
RFI	Requests for Information / Requerimientos de información
RIF	Response Information Folders / Carpetas de información de Respuestas
SIGINT	Signals Intelligence / Inteligencia de Señales
SITEMP	Situation Temple / Plantilla de Situación
TEW	Terrorism Early Warning Group / Grupo de Alerta Temprana contra el Terrorismo
TLO	Terrorism Liaison Officers / Oficiales de Enlace contra el Terrorismo
TO	Teatro de Operaciones
T/P	Tendencias y Potenciales
T/S	Transacciones y Firmas
TTP	Tácticas, técnicas y procedimientos
UAV	Unmanned Aerial Vehicle / Vehículo No Tripulado
UE	European Union / Unión Europea
WDM	Weapons of Mass Destruction / Armas de Destrucción Masiva
WTC	World Trade Center

TABLAS

Tabla 1 33
Tabla 2 42
Tabla 3 65
Tabla 4 73
Tabla 5 75
Tabla 6 83
Tabla 7 87
Tabla 8 95

IMÁGENES

Imagen 1 28
Imagen 2 60
Imagen 3 61
Imagen 4 62
Imagen 5 65
Imagen 6 66
Imagen 7 68
Imagen 8 72
Imagen 9 94
Imagen 10 95

RESUMEN

A inicios de la década del dos mil, surgió después del atentado al World Trade Center (WTC) en Estados Unidos, un nuevo concepto y herramienta para analizar posibles amenazas de naturaleza irregular denominada “Intelligence Preparation for Operations” (IPO), proceso del cuál no existen conocimientos en nuestra institución y el cual ilumina esta investigación, la cual consiste en identificar y comprender sus elementos constitutivos y a raíz de lo anterior, compararla con las herramientas existentes en nuestra doctrina, dilucidando con lo anterior, sobre cuál sería la herramienta más adecuada en apoyo a nuestros procesos de planificación actualmente para la evaluación de amenazas de naturaleza híbridas. Por su parte, nuestra doctrina institucional y conjunta, cuenta con textos para sus actividades de preparación de inteligencia tanto en el nivel táctico como operacional, los que contribuyen a comprender el campo de batalla, ambiente operacional y analizar las posibles amenazas asociadas, para establecer las capacidades, fortalezas, vulnerabilidades y en definitiva, lo que pueden ser capaces de hacer.

Sin embargo, harían énfasis mayoritariamente en el análisis de fuerzas o amenazas convencionales, dejando en un plano inferior a otros tipos de amenazas como lo son, las irregulares y asimétricas, y más aún, no estimando explícitamente el concepto de amenaza híbrida.

Finalmente, esta investigación consiste en indagar sobre una herramienta específica de inteligencia empleada con anterioridad, pero con la particularidad, que está enfocada a amenazas irregulares y asimétricas, permitiendo posteriormente luego de su vinculación con el concepto de amenaza híbrida, determinar si es pertinente para su evaluación y análisis, y si sus fundamentos son atingentes de complementación o aporte a las herramientas ya existentes en nuestra doctrina.

Palabras claves: *Conflicto Híbrido, Amenaza, Amenaza Híbrida, “Intelligence Preparation for Operations” IPO, IPB, JIPOE.*

ABSTRACT

At the beginning of the 2000s, after the attack on the World Trade Center (WTC) in the United States, a new concept and tool to analyze possible threats of an irregular nature called "Intelligence Preparation for Operations" (IPO) arose, a process from which There is no knowledge in our institution and which illuminates this research, which consists of identifying and understanding its constituent elements and, as a result of the above, comparing it with the existing tools in our doctrine, elucidating with the above, what would be the most appropriate tool. in support of our current planning processes for the evaluation of threats of a hybrid nature. For its part, our institutional and joint doctrine has texts for its intelligence preparation activities, both at the tactical and operational level, which contribute to understanding the battlefield, operational environment, and analyzing possible associated threats to establish capabilities, strengths, vulnerabilities and ultimately, what these threats may be capable of doing.

However, they would mainly emphasize the analysis of conventional forces or threats, leaving other types of threats such as irregular and asymmetric threats on a lower plane, and even more so, not explicitly estimating the concept of hybrid threat.

Finally, this research consists of inquiring about a specific intelligence tool previously used, but with the particularity that it is focused on irregular and asymmetric threats, allowing later, after its link with the concept of hybrid threat, to determine if it is relevant to its application. evaluation and analysis, and if its foundations are contingent on complementing or contributing to the already existing tools in our doctrine.

Keywords: Hybrid Conflict, Threat, Hybrid Threat, "Intelligence Preparation for Operations" IPO, IPB, JIPOE.

INTRODUCCIÓN

El advenimiento de nuevas amenazas a la Seguridad y Defensa de los Estados, rápidamente ha condicionado los enfoques tradicionales de inteligencia de sus organismos en el análisis de entornos operativos y de posibles adversarios más complejos, quienes por medio de diversos mecanismos de acción, pueden afectar determinantemente a la seguridad interior y exterior de las naciones. Es en este contexto, que la mayoría de las Fuerzas Armadas poseen recursos formales y doctrinarios para realizar las tareas de inteligencia necesarias para proporcionar información útil a los comandantes de los diferentes niveles, y de esta manera contribuir de la mejor forma a la toma de decisiones en el empleo eficaz y eficiente de sus fuerzas.

De lo antes señalado, es que se desprende la necesidad de indagar y cuestionarse acerca de la pertinencia de nuestros procesos de inteligencia, surgiendo de esa inquietud, lo planteado por la Dirección de Planificación e Informaciones del Ejército (DIPLINE) al momento de generar este tema de investigación, aludiendo que nuestra Institución utiliza el IPB o el JIPOE para conflictos convencionales. Sin embargo, para el análisis de conflictos híbridos, no se contaría con una herramienta similar como el proceso IPO (Intelligence Preparation for Operations), metodología impulsada por Matt Begert y Dan Lindsay en Estados Unidos, como alternativa para enfrentar este latente entorno híbrido. Lo anterior, decantó en que para analizar este proceso extrainstitucional, también fue necesario evaluar y revisar nuestros procesos, buscando semejanzas, diferencias y pertinencias relacionadas. En consecuencia, el propósito de este trabajo de investigación fue proporcionar los argumentos necesarios para discernir sobre cuál de las herramientas de preparación de inteligencia IPO, IPB o JIPOE, sería las más adecuada para analizar y evaluar amenazas de naturaleza híbrida.

En este sentido, para lograr el objetivo propuesto, el desarrollo de esta investigación se realizó por medio de cuatro capítulos específicos, siendo el primero de ellos, establecer preliminarmente un marco conceptual referencial, a través de la precisión de algunos conceptos nucleares con respecto a la amenaza y los procesos destinados a analizarlas.

En efecto, se establecieron los parámetros de análisis y los objetivos específicos que contribuyeron a validar la tesis de este trabajo de investigación.

En segundo lugar, se realizó un trabajo orientado a definir un concepto objetivo de *Amenaza Híbrida,* con el propósito de que sirviera para los siguientes capítulos, por medio de la descomposición, análisis y conclusión de diferentes posturas teóricas y de lo plasmado en doctrinas vigentes en instituciones armadas de países de referencia, las cuales en la actualidad, han internalizado esta conceptualización y presentan en sus realidades nacionales, amenazas más cercanas y ligadas a estas características. Con lo anterior, se dio cumplimiento al primer objetivo específico, el cual fue definir el concepto antes mencionado.

En tercer lugar, los esfuerzos investigativos estuvieron enfocados en la identificación y descripción de las características, antecedentes, objetivos y metodología del proceso de inteligencia IPO. Lo anterior, por medio de su revisión bibliográfica y vinculación con el contexto híbrido y por medio de la descripción de sus factores y recursos analíticos, buscando con lo anterior, su posible pertinencia. Lo anterior, permitió concluir acerca de su obsolescencia y enfoque específico de análisis, siendo contradictorio con lo señalado y propuesto al momento de levantar este tema de investigación, el cual sin embargo, fue útil para el análisis de su metodología.

Seguidamente y por medio de un cuarto capítulo, se buscó identificar las semejanzas y diferencias de los procesos de inteligencia vigentes en nuestra doctrina institucional y conjunta en apoyo a los procesos de planificación de operaciones militares. Para esto, se planteó inicialmente, señalar el grado de pertinencia explicita con respecto a amenazas híbridas producto de la revisión documental. Posteriormente, y habiendo dilucidado lo anterior, se realizó un análisis comparativo de ambos procesos a base de criterios de comparación, lo que permitió establecer conclusiones objetivas acerca de su vinculación con la definición de amenaza hibrida realizada precedentemente, siendo complementadas con la opinión de especialistas en inteligencia, lo que contribuyó a respaldar estas conclusiones. Estas actividades realizadas, permitieron dar cumplimiento al objetivo específico planteado, y más importante aún, tributar en forma robusta al objetivo principal de la investigación.

Todo lo anterior, fue sustentado por medio de una rigurosa revisión teórica de destacados exponentes, de la doctrina nacional y extranjera, así como también, de publicaciones y artículos afines, confrontado además, con la experiencia de diferentes especialistas en el ámbito de la inteligencia militar, lo que permitió dar la rigurosidad científica a esta investigación.

Por último, y considerando lo anteriormente expuesto, fue factible para el autor establecer conclusiones concretas respecto a cada uno de los objetivos parciales, y más importante aún, comprobar la tesis planteada pudiendo determinar cuál de las herramientas de preparación de inteligencia estudiadas, IPO, IPB o JIPOE, sería las más adecuada para evaluar amenazas de naturaleza híbrida.

CAPÍTULO I
PROBLEMA DE INVESTIGACIÓN

1. Planteamiento del Problema

1.1 Antecedentes del Problema

Como forma definir el problema de investigación, la Dirección de Planificación e Informaciones del Ejército (DIPLINE), al ser el estamento directivo que generó este tema de investigación, declaró textualmente lo siguiente:

> "Nuestra Institución utiliza como herramienta de Inteligencia militar para conflictos convencionales el IPB y/o el JIPOE, dependiendo del nivel de la conducción militar, sin embargo, autores como Matt Begert y Dan Lindsay han empleado el concepto IPO "Intelligence Preparation for Operations", para referirse a la herramienta de análisis que aplica a conflictos híbridos, sin existir una referencia similar a ésta, en nuestro país" (CESIM III SIDE (R) Nº 6030/2359, 2020).

Conforme a lo anterior e indagando en la bibliografía, estos fundamentos carecerían de bases sólidas, ya que no se sustentan en estudios, informes o resultados empíricos existentes actualmente en nuestra institución, considerando adicionalmente que el concepto y herramienta de preparación de inteligencia IPO, fue desarrollado para el análisis de amenazas de naturaleza irregular y no híbridas, ya que en los primeros años de la década del dos mil cuando fue creado, no se abordaba este concepto con solidez.

Ahora si bien, e independiente de que las herramientas existentes en nuestra doctrina no contengan explícitamente los fundamentos para el análisis de amenazas híbridas, de igual manera, hacen referencia al análisis de amenazas de naturaleza irregular, y dejan abierta además, la factibilidad de emplear sus factores de análisis a elementos emergentes, flexibilizando con lo anterior, el estudio de nuevos componentes y factores constitutivos del ambiente operacional y del campo de batalla y por ende, de las nuevas amenazas que interactúan y se pueden presentar en él.

A su vez, como forma de sustentar lo expresado previamente por este estamento directivo, surgió a principios de la década del dos mil, una percepción de que herramientas como el IPB no contaban con los fundamentos específicos para analizar los nuevos escenarios, en donde sus actores, procedimientos e intenciones, eran disimiles a los convencionales enfrentados con anterioridad. Por lo tanto, estas nuevas amenazas requerirían de un análisis exhaustivo y profundo. Así, Martínez (2012), manifiesta que autores como Matt Begert y Dan Lindsay desarrollaron hace casi dos décadas atrás, el concepto de IPO *"Intelligence Preparation for Operations*", como evolución del IPB, siendo este concepto una visualización enfocada a conflictos de naturaleza asimétricos, ya que habrían identificado notorios vacíos doctrinarios con respecto al análisis de factores asociados a amenazas irregulares en la doctrina existente en el momento de estos postulados.

De esta manera, Begert y Lindsay (2002), centraron adecuadamente sus estudios en la inteligencia en MOUT[1], y reconocieron la complejidad adicional del entorno, y en consecuencia, las deficiencias que presentaba la doctrina de IPB, ya que el uso de esta herramienta sólo se había tratado en un constante razonamiento sobre elementos predecibles como el terreno y el clima, basado en una doctrina militar convencional en cuanto a equipamiento e intenciones militares.

Ahora si bien, y aunque se manifestó que la doctrina militar había definido el rol del IPB, el cuál era preponderantemente para acciones de fuerzas convencionales, es decir, oponentes asociados de (Estado-nación), de igual manera algunas partes y elementos del IPB, son aplicables a entornos de amenazas irregulares. Sin embargo, según los análisis y comentarios realizados por estos expertos, el IPB era incompleto cuando se trataba de una amenaza asimétrica.

Es por lo anterior, que la presente investigación buscó indagar en el origen, fundamentos y características de *"Intelligence Preparation for Operations" (IPO),* como concepto y como herramienta de preparación de inteligencia, con la particularidad que presentaría un enfoque específico en el análisis de amenazas del tipo irregular, no existiendo información

[1] MOUT (Operaciones Militares en Terrenos Urbanos).

o fundamentos formales sobre esta herramienta en nuestra doctrina, para a base de ello, buscar su vinculación al análisis de nuevas amenazas de naturaleza híbridas, junto con homologar este mismo ejercicio, a nuestros procesos vigentes de inteligencia en nuestra doctrina institucional y conjunta, y de esta forma, dar respuesta al objetivo general de esta investigación, cuyo propósito es, *Determinar cuál de las herramientas de preparación de inteligencia IPO, IPB o JIPOE, sería la más adecuada para analizar y evaluar amenazas de naturaleza híbrida*.

Finalmente, como forma de contextualizar la problemática que iluminó esta investigación, es necesario expresar que los procesos de preparación de inteligencia constantemente deben flexibilizar sus recursos amoldándose a nuevas amenazas que se presentan en los conflictos contemporáneos, las cuales se caracterizan por ser variadas y confusas, lo que conlleva a analizar nuevas herramientas, o por el contrario, indagar en recursos ya empleados con anterioridad, pero que se caracterizan por poseer un mayor grado de especificidad o vinculación con el análisis de amenazas no convencionales, dilucidando con lo anterior, si contribuyen a la complementación de las herramientas vigentes en nuestra doctrina.

1.2 Preguntas de investigación

1.2.1 Pregunta general

¿Cuál de las herramientas de preparación de inteligencia, IPO, IPB o JIPOE, sería las más adecuada para analizar y evaluar amenazas de naturaleza híbrida?

1.2.2 Preguntas específicas

1) ¿Qué es una Amenaza Híbrida?
2) ¿En qué consiste el Proceso IPO y cuál es su pertinencia en el análisis de amenazas híbridas?.
3) ¿Cuáles son las diferencias analíticas de los procesos IPB y JIPOE, y cuál es su pertinencia en el análisis de amenazas híbridas?

1.3 Objetivos

1.3.1 Objetivo general

Determinar cuál de las herramientas de preparación de inteligencia, IPO, IPB o JIPOE, sería las más adecuada para analizar y evaluar amenazas de naturaleza híbrida.

1.3.2 Objetivos específicos

1) Definir qué es Amenaza Híbrida.
2) Describir en qué consiste el Proceso de Preparación de inteligencia IPO, y cuál es su pertinencia de análisis en el contexto de amenazas híbridas.
3) Describir cuales son las diferencias analíticas de los procesos IPB y JIPOE, en el contexto de amenazas híbridas.

Respecto a lo anterior, se menciona que la pregunta general fue sujeta a modificación producto de las orientaciones y recomendaciones recibidas en la defensa del proyecto de investigación. De esta manera, la pregunta general mutó desde el propósito de buscar un valor de aplicabilidad de la herramienta IPO, a orientarse a determinar sobre cuál de las herramientas ya existentes en nuestra doctrina y comparado con el análisis de ellas, sería la más adecuada para analizar y evaluar amenazas de esta naturaleza. Por otra parte, las preguntas especificas de igual forma fueron modificadas con el propósito de dar coherencia y delimitación a la pregunta general, orientando y direccionándolas a la definición de amenaza híbrida y a la descripción y comparación de estos diferentes procesos de inteligencia, en relación a la evaluación de amenazas de esta tipología.

1.4 Justificación de la investigación

Debido a los ataques terroristas acontecidos al World Trade Center el año 2001[2], y como resultado del análisis de las amenazas identificadas y responsabilizadas de aquellos atentados, destacados analistas y expertos en seguridad de organismos ligados a la

[2] World Trade Center (WTC), en castellano, “Centro Mundial de Comercio”, fue un complejo de edificios en Manhattan, ciudad de Nueva York, Estados Unidos, que incluía a las emblemáticas Torres Gemelas, inauguradas el 4 de abril de 1973 y destruidas en los atentados del 11 de septiembre de 2001 debido a un ataque terrorista.

defensa y agencias policiales en Estados Unidos, desarrollaron y posteriormente emplearon nuevas herramientas de análisis, con el objetivo de identificar y generar las condiciones para contrarrestar estas nuevas amenazas que se alzaban como protagonistas a principios del siglo XXI. Por lo tanto, IPO fue una herramienta que se generó con el propósito de analizar específicamente posibles amenazas de naturaleza no convencional, las cuales se asociaban principalmente al terrorismo que aquejaba la situación interna del país.

Es por lo anterior, que se desarrolló la presente investigación sobre esta herramienta desconocida denominada IPO y de la cual no existían referencias en nuestra doctrina. Lo anterior, con la finalidad de en primer lugar, indagar en sus fundamentos, elementos constitutivos y metodología de análisis, para posteriormente identificar sus fortalezas y debilidades con el propósito de dilucidar en que forma contribuyen al análisis de estas amenazas emergentes y contemporáneas. Finalmente, la investigación fue viable de realizar, debido al tiempo asignado, complementando además, a que no consideró el empleo de recursos económicos y materiales de significación.

1.5 Delimitación de la investigación

La presente investigación se focalizó en situaciones acontecidas durante el siglo XXI, asociados a la seguridad de EEUU después del atentado al WTC. Por otra parte, se indagó en los textos institucionales y conjuntos vigentes en nuestra doctrina, y otros de connotación teórica que entregaron información actualizada sobre este tipo de amenazas. Lo anterior, contribuyó a entregar antecedentes fidedignos sobre sus elementos constitutivos, permitiendo posteriormente, vincularlas a los distintos procesos y herramientas abordadas en esta investigación. Por lo tanto, los antecedentes que se recopilaron estuvieron enmarcados entre los primeros años de la década del dos mil (2001) hasta la actualidad.

A su vez, la investigación se enfocó en los procesos y métodos de preparación de inteligencia y su vinculación con amenazas no convencionales, los cuáles se presentan e

interactúan de una u otra manera, en los diferentes niveles de la conducción militar. Sin embargo, se hizo énfasis en el ámbito militar y en los niveles operacionales y tácticos, ya que en estos niveles y producto del amparo de recursos doctrinales disponibles y vigentes de inteligencia, se realizan principalmente las actividades destinadas a identificar, definir y evaluar las amenazas, y en definitiva, generar insumos para contrarrestarlas.

1.6 Marco Teórico - Conceptual Referencial

Con respecto a los conceptos y fundamentos que le dan estructura al marco teórico para la presente investigación, es importante mencionar que se centran principalmente en el fenómeno de las nuevas amenazas y de los recursos de preparación de inteligencia existentes para evaluarlas. De esta manera, el debate sobre los nuevos tipos de conflictos, guerras y amenazas en la últimas décadas, hacen referencia a los acontecimientos posteriores a la Guerra Fría, en donde se habla acerca de una revolución de la guerra, las cuales se caracterizan por la presencia de nuevos actores, métodos de empleo, objetivos por alcanzar y nuevos escenarios y dominios.

Es por esto, que con el propósito de facilitar la comprensión del objeto de estudio, se estimó definir los siguientes núcleos conceptuales, los que permitieron entender las características, fundamentos y vínculos de esta investigación, siendo los que se presentan a continuación: Conflicto / Guerra Híbrida, Amenaza, Amenaza Híbrida, IPO “Intelligence Preparation for Operations”, IPB y JIPOE.

1.6.1 Conflicto / Guerra Híbrida

Como se ha mencionado, los conflictos han modificado sus elementos constitutivos en muchos aspectos. De esta manera, actualmente se ven representados por la participación de nuevos actores y amenazas muchas veces difusas en su identificación, en donde los objetivos a conseguir son disimiles a los establecidos en guerras tradicionales o convencionales. En relación a este núcleo conceptual, nos referimos principalmente a lo establecido por el Centro de Estudios Estratégicos de la Academia de Guerra (CEEAG), ya que a través de una revisión bibliográfica realizada por parte de destacados analistas,

tanto de fuentes bibliográficas doctrinarias, como a su vez teóricas, se llegó a una conclusión de ciertos fundamentos que caracterizarían a este tipología de conflicto y guerra.

De esta manera y como lo señala el CEEAG (2020), el Conflicto Híbrido se entiende como una forma de interacción interestatal en donde se desarrollan acciones que se sitúan tanto en el ámbito de lo convencional como de lo asimétrico. Lo anterior, se puede ver ejemplificado a través de acciones económicas, diplomáticas, como también por medio de amenazas contra la infraestructura del Estado-objetivo incluyendo la Defensa. Por otro lado, también se busca la consecución de los objetivos políticos y estratégicos a través de acciones en el ciberespacio, operaciones de desinformación, empleo de grupos de poder no militares y ejercicio del terrorismo.

Por otra parte, según este mismo texto, la Guerra Híbrida se define como aquella acción en donde se acepta el inicio de ésta de manera encubierta y con la participación de medios que buscan el debilitamiento estructural político y administrativo, como así mismo, la defensa del Estado-objetivo, por medio de recursos asociados a la agitación social, operaciones de información, ciberataques contra la infraestructura crítica, económica y financiera, ciberataques contra sistemas de defensa, acciones diplomáticas y bloqueos comerciales, entre otras muchas acciones. Logrado lo anterior, abre la posibilidad y las condiciones para llevar a cabo la ejecución de acciones militares convencionales, las que sin duda, pueden seguir siendo reforzadas por la continuación de los esfuerzos antes mencionados.

Al relacionar ambos párrafos, se señala que, tanto en el conflicto híbrido como en la guerra híbrida, participan las capacidades convencionales y las capacidades asimétricas de un Estado. En consecuencia, se puede afirmar que la guerra híbrida corresponde al empleo de las capacidades ya señaladas, con el propósito de generar condiciones favorables para la obtención de los propios objetivos, y a su vez, postergar el empleo de las capacidades militares convencionales, generando con lo anterior superioridad política y estratégica con el propósito de provocar vulnerabilidades al oponente.

1.6.2 Amenaza

Como forma de contextualizar este concepto, nuestra doctrina institucional define una amenaza, como “acciones reales o percibidas, provocadas consciente o inconscientemente por un eventual adversario a quien se le supone la intención y la capacidad para afectar negativamente los intereses propios en el corto o largo plazo” (RDI-20005, 2015, p. 35). Si analizamos lo anterior, podemos evidenciar que esta definición es bastante general, la cual puede abordar dentro de ella varias significaciones y opciones específicas.

Por otra parte, el Ejército de Estados Unidos en su doctrina de inteligencia la define como:

> cualquier combinación de actores, entidades o fuerzas que tengan la capacidad y la intención de dañar las fuerzas de los Estados Unidos, los intereses nacionales de los Estados Unidos o el territorio nacional, pudiendo incluir fuerzas paramilitares o militares, Estados-nación, alianzas nacionales, individuos, grupos de individuos (organizados o no organizados) o condiciones que pueden dañar o destruir vidas, recursos vitales o instituciones” (ATP 2-01.3, 2019, p. 5-1).

Se infiere por lo tanto, que las dos definiciones poseen una connotación similar, la cual se sustenta en el daño que puede causar un ente, actor, fuerza o adversario por medio de su capacidad o intención. Sin embargo, en la definición doctrinaria estadounidense, esta definición entrega mayores matices ya que no sólo se refiere a fuerzas militares, sino que, incluye a fuerzas paramilitares y grupos no organizados los que se pueden asociar al tipo de amenaza irregulares e híbridas, las cuales serán detalladas posteriormente. Por lo tanto, podemos concluir que el concepto de amenaza, trasciende no sólo a la idea de un potencial adversario de carácter militar, ya que por el contrario, incluye una amplia gama de actores y participantes los cuales actualmente buscan influir sobre el adversario por medio de variados métodos y procedimientos de empleo, no siendo solamente los convencionales.

1.6.3 Amenaza Híbrida

Con respecto a este núcleo conceptual, existe una variada bibliografía teórica de destacados exponentes que abordan el surgimiento y evolución de esta tipología de amenazas, como asimismo, textos doctrinarios que a través de sus contenidos se refieren a su fundamentación y particularidades, aunque en una forma bien somera. Sin embargo, en este marco, sólo se cimentarán ciertas bases teóricas, ya que se ahondarán con mayor profundidad en el siguiente capítulo con la finalidad de determinar una definición crítica producto del análisis de fuentes doctrinarias de países de referencia y de otros textos de destacados estudiosos en el ámbito de la seguridad y defensa, lo que permitirá establecer una definición con un mayor grado de robustez.

En tal sentido, y según lo publicado por Sánchez García (2012), Frank Hoffman, antiguo oficial del Cuerpo de Marines Estadounidense, al que algunos llamaron “el padrino intelectual de la guerra híbrida”, utilizó diversos ejemplos históricos que representarían la evolución de las amenazas y del conflicto asimétrico, desde las guerras del Peloponeso, pasando por la Guerra de la Independencia Española, llegando finalmente al conflicto Árabe-Israelí del año 2006 en el Líbano, el cuál según él, es considerado paradigma de este nuevo tipo de amenazas, en la que el mismo bando utilizó de forma simultánea la guerra convencional y la irregular con un destacado apoyo de la población civil en las acciones militares.

Así mismo, Hoffman (2009), establece que las amenazas híbridas incorporan una gama completa de modos de guerra, incluidas capacidades convencionales, tácticas y formaciones irregulares, actos terroristas, incluyendo violencia y coerción indiscriminada y desorden criminal. Lo anterior, puede ser llevado a cabo por unidades separadas o incluso por la misma unidad, pero que generalmente están dirigidas y coordinadas operativa y tácticamente dentro del espacio de batalla principal, buscando sinergia en dimensiones físicas y psicológicas del conflicto.

En otro orden de ideas, el Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile, señala que estos nuevos actores en la disputa:

> Recurren a acciones tanto convencionales como asimétricas, que son dispuestas por la autoridad política del Estado, atendiendo a que implican riesgos políticos y jurídicos en el contexto internacional, debido a que dichas acciones asimétricas corresponden, entre otras, a operaciones de desinformación, al accionar terrorista, a brindar apoyo a grupos opositores o disidentes del estado contenedor, a operaciones de desestabilización política, a ciberataques, e inclusive, al accionar vinculado con el crimen organizado. (CEEAG, 2020, p. 16).

Se infiere entonces hasta el momento, que este tipo de amenazas fundamenta su accionar principalmente en la coexistencia de métodos tanto regulares, como a su vez, irregulares y asimétricos, los cuales emplean un diverso abanico de métodos, técnicas y procedimientos mencionados previamente, con la particularidad que buscan influir determinantemente en la población civil, por medio de su apoyo y adhesión.

1.6.4 IPO "Intelligence Preparation for Operations"

Esta metodología, surgió en los primeros años de la década del dos mil, como un concepto y herramienta análoga civil al IPB, para atender las necesidades de información en la generación de respuestas rápidas, la cual, según sus gestores actuaba principalmente en el ámbito de las amenazas convencionales y en el apoyo de nivel táctico, siendo por lo tanto, incompleto al enfrentarse a una amenaza asimétrica. Por consiguiente, Martínez (2012), señala que la clara diferencia entre los escenarios convencionales y asimétricos-híbridos desde el punto de vista de la inteligencia, motivó a que se haya implementado el término de IPO *"Intelligence Preparation for Operations",* como evolución a la herramienta existente de aquellos años.

Es por ello, que IPO se asocia a un enfoque no tradicional de inteligencia que comparte elementos de inteligencia militar e inteligencia de tipo criminal o policial, y responde al principio de enfrentarse a una amenaza irregular y asimétrica, empleando medios híbridos, los que según, CEEAG (2020), serían los recursos destinados a la materialización de

acciones relacionadas con las operaciones de información, ciberataques, acciones diplomáticas y bloqueos comerciales, entre muchas otras.

Como expresan Begert y Lindsay (2002), se contextualiza como la implementación de un concepto de preparación de inteligencia que mediante la preparación, observación y análisis, busca identificar una posible amenaza con el propósito de disuadir, detectar, disminuir y comprometerla tan pronto sea posible, siendo un concepto de defensa activa, logrado a través de un reconocimiento y vigilancia constante. Asimismo, proporciona un conjunto de herramientas estandarizadas para realizar reconocimientos de la situación, desarrollo del curso de acción y ensayos enfocados en las acciones a realizar, uniendo la brecha entre la planificación deliberada y la planificación en acciones de crisis.

Cabe resaltar, que al igual que otros procesos y herramientas de preparación de inteligencia, cuenta con etapas definidas y destinadas a analizar las variables y factores que afectan el campo de batalla y que son fundamentales para el entendimiento de un entorno operacional y para definir posibles amenazas de características irregulares. Por consiguiente, los pasos que fundamentan este proceso son, “Definir el espacio de operaciones”, “Describir los efectos en el espacio de operaciones”, “Evaluar elementos de la potencial amenaza” y “Determinar las posibilidades y cursos de acción propios”. (Sullivan y Bauer, 2008, p. 30,31).

Por último, este concepto y herramienta será profundizado posteriormente durante el desarrollo de la investigación, señalando su origen, desarrollo, propósito y adicionalmente, realizando una descripción y análisis de sus componentes, con la finalidad de determinar sus fortalezas y debilidades, y así dilucidar acerca de su posible pertinencia en el análisis de amenazas de naturaleza híbrida.

1.6.5 IPB “Intelligence Preparation of the Battlefield/battlespace”

Conforme a lo que señala el RDI-20005, IPB corresponde al “conjunto de actividades sistemáticas, cíclicas y dinámicas donde se integra el terreno, la amenaza, el tiempo

atmosférico y otros factores que permiten entender el campo de batalla y las opciones que presentan a las propias fuerzas y adversarias". (2015, p. 19).

Este proceso genéricamente se sustenta en la superposición de calcos y matrices que se deben modificar de manera continua y permanente para reflejar los cambios en la situación con respecto al campo de batalla y a la amenaza, proporcionando con lo anterior, una representación de la situación de inteligencia en sus diferentes pasos correspondientes. Con respecto a lo anterior, sus pasos de pueden indagar en el respectivo texto, el cual, es parte de la doctrina de inteligencia vigente en nuestra institución.

1.6.6 JIPOE "Joint intelligence Preparations Operational Environment"

Para referirnos a este proceso, nos basaremos en la publicación DNC 2-04, texto actualizado el año 2022 por el Ministerio de Defensa Nacional. Así, y como señala el DNC 2-04, JIPOE corresponde al "proceso metodológico de análisis utilizado por las unidades directivas de inteligencia de carácter conjunto para producir inteligencia que aporte a las apreciaciones y planes de la función, en beneficio del comandante conjunto (JFC) en los procesos de planificación, preparación y ejecución de las operaciones" (2022, p. 15).

En tal sentido, es un proceso utilizado para analizar el entorno físico y de información de diferentes dominios, como lo son el aire, tierra, mar, espacio y el ciberespacio. Además, también considera variables como los sistemas políticos, militares, económicos, sociales e infraestructura (PMESII), siendo su objetivo principal, proporcionar inteligencia descriptiva para comprender las intenciones y capacidades del adversario.

1.7 Marco Metodológico

1.7.1 Paradigma de investigación, nivel de conocimiento, método investigativo

Respecto al paradigma de investigación, se consideró el del tipo cualitativo. Es así como Herrera (2017), manifiesta que los estudios cualitativos tienden a hacer un análisis exhaustivo y en profundidad, relatando los eventos de manera sistemática sobre lo que

está aconteciendo en la realidad, priorizando la información contextual para de esta forma, dar respuesta a la pregunta de investigación. De lo anterior, la investigación se sustentó en un fenómeno basado en un contexto que afectó a la sociedad, entorno político y militar, por lo tanto, se buscó analizar lo que ocurrió y lo que se implementó, considerando sus motivos, implicancias y repercusiones sin alterar el objeto de estudio. Es así, como la relación entre la pregunta general de la investigación, *¿Cuál de las herramientas de preparación de inteligencia IPO, IPB o JIPOE, sería las más adecuada para analizar amenazas de naturaleza híbrida?*, se vinculó con lo definido por Collier (2010), ya que manifiesta que este tipo de enfoque se centra en la capacidad amplia de generar inferencias causales que lo provocan.

Conforme al nivel de conocimiento, fue del tipo descriptivo, ya que se basó en esta misma acción para obtener y retratar la información existente en las distintas fuentes informativas, a partir de publicaciones, textos, experiencias reales y análisis de doctrina. Por consiguiente, se infirió que se estaba investigando sobre un tema ya tratado al menos en sus partes y que obligó al investigador a indagar sobre cuál era el nexo que vinculaba el objeto de estudio y como podría contribuir a complementar las acciones realizadas en nuestro contexto particular. Además, y tal como se indicó en la catedra de Cervantes (2021) “metodología de la investigación”, el nivel de conocimiento descriptivo radica en que se buscó especificar las características de hechos o situaciones, describiendo, comparando o midiendo diversos aspectos, atributos, dimensiones o componentes del fenómeno estudiado y sus relaciones.

A su vez, y como nuevamente como lo señala Cervantes, el método investigativo que se empleó en este trabajo fue de carácter documental, ya que consistió en un “proceso sistemático de indagación, recolección, organización, análisis e interpretación de datos e información en torno al objeto o fenómeno de estudio, obtenido de fuentes documentales escritas o gráficas (2017, p. 88). Asimismo, también está basado en un método comparativo, ya que como lo expresa el mismo texto, este método aplica principalmente al área de investigación de la doctrina, contribuyendo a conocer rasgos comunes o diferenciadores de un fenómeno y a buscar probar sus relaciones causales.

Consecuente con lo anterior, Gómez (2011), expresa que la construccion del conocimiento desde fuentes documentales es una forma de velar por la tradición del pensamiento original, trayéndolo al presente con una lectura hermenéutica que favorece la discusión al hacer nuevos aportes al desarrollo científico con propuestas que pueden ser cuestionadas en forma permanente, pero que siempre se orientarán a alcanzar nuevos desarrollos.

1.7.2 Selección de fuentes de información

Con respecto a la revisión bibliográfica, el investigador se basó principalmente en la recolección de información por medio de fuentes primarias como es el caso de artículos escritos por investigadores y expertos que han establecido las bases teóricas de este concepto y de estas amenazas. De ahí, que se nombran algunos textos, destacando los siguientes:

- IPO “Intelligence Preparation for Operations” de Matt Begert y Dan Lindsay.
- Terrorism Early Warning de Sheriff Lee Baca.
- Hybrid Warfare de Murray and Mansoor.
- Hybrid Warfare and Challenges de Frank Hoffman.

Además, por medio de la recopilación de información a través de individuos encuestados que desarrollan actividades inherentes a la preparación de inteligencia, los que contribuyeron directamente a sustentar y complementar la información antes mencionada, como es el caso de:

- Oficiales con la especialidad de inteligencia que se desempeñen como comandantes de Agrupaciones de Inteligencia en nuestra institución.
- Oficiales con la especialidad de inteligencia que se hayan desempeñado como asesores de inteligencia en UACs.
- Oficiales con la especialidad de inteligencia que se desempeñan o hayan desempeñado impartiendo la doctrina de los procesos de preparación de inteligencia en la Escuela de la especialidad.

Por otra parte, también se consultó en fuentes secundarias como es el caso de textos doctrinarios y herramientas de preparación de inteligencia empleadas actualmente en nuestra institución y en organizaciones extrainstitucionales, siendo atingentes a esta investigación, algunos que se detallan a continuación:

- IPB *(Intelligence preparation of the battlefield/battlespace) RDI – 20005.*
- JIPOE (*Joint Intelligence Preparation of the Operational Environment) DNC 2-04.*
- El Conflicto Híbrido y sus Efectos en la Conducción Operacional y Táctica, del CEEAG.
- IPB (ATP 2-01.3), edic. 2019.
- Amenaza Híbrida en un Ambiente Operacional (MCE 3-24.0), Ejército de Colombia.
- El Enfoque Multidisciplinar en los Conflictos Híbridos, Centro Superior de Estudios de la Defensa Nacional, Ministerio de defensa de España.

1.7.3 Técnicas e instrumentos para la recopilación de datos de información

En un primer momento se realizó la técnica de revisión documental a base del sustento informativo tanto de fuentes primarias y secundarias, con el propósito de identificar los contenidos atingentes a los núcleos conceptuales y al contexto de la investigación, estableciendo con lo anterior, el marco teórico y estructura sólida.

Seguidamente, la investigación se complementó con información aportada por la aplicación de la técnica de “Encuesta” de tipo estratificado, la cual según Herrera (2017), son un método sistemático para obtener información de individuos con el propósito de obtener percepciones y actitudes que representan una población con la finalidad de agregar y cuantificar las respuestas que obtenemos de ellos.

1.7.4 Técnica (s) y procedimientos de análisis de los datos recopilados (técnicas a utilizar)

Para la presente investigación, el análisis de los datos obtenidos durante el proceso de investigación, se realizó a través de la técnica de “Análisis de Contenido”, entendido como el “análisis centrado en el contenido de una comunicación escrita, oral o visual a través de la búsqueda de palabras, frases o símbolos que configuran el contenido de un texto”.

(Pérez Serrano, 2011, p. 134). Esto permite “leer e interpretar el contenido de toda clase de documentos (investigaciones, entrevistas, discursos, revistas, diarios, cartas personales, fichas, testamentos”. (CEEAG, 2017, p. 154).

Como se expresa, el uso de esta técnica implica “organizar, categorizar, codificar, interpretar y analizar los datos y antecedentes producto de la recopilación de información, y comprender cómo los sujetos construyen a través de un lenguaje propio y espontáneo, transformando esa información “subjetiva” en datos factibles de ser analizados” (Gaete, 2017, p. 154).

Simultáneamente, se realizó un análisis respecto a las herramientas de preparación de inteligencia existentes en nuestra doctrina vigente y al concepto y herramienta IPO, en relación al análisis de amenazas de naturaleza híbrida, donde se analizó el material “cualitativo” para clasificar, ordenar, cuantificar e interpretar los productos del documento, contribuyendo al desarrollo e implementación de un método científico.

CAPÍTULO II
AMENAZA HÍBRIDA

2.1 Metodología del capítulo.

En el capítulo anterior, se construyeron las bases teóricas y metodológicas que sustentaron la secuencia y el marco para comprender la presente investigación, beneficiando con lo anterior, el entendimiento de los conceptos que se abordaron durante el desarrollo de este trabajo. De esta manera, el presente capítulo tuvo la finalidad de responder la pregunta específica Nº1: *¿Qué es una Amenaza Híbrida?.*

Sin embargo y como ya se expresó, los fundamentos existentes en nuestra doctrina institucional y conjunta y también de nuestras directivas del nivel político en el sector Defensa, abordan esta tipología de conflicto y amenazas de una manera muy sucinta y poco clara, lo que obligó a profundizar en el estudio y análisis de sus características desde una perspectiva más crítica y por medio de otras fuentes bibliográficas, con el propósito de definir a base de un ejercicio metódico, que se entiende por amenaza híbrida.

Por tal motivo, se aspiró a describir inicialmente este concepto por medio de la fundamentación teórica de destacados autores con una mirada histórica y mundial, para luego, a través de un análisis de contenido de textos directivos y doctrinarios a nivel nacional y extranjera de países de referencia, dilucidar sobre sus fundamentos propios y definitorios.

Lo anterior, permitió a través de un análisis integral, identificar ciertas concordancias y discrepancias, permitiendo identificar algunas cualidades equivalentes relacionadas con este tipo guerra y amenazas. A raíz de lo anterior, a través de un caso de estudio basado en los sucesos y experiencias ocurridas en el conflicto del Líbano del 2006 y de lo que está aconteciendo actualmente en la guerra de Ucrania, se comprobaron las cualidades equivalentes previamente definidas. Lo antes señalado, permitió establecer las conclusiones para construir una aproximación propia de este concepto, aportando los insumos necesarios para desarrollar los siguientes capítulos de esta investigación

2.2 Amenaza híbrida y su fundamentación a base de la teoría y análisis académico.

Es necesario expresar, que durante el transcurso de la historia las amenazas existentes en los conflictos han sufrido grandes transformaciones lo que ha modificado las formas de hacer la guerra. Por consiguiente, se señala que lo híbrido indudablemente ha sobrepasado el umbral de lo convencional, y es por lo anterior, que las amenazas han incrementado su peligrosidad obligando a los Estados a asumir los retos para proveerse de seguridad y defensa, con el propósito de proporcionar tranquilidad a su población y también a su crecimiento y desarrollo.

Es por lo anterior, que en las últimas décadas ha existido un significativo debate sobre la evolución de la guerra moderna en el mundo posterior a la Guerra Fría[3], lo que ha provocado que expertos hayan llevado esta discusión a un plano más amplio, innovador y concreto, reconociendo que los conflictos y guerras han entrado en una época en la que los adversarios se caracterizan por su flexibilidad, sofisticación y capacidad de empleo de múltiples tipos de guerra, en donde la adaptación será en directa relación a los objetivos por alcanzar. En concordancia con lo anterior, la publicación, “Evolución de las nuevas amenazas a la Seguridad Nacional” expresa que:

> las amenazas hasta finales del siglo XX se podían catalogar como amenazas regulares, representadas por acciones bélicas de un Estado contra otro, y básicamente el origen estaba en la tenencia de intereses comunes como afectar la integridad territorial, la soberanía y la nación. Así, para finales del siglo XX la casi totalidad de los Estados en el hemisferio occidental cuentan con gobiernos elegidos por voto democrático, contemplándose con esto, el surgimiento de nuevas amenazas y por ende, la necesidad de abordar temas sobre seguridad y estabilidad regional. (Grisales, 2015, p. 2).

[3] Guerra Fría: enfrentamiento político, económico, social, ideológico, militar e informativo el cual comenzó al término de la Segunda Guerra Mundial entre los bloques Occidental (capitalista) y Oriental (socialista), liderados por los Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas respectivamente.

Complementariamente, el CEEAG (2020), señala que gracias a la práctica del pensamiento crítico, sumado a la colaboración del estudio de la historia, existiría la factibilidad de poner en duda muchas de estas afirmaciones sobre las nuevas amenazas, ya que existen antecedentes para sostener la tesis de que la práctica de lo híbrido se ha practicado desde siempre. Además, quizás lo que ha ocurrido es que ha existido una carencia en la identificación y participación de actores no tradicionales, como es el caso del crimen organizado, el empleo de mecanismos de acción asimétricos, ciberataques, la desestabilización política, y por sobre todo, la intervención del Estado que resuelve asumir esta alternativa para enfrentar el desafío del conflicto interestatal.

No obstante, y como se señaló en forma previa, existe actualmente una amplia fundamentación sobre la definición y particularidades de este tipo de amenazas, las que contribuirán a componer una definición con un mayor grado de objetividad. Es por lo anterior, que nos referiremos a destacados exponentes en este ámbito.

En primer lugar, haremos mención a los postulados realizados por Frank Hoffman, Teniente Coronel en retiro del Cuerpo de Marines de los EE. UU., quien ha sido analista y consultor de asuntos de seguridad nacional con más de 30 años de experiencia y el cual según la comunidad internacional, es denominado el padrino intelectual del conflicto híbrido, sosteniendo que la conceptualización del conflicto y amenaza híbrida no es clara y que a lo largo de su evolución ha estado sometida a un constante cuestionamiento. De esta manera, Hoffman a través de la descomposición de diversas teorías como son las guerras de Cuarta Generación, Guerras “No Trinitarias”, Guerras Compuestas y Guerras sin Restricciones, teorías prominentes en el momento en que comenzaron sus estudios, logró estructurar un marco más robusto en relación a estas nuevas amenazas.

Así en el 2007 publica una de sus obras más conocidas, Conflict in the 21st Century: The Rise of Hybrid Wars, la cual asienta que estas amenazas incorporaban “una amplia gama de diferentes modalidades de guerra, incluyendo capacidades convencionales, tácticas y formaciones irregulares, actos terroristas que incluyen violencia y coerción indiscriminada y desorden criminal” (Hoffman, 2007, p. 8). En ese mismo sentido, y analizando lo

plasmado, se sintetiza que las guerras y amenazas híbridas se caracterizan principalmente por los siguientes atributos:

- Realizadas tanto por amenazas estatales, como por una variedad de actores no estatales.
- Materializadas tanto por unidades separadas como también por una misma unidad, con la particularidad que debían estar dirigidas y coordinadas operativa y tácticamente dentro de un espacio de batalla principal, con el objetivo de lograr efectos sinérgicos en las dimensiones físicas y psicológicas del conflicto.
- Debían accionar en terrenos altamente complejos como selvas, zonas urbanas, zonas montañosas, entre otras, ya que proporcionaba a los defensores y fuerzas más débiles, una serie de situaciones ventajosas que compensaban la inferioridad frente a una superioridad convencional.
- Su tendencia radicaba en no aceptar normas y reglas, explotando por lo tanto, formas inesperadas, modos de ataques despiadados y uso indiscriminado de la tecnología de manera única e imprevista.
- No se constituían como un conjunto de retadores distintos con métodos alternativos o diferentes, sino por medio de su convergencia de fuerzas y medios en guerras multimodales o híbridas.
- Mezclaban la letalidad del conflicto estatal, con el fervor fanático y prolongado de la guerra irregular.
- Podían tener una estructura política jerárquica, junto con células descentralizadas o unidades tácticas en red.
- Estas amenazas (Estados, grupos patrocinados por el Estado o actores autofinanciados) aprovechaban el acceso a las capacidades militares modernas, incluyendo sistemas de mando y control encriptados y misiles portátiles aire-tierra.
- Promovían la insurgencia empleando emboscadas, IED y asesinatos coercitivos.
- Podrían incluir estados que combinasen capacidades de alta tecnología, como armas antisatélite, terrorismo y guerra cibernética dirigida contra objetivos financieros.
- Buscaban la victoria mediante la fusión de tácticas irregulares y los medios más letales a disposición, para atacar y alcanzar sus objetivos políticos.

- El componente disruptivo provenía de la criminalidad.
- La actividad delictiva servía para sostener a la fuerza híbrida o para facilitar el desorden y la perturbación de la nación-objetivo.

Por su parte, un par de años más tarde y de manera complementaria en su texto Hybrid vs Compound War", Hoffman define amenaza híbrida, "como cualquier adversario que emplee de manera simultánea y adaptativa una mezcla fusionada de armas convencionales, tácticas irregulares, terrorismo y comportamiento delictivo en el espacio de batalla para lograr sus objetivos políticos" (Hoffman, 2009, p. 3). Si analizamos ambos textos, indudablemente se pueden identificar importantes elementos en común, los cuales se basan sustancialmente en la presencia de fuerzas y medios convencionales o regulares con el accionar simultáneo de fuerzas irregulares y también por la presencia de otros mecanismos de acción, como el terrorismo, el crimen y la acción delictiva cuyos objetivos ya se centraban en un nivel más amplio.

En otro orden de ideas y como señala Bowers, las amenazas híbridas combinan los puntos fuertes de una fuerza de combate irregular con diversas capacidades de una fuerza armada estatal, jugando actualmente un rol más destacado los asuntos de seguridad nacional. Asimismo, establece que no existía una definición unánime acerca de este tipo de amenazas en la bibliografía ni tampoco en el léxico militar. Alude entonces, a que en el Boletín de Entrenamiento 7-100 del Ejército de EUA, amenazas híbridas se definían como "la combinación diversa y dinámica de fuerzas regulares, fuerzas irregulares y/o elementos criminales que se han unificado para lograr efectos mutuamente beneficiosos" (2014, p. 30), señalando además, que un adversario hibrido completamente desarrollado tendría la capacidad de lograr la transición entre la guerra irregular o de guerrillas y la guerra sumamente convencional en formaciones del nivel compañía o superior.

Como resultado entonces, estas amenazas tendrían la cabida para emplear distintas capacidades, incluyendo medios cibernéticos, medios de comunicación social, comunicaciones protegidas, crimen organizado a través de redes trasnacionales y tecnologías avanzadas como es el caso del uso de UAV. Por lo tanto, y al realizar el

análisis teórico igual que con el exponente anterior, las principales características que definirían a una amenaza híbrida según este autor, radicarían principalmente en lo que a continuación se detalla:

- Mantención de un carácter celular y relativamente inconexo.
- Mantención de estrechos vínculos con la población civil, lo que hace dificultoso derrotar a la insurgencia, el terrorismo y el crimen organizado.
- Desarrollo de capacidades de combate avanzadas, para equipararlas con fuerzas militares no equipadas para la guerra de fuegos y maniobra de armas combinadas conjuntas y modernas.
- Capacidad de maduración, en donde los grupos armados podrán transitar de organismos asociados a pandillas con objetivos a corto plazo, a grupos armados organizados a un nivel que buscarán el logro de objetivos en el poder político y más aún, para aumentar su capacidad militar.
- Capacidad de actores no estatales para estudiar y deconstruir las vulnerabilidades de fuerzas armadas estatales, diseñando las contramedidas apropiadas.

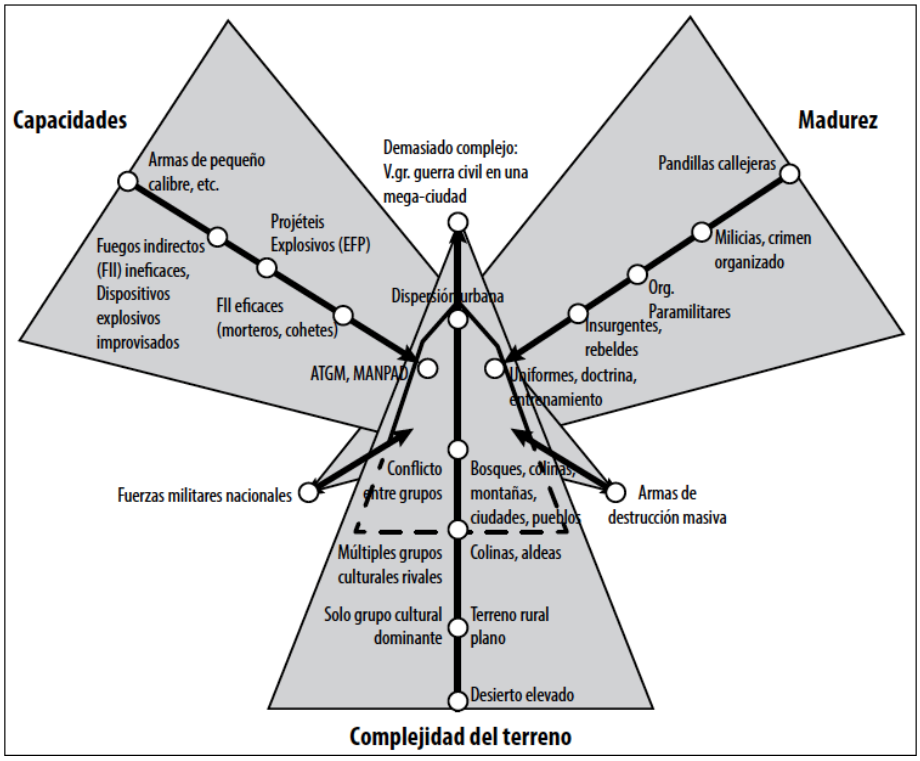
No obstante, Bowers también señala que estas amenazas para ser consideradas como tal, debían poseer las siguientes capacidades mínimas:

- Posesión de un tipo concreto de arma o tecnología en grandes números, como es el caso de misiles antitanques guiados (ATGM) o sistemas de defensa antiaérea (MANPADS), entre otras. Lo anterior, para ser empleadas bajo una visión estratégica en una operación de mayor envergadura y no sólo bajo una perspectiva individual y aislada.
- Entrenamiento adecuado para utilizarlas de correcta forma, ya sea como parte de una misma fuerza que se adhiere a organizaciones híbridas, o como parte de un patrocinador tercero estatal.
- Capacidad para mantener la sostenibilidad.

Por todo lo sostenido precedentemente, la metodología para identificar estas amenazas y sus capacidades radicaba en tres variables centrales que caracterizarían a una amenaza híbrida organizada, siendo éstas, la madurez, sus capacidades y su actuación en terrenos complejos, las cuales traslapan el accionar en los distintos niveles de la conducción militar. Por consiguiente y como se indica en la imagen 1, se pueden identificar los respectivos elementos que constituyen cada una de estas variables de análisis.

Imagen 1

"Intersección de Amenazas híbridas "



Nota: Antecedentes que representan la interacción entre: las capacidades, madurez y complejidad del terreno, variables desarrolladas en el análisis de una amenaza híbrida. extraídos de (Bowers, 2014, p. 34).

De igual manera y para complementar este análisis, aparecen otro autores más contemporáneos que se han referido a las distintas interpretaciones realizadas sobre lo híbrido y en ese sentido destacan autores como Guillem Colom Piella, quien expresa que si bien, estas amenazas híbridas se definen ampliamente por la integración de elementos

convencionales e irregulares, actualmente lo híbrido está siendo utilizado por académicos y políticos para describir de casi exclusiva, las actividades que está realizando el Kremlin para proyectar su Política Exterior. Esto se sustenta a través del concepto de guerra política, en donde un Estado “emplea todos los instrumentos a su disposición para debilitar y desmoralizar política, militar, económica o socialmente al adversario” (Colom, 2019, p.3).

Por esta razón, el autor hace hincapié en que las “cosas híbridas” han experimentado un largo viaje conceptual desde el 2006 con el choque entre Israel y Hezbollá, cuando se basaba enfáticamente en una idea para definir sólo la combinación de elementos convencionales e irregulares, hasta el 2019, en donde por el contrario, las concepciones abarcan “desde cualquier actividad informativa, cibernética, subversiva o cinética realizada bajo el umbral del conflicto armado o cualquier manifestación de guerra política que signifique el empleo de medios diplomáticos, informativos, militares, económicos, financieros, legales o de inteligencia en tiempos de paz, crisis o guerra” (p. 4,5).

Reforzando lo anterior, y como expresa Quiñones de la Iglesia (2020), toma una especial importancia el concepto de Zona Gris (GZ), generada por el actor híbrido que se mueve y actúa con impunidad entre sus imprecisos límites, puesto que es él, quien los establece y en donde a través de operaciones de información, desinformación, coerción política y económica y operaciones en el ciberespacio, entre otras, buscará la mayor asertividad en sus acciones. Así, la única línea que se autoimpone el actor híbrido en la GZ, es mantenerse bajo el umbral del conflicto armado ya que traspasarlo significaría que la estrategia en la que se inscribe ha cambiado de fase.

Recapitulando acerca de las ideas de Colom y llevando estas concepciones a un ámbito militar, señala que entre algunos elementos característicos que destacan en el siglo XXI acerca de la construcción híbrida, se revelan las siguientes ideas:

- Intervención de Estados de manera directa o delegando su actuación a agentes domésticos o *proxies*[4], hasta guerrillas, terroristas, redes criminales o contratistas militares privados (mercenarios).
- Utilización novedosa de armas sencillas, empleo de sistemas de armas sofisticados transferidos por Estados, utilización de armamento pesado o tecnologías de uso dual disponibles en el mercado. A su vez, empleo irregular de medios informativos.
- Empleo desde acciones convencionales limitadas, actos terroristas, insurgencia, ciber operaciones en todo el espectro, ocultación y engaño o propaganda multicanal.
- Empleo de sistemas de posicionamiento, SIGINT, OSINT y redes sociales, drones, comunicaciones avanzadas y toda una gama de INFOOPS, utilizando vectores, guerra electrónica, operaciones psicológicas, engaño, ciberoperaciones e instrumentos de control social, manipulación de la información, chantaje, extorsión o presión de medios o redes sociales.
- Desde actividades legales hasta delictivas con estrecha colaboración con el crimen organizado.
- Desmoralización del adversario sin empleo de la fuerza militar cinética.
- Empleo de tácticas asimétricas difusas entre la población.
- Explotación de las debilidades políticas, sociales, jurídicas, morales, económicas, demográficas o militares del adversario.

De lo anterior, se infiere que muchas de estas proposiciones más actualizadas, se basaron en fundamentos precedentes, como es el caso de las publicaciones realizadas por dos coroneles chinos quienes fueron conocidos por la concepción de la Guerra sin Restricciones o “Guerra Más Allá de los Límites”. Así, Qiao Liang y Wang Xiangsui, no sugirieron que la guerra fuera sin restricciones morales o más allá de cualquier límite, sino que buscaron ampliar la definición y comprensión de la guerra más allá de su dominio militar tradicional, expresando lo siguiente:

[4] El concepto de agente proxies”, se refiere a un (representante), agente o sustituto autorizado para actuar en nombre de otra persona (máquina o entidad). Son *tipos de conflictos en los que se distingue un conflicto interno entre distintos bandos o actores que se engloba como parte de otra rivalidad entre potencias o actores externos.*

> la gran fusión de tecnologías está impulsando a los dominios de la política, la economía, el Ejército, la cultura, la diplomacia y la religión a superponerse entre sí. Los puntos de conexión están listos y la tendencia hacia la fusión de los distintos dominios es muy clara. “Todas estas cosas están volviendo cada vez más obsoleta la idea de confinar la guerra al dominio militar y de utilizar el número de bajas como medida de la intensidad de una guerra”. (Hoffman, 2007, p. 22).

De este modo, comprendieron que los conflictos desde de la Guerra del Golfo en 1991, habían sufrido radicales transformaciones producto de los avances tecnológicos, pero también se percataron que ciertas acciones que iban más allá de las convencionales habían florecido, lo que sin duda alteró la forma de analizar los conflictos y operaciones en particular.

De esta manera, y con un asombroso énfasis, Liang y Xiangsui (1999), señalaron que este este tipo de guerra significaba que todos los medios estarían listos, que la información sería omnipresente y el campo de batalla estaría en todas partes, las armas y la tecnología se podrían superponer a voluntad, lo que significaba que todos los límites se encontraban entre los dos mundos de guerra y no guerra, de lo militar y no militar, y también significaba que muchos de los principios de combate serían modificados. Nuevamente y en concordancia, Quiñones de la Iglesia (2020), afirma que la destacada publicación realizada por ambos coroneles podía considerarse como la primera aproximación concreta al concepto de “Guerra y amenaza Híbrida”, en donde la guerra se había ampliado a otros ámbitos más allá de los tradicionales, destacándose dominios como el político, económico, recursos críticos, religión, cultura, redes sociales, medioambiente e incluso el espacio exterior.

Ahora bien, en nuestro ámbito nacional y de manera complementaria, algunos destacados representantes en materias de defensa, y por medio de un exhaustivo análisis crítico de diferentes teorías, han construido sus fundamentos sobre estas nuevas amenazas. En tal sentido, Arteaga (2020), señala que estas amenazas utilizan una amplia gama de técnicas y procedimientos, como son las acciones de desestabilización, ciberataques, apoyo a

grupos opositores, operaciones de información y desinformación, acciones diplomáticas, empleo de fuerzas irregulares, grupos que se relacionan con el crimen organizado, empleo de fuerzas especiales y de fuerzas y capacidades convencionales.

De la misma manera, el CEEAG postula a que:

> los actores en la disputa, recurren a acciones tanto convencionales como asimétricas que son dispuestas por la autoridad política del Estado, atendiendo a que implican riesgos políticos y jurídicos en el contexto internacional, debido a que dichas acciones asimétricas corresponden, entre otras, a operaciones de desinformación, al accionar terrorista, a brindar apoyo a grupos opositores o disidentes del Estado contendor, a operaciones de desestabilización política, a ciberataques e, inclusive, al accionar vinculado con el crimen organizado (2020, p. 16).

En conclusión, los párrafos anteriores permiten identificar una notoria evolución en cuanto a la conceptualización de estas amenazas, reconociendo en los primeros teóricos una fuerte tendencia hacia el ámbito militar en donde a través del uso cinético de diferentes recursos y por medio de diferentes modalidades, se buscaba la consecución de los objetivos políticos y estratégicos. Sin embargo, en la indagación de autores más contemporáneos, evidenciamos otros métodos y mecanismos de acción y objetivos, los cuales se enmarcan en el empleo de todos los instrumentos del poder de un estado, de operaciones multidominio, acciones bajo el umbral del conflicto y del uso del ciberespacio como herramienta fundamental para erosionar e influir en los Estados, en donde el empleo de la fuerza no cinética adquiere gran connotación desde el más alto nivel de la planificación y conducción.

En razón de los párrafos anteriores, se estima necesario realizar una síntesis con las principales características identificadas en esta conceptualización, lo que contribuirá a realizar un análisis más específico con la finalidad de establecer posteriormente ciertas cualidades equivalentes tanto de esta base teórica académica, como también de la base doctrinaria nacional y extranjera la cual será abordada posteriormente

Tabla 1

"Características generales de amenaza híbrida según diferentes exponentes"

Exponente teórico	Características principales sobre amenaza híbrida
Hoffman, F. (2007, 2009)	- Empleo de diferentes modalidades de guerra (capacidades convencionales, tácticas y formaciones irregulares). - Terrorismo. - Delincuencia. - Criminalidad. - Amenazas estatales y actores no estatales. - Empleo de unidades separadas y por una misma unidad dirigidas y coordinadas operativa y tácticamente dentro de un espacio de batalla principal. - Empleo en terrenos altamente complejos. - Tendencia en no aceptar normas, reglas y leyes. - Mezcla de letalidad de conflicto estatal con guerra irregular. - Patrocinados por terceros Estados. - Capacidad de estructura política jerárquica junto a células descentralizadas. - Promoción de la insurgencia.
Bowers, C. (2014)	- Combinación de fuerzas irregulares con diversas capacidades de una fuerza armada estatal. - Capacidad de mutación de guerra irregular a convencional. - Empleo de distintas medios y capacidades (cibernéticos, comunicación social). - Presencia de crimen organizado. - Empleo de avanzada tecnología. - Mantención de un carácter celular y relativamente inconexo. - Estrechos vínculos con la población civil. - Capacidades de combate avanzadas. - Mutación de organismos asociados a las pandillas a grupos armados organizados. - Empleo y capacidades de actores no estatales. - Posesión de gran número de armas, empleado bajo una visión estratégica y no solo individual. - Capacidad de sostenibilidad.
Colom, G. (2019)	- Integración de medios y elementos convencionales e irregulares. - Empleo de la totalidad de los instrumentos de un Estado (Político, Militar, Económico, Social). - Empleo de medios cibernéticos, subversivos o cinéticos bajo el umbral del conflicto. - Empleo de medios diplomáticos, informativos, militares, económicos, financieros, legales o de inteligencia en paz, crisis o guerra. - Empleo de operaciones de información, desinformación y ciberoperaciones. - Intervención de Estados en forma directa o por delegación. - Actuación de mercenarios. - Delincuencia. - Utilización novedosa de armas ligeras, sencillas y también armamento pesado y

Exponente teórico	Características principales sobre amenaza híbrida
	sofisticado. - Empleo de acciones convencionales, irregulares, asimétricas, terrorismo, insurgencia. - Empleo no cinético de la fuerza.
Arteaga, M.	- Uso de acciones de desestabilización. - Ciberataques. - Apoyo a grupos opositores. - Operaciones de información y desinformación. - Acciones diplomáticas. - Empleo de fuerzas irregulares. - Crimen organizado. - Empleo de fuerzas especiales. - Empleo de fuerzas convencionales.

Nota: tabla que explica las características principales de la amenaza hibrida según diferentes autores.

2.3 Amenaza híbrida y su fundamentación a base de la Directivas Políticas para el Sector Defensa y la Doctrina Nacional y Extranjera.

2.3.1 Directivas Políticas para el Sector Defensa

Nuestro país y diversas instituciones no se han mantenido ajenos e indiferentes ante estos nuevos actores, mecanismos de acción y propósitos propios de estos tipos de guerra y amenazas. Es por eso, que en el ámbito de nuestra Defensa Nacional, si bien se aborda el concepto híbrido en una forma incipiente, este no contaría con una base sólida y robusta que defina una categorización o ejemplificación concreta de estas amenazas para ser empleadas en los procesos propios de planificación en las operaciones. En consecuencia, existen principalmente dos textos a nivel político y estratégico que abordan estas nuevas contextualizaciones de amenazas, siendo el Libro de la Defensa Nacional (LDN) publicada en el 2017 y posteriormente la Política de Defensa Nacional (PDN) publicada en el 2020.

Así, el LDN expresa en su capítulo V, que “la mayoría de los conflictos contemporáneos no se desarrollan en el ámbito interestatal, diferenciándose del conflicto tradicional, con la

implicancia de nuevas conceptualizaciones y categorizaciones". En consecuencia, se ha acuñado el concepto de "Guerra Híbrida", la cual incorpora características del conflicto contemporáneo e incluye el hecho que las amenazas puedan provenir tanto del Estado como de actores No-Estatales, y que el uso de tácticas y formas de enfrentamiento pueden ser convencionales e irregulares, siendo la población civil, la principal víctima. (MDN, 2017, p. 73).

Si analizamos lo descrito, dilucidamos que la información y fundamentos doctrinarios y bibliográficos existentes en nuestro contexto nacional hasta la fecha de publicación de este texto, eran escuetos y carentes de bases consistentes que avalaran este tipo de conflicto y las amenazas asociadas a su ámbito. Es por lo anterior, y siguiendo con la idea y contextualización de los actuales conflictos, que posteriormente en el año 2020, la Política de Defensa Nacional de Chile, incluye en sus contenidos el concepto de naturaleza híbrida de las potenciales amenazas, en donde establece que:

> en los últimos años a nivel mundial las amenazas de naturaleza híbrida han aumentado, por medio de acciones hostiles tanto de origen interno como externo, combinando métodos y capacidades convencionales y no convencionales, por medio de campañas de desinformación, ciberataques, terrorismo, sabotaje, insurgencia, entre otros. Esto, coordinado o ejecutado tanto por agentes estatales como otros grupos u organizaciones no estatales, manteniéndose en general bajo el umbral de agresión que conlleve una respuesta militar convencional por parte de los Estados afectados. Lo anterior, con el propósito de dañar a la población, infraestructura crítica, desestabilizar los procesos políticos democráticos o debilitar la capacidad de respuesta de un Estado frente a amenazas a su soberanía, integridad territorial o independencia política. (MDN, 2020, p. 43).

Al analizar con una visión crítica este texto, difiere considerablemente del antecesor, ya que en este, se plasman en una forma más precisa los fines, modos y medios de este tipo de categorización de amenazas. Por el contrario, el LDN plantea en una forma excesivamente amplia sólo algunas consideraciones relacionadas a sus modos y medios,

quedando en deuda sus fines, los cuales se supeditan solamente al daño contra la población civil.

De igual manera, en la PDN, se hace referencia a la capacidades estratégicas que se deben alcanzar para enfrentar amenazas híbridas, manifestando que “actualmente no es posible enfrentar amenazas del tipo híbrido desde un enfoque tradicional del empleo de los elementos del poder nacional. Ante eso, la Defensa tiene la obligación de explorar aproximaciones estratégicas novedosas, coordinando esfuerzos en ciberdefensa, inteligencia, operaciones especiales y fundamentalmente la capacidad de maniobrar en el ambiente de la información, dada la disputa por la superioridad de influencia en el dominio cognitivo del conflicto”. (2020, p. 96,97).

En conclusión, se deduce que el espíritu de estos textos directivos se enfocan principalmente a un esfuerzo de concientizar al sector Defensa con una mirada prospectiva para asumir los desafíos y retos como resultado de los nuevos escenarios, conflictos y amenazas, los cuales rápidamente están emergiendo, propendiendo con lo anterior, a desarrollar e incrementar una serie de capacidades y atributos necesarios para poder sortear y contrarrestar el impacto de éstas, tanto en Seguridad como en Defensa. Lo anterior, a través de una serie de acciones como lo son la coordinación interagencial en materias de ciberseguridad, inteligencia, cooperación internacional, incluyendo la coordinación entre Defensa, policías, extranjería y aduanas.

A su vez, en acciones concretas para potenciar y aumentar las capacidades de operaciones en ambientes multidominio con énfasis en el dominio cognitivo o de la información, integración de fuerzas altamente entrenadas con capacidad de maniobrar en el ambiente de la información y escenarios de amenaza híbrida, para finalmente, potenciar las capacidades de anticipación, elaboración de escenarios, doctrina, alistamiento operacional y respuesta, entrenamiento conjunto e interagencial para operar en este ambiente.

2.3.2 Doctrina Nacional

Es pertinente señalar, que en nuestra doctrina institucional el concepto de amenaza híbrida no se ha abordado y desarrollado como tal y de manera explícita. Lo anterior, se pudo constatar analizando una serie de reglamentos institucionales, los cuales, principalmente abordan otras definiciones que muchas veces tienden a confundir, como es el caso de conflicto, guerra y amenaza irregular y asimétrica. No obstante, la guerra híbrida en nuestra reglamentación, es entendida como "la combinación de operaciones de un Estado contra otro o más Estados a través de terceros y métodos no atribuibles al Estado agresor, que no alcanzan a constituir un conflicto armado" (DD-10001, 2019, p. 31), no haciendo referencia directa a la definición de amenaza.

Sin embargo, y como una forma de indagar más en esta definición, se realizó la siguiente pregunta a personal especialista en inteligencia, con el propósito de dilucidar sobre la percepción y existencia de esta tipología de amenazas en nuestro contexto nacional, lo que sin duda contribuirá a las conclusiones de esta investigación.

1) *¿Considera que actualmente nuestra institución a través del trabajo directivo y operativo de sus organismos de inteligencia, analiza amenazas de naturaleza híbrida?*

Una vez analizadas las respuestas, se concluyó de lo anterior, que el análisis de nuevas amenazas bajo el contexto de los últimos EE-C declarados en nuestro país, se plantea la posibilidad de modificar o cambiar la percepción de las amenazas en el ámbito nacional. En términos de seguridad exterior, se espera que los organismos de inteligencia estén capacitados para analizar y enfrentar amenazas de esta índole, mientras que en seguridad interior se hace más complejo, debido a que actualmente existe una brecha en términos de doctrina, estructura, recursos humanos, capacitación, tecnología y material frente a estas amenazas, lo que debería ser priorizado. No obstante, aunque la doctrina institucional no aborda completamente esta tipología de amenazas, el trabajo directivo y operativo las considera en cuanto a su naturaleza y formas de empleo, ya que, según los encuestados, la institución se ha visto involucrada en el análisis de estas amenazas

debido a su impacto evidente en el país en el último tiempo y sus formas de empleo los cuales se alinean con los métodos en el accionar.

2.3.3 Doctrina Extranjera

Con respecto a este punto, existen organismos extrainstitucionales ligados a la Defensa y seguridad que tienen internalizadas en su doctrina el concepto de amenaza híbrida. lo anterior, debido a que en sus panoramas y escenarios tanto regionales como internacionales, han tenido que desarrollar mecanismos y capacidades para enfrentar una serie de nuevas amenazas que han buscado erosionar diferentes organismos del Estado, influir en sus poblaciones a través del crimen organizado, narcotráfico y delincuencia desatada, e incluso atacar organismos públicos y privados por medio del ciberespacio.

Es así, como el Ejército de Estados Unidos ha incorporado esta definición en sus textos más recientes como el IPB, definiendo amenaza híbrida como:

> la combinación diversa y dinámica de fuerzas regulares, fuerzas irregulares, fuerzas terroristas o elementos criminales unificados para lograr efectos de beneficio mutuo. Así, una amenaza híbrida también busca lograr propósitos compartidos o separados, objetivos compartidos o separados, o cualquier combinación de efectos, propósitos u objetivos. (ATP 2-01.3, 2019, p. 5-3).

Sin embargo, y sí se profundiza en este texto doctrinario, se puede obtener una valiosa información acerca de otras particularidades que caracterizan a este tipo de amenazas, siendo las siguientes:

- Combinación, asociación o afiliación de dos o más entidades representadas por una amenaza regular del Estado-nación, una amenza irregular del Estado-nación, organizaciones insurgentes, unidades guerrillerras y organizaciones criminales.
- Buscan la sinergia y sincronización entre las operaciones convencionales y no convencionales.

- Buscan introducir complejidad adicional mediante el uso de variadas fuerzas, tecnologías, dominios y técnicas en constante cambio.
- Financiados por agrupaciones afiliadas como grupos no militares o paramilitares como carteles criminales, insurgencias, células terroristas o mercenarios.

En consecuencia, si apelamos a un ejemplo sobre esta conceptualización, en el 2006 Hezbolá mezcló capacidades convencionales (armas antiblindaje, cohetes portátiles, redes de mando y control), con tácticas irregulares (guerra de información, combatientes no uniformados y empleo de la población civil como escudos). Esto resultó en un estancamiento táctico y en un revés estratégico para las fuerzas armadas de Israel.

Por otra parte, la doctrina del Ejército de Colombia define amenaza híbrida como:

> la combinación diversa y dinámica de fuerzas convencionales, fuerzas irregulares, fuerzas terroristas y/o elementos criminales unificados, para lograr efectos mutuamente beneficiosos, incluye actores estatales y no estatales que pueden llegar a emplear diversos métodos tradicionales de una guerra convencional, junto con otros de la guerra irregular, como la subversión, la insurgencia, la guerra de guerrillas, el sabotaje, el terrorismo y actividades criminales que se fusionan de manera sincronizada y coordinada con ataques a los sectores vulnerables de un Estado-nación (organización política del Estado, campos militar, económico, social, jurídico y educativo), haciendo uso del espacio virtual o ciberespacio como herramienta de mayor aplicación. (MCE 3-24.0, 2021, p. 1-1).

Además, señala que son generalmente Estados-nación, organizaciones, personas, grupos o condiciones que pueden hacer daño o destruir la vida, los recursos vitales o las instituciones. Con respecto a lo anterior, la definción doctrinaria del Ejército de Colombia, hace énfasis en los elementos del poder nacional como posibles objetivos de estas amenazas, la cual no se considera explícitamente en la doctrina estadounidense.

Algo semejante ocurre con el Ejército español, el cual en su publicación MDN (2012), señala que las amenazas híbridas se definen como las combinaciones diversas y dinámicas de capacidades convencionales, irregulares, terroristas y criminales. Del mismo modo, el texto PD3-308 (2014) utilizado por su Ejército de Tierra, las define como amenazas de naturaleza difusa, interconectada y de dificultosa predicción, debido a la mezcla de formas de combate y actividades irregulares, como es el caso de la insurgencia, terrorismo, crimen organizado, acciones delictivas y desórdenes públicos, ya sea a nivel nacional o exterior.

En complementación a lo anterior, y como señala Cárdenas (2022), según lo establece la Estrategia Nacional de Ciberseguridad de 2019 del Gobierno de España, son acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios militares tradicionales, ciberataques, operaciones de manipulación de la información o elementos de presión económica.

Por otra parte, las amenazas híbridas son una fuente de inseguridad internacional y prevenirlas es una acción sumamente dificultosa debido a su rapidez, intensidad y a la gran escala que pueden alcanzar. Es por esto, que la UE y la OTAN, las contemplan entre sus principales líneas de actuación sobre seguridad. La Comisión Europea identificó el carácter coercitivo y subversivo de estas amenazas expresando su pronunciamiento en el 2016.

Así, la OTAN ha asumido estos desafíos producto de los rápidos cambios en el sistema internacional, lo que ha desencadenado en que ambas organizaciones hayan adquirido el compromiso de cooperar y mejorar su capacidad para prevenir y responder a estos fenómenos. Por consiguiente, la OTAN se refiere a la amenaza híbrida como una combinación de medios militares y no militares, como también encubiertos y manifiestos, como es el caso de la desinformación, los ciberataques, la presión económica, el despliegue de grupos armados irregulares y el uso de fuerzas regulares. En tal sentido, los

métodos híbridos se utilizan para difuminar las líneas entre la guerra y la paz e intentar sembrar dudas en las poblaciones.

La UE, también declara que estas amenazas combinan actividades militares y no-militares convencionales y no-convencionales que pueden ser utilizadas de manera coordinada por actores estatales y no-estatales para lograr sus objetivos políticos. Las campañas híbridas son multidimensionales, combinando medidas coercitivas y subversivas, utilizando herramientas y tácticas tanto convencionales como no convencionales. A su vez, estas amenazas apuntan a vulnerabilidades críticas y pretenden generar confusión para dificultar la toma de decisiones rápida y efectiva. Las amenazas híbridas pueden abarcar desde ataques cibernéticos a sistemas de información críticos, pasando por la interrupción de servicios críticos como el suministro energético o servicios financieros, hasta el debilitamiento de la confianza pública en las instituciones gubernamentales o la profundización de las divisiones sociales. Como la atribución es difícil, estos desafíos requieren medidas específicas y coordinadas para contrarrestarlos.

Finalmente, tomando en consideración la totalidad de las posturas mencionadas, a continuación se plasman las principales ideas acerca de la amenaza híbrida desde la perspectiva doctrinal, lo que complementado con la revisión bibliográfica teórica de los exponentes académicos mencionados en los pasajes anteriores, permitirán establecer las concordancias para determinar ciertas cualidades equivalentes de esta tipología de amenazas.

Tabla 2

"Características generales de la amenaza híbrida según directivas y doctrina de países de referencia"

Fuente directiva y doctrinaria	Características principales sobre amenaza híbrida
	- Participación de organismos estatales y de actores no estatales. - Empleo de tácticas y formas de enfrentamiento convencionales e irregulares. - Objetivo principal es la población civil.
	- Participación de agentes estatales y no estatales. - Combinación de métodos y capacidades convencionales y no convencionales. - Uso de campañas de desinformación, Ciberataques. - Terrorismo. - Sabotaje. - Insurgencia. - Empleo bajo el umbral del conflicto. - Daño a la población como objetivo, IC, desestabilización de procesos políticos democráticos y objetivos nacionales de un Estado.
	- Combinación diversa y dinámica de fuerzas regulares, irregulares, terrorismo y crimen organizado. - Sinergia entre operaciones convencionales y no convencionales. - Empleo de tecnología. - Sostenimiento y financiamiento por agrupaciones afiliadas (grupos no militares o paramilitares como carteles criminales, insurgencias). - Terrorismo.
	- Combinación diversa y dinámica de fuerzas convencionales, irregulares, terroristas y criminales unificados. - Participación de actores estatales y no estatales. - Empleo fusionado y sincronizado de diversos métodos tradicionales de una guerra convencional con métodos de una guerra irregular (subversión, insurgencia, guerrillas, sabotaje, terrorismo y crimen organizado). - Ataques a sectores vulnerables del Estado-nación (organización política estatal, ámbito militar, económico, social, jurídico y educativo). - Empleo del espacio virtual o ciberespacio.
	- Combinación de capacidades convencionales, irregulares, terroristas y criminales. - Formas de combate convencionales e irregulares (insurgencia, terrorismo, crimen organizado, acciones delictivas, desorden público).
	- Combinación de medios militares y no militares encubiertos y manifiestos. - Empleo de operaciones de desinformación, ciberataques, presión económica. - Despliegue y empleo de medios regulares e irregulares.

Fuente directiva y doctrinaria	Características principales sobre amenaza híbrida
	- Combinación de actividades militares y no militares convencionales y no convencionales. - Participación de actores estatales y no estatales. - Campañas multidimensionales. - Empleo de medidas coercitivas y subversivas. - Vulnerabilidades críticas como objetivo. - Empleo de ataques cibernéticos, infraestructura crítica, sistemas financieros. - Influencia cognitiva en la población creando desconfianza en las instituciones gubernamentales y profundización de las divisiones sociales.

Nota: Cuadro de características principales de la conceptualización de una amenaza híbrida extraída de textos directivas nacionales y textos doctrinarios de países de referencia.

2.4 Identificación de cualidades equivalentes sobre una amenaza híbrida.

Como se mencionó en la metodología capitular, y a base de la revisión bibliográfica realizada, se establecieron como resultado del análisis tanto de autores que plasmaron sus ideas teóricas, como también de las directivas y de la información existente en la doctrina extranjera consultada, las siguientes cualidades equivalentes acerca de esta tipología de amenaza. Por lo anterior y desde una perspectiva militar, son las que se definen a continuación:

1. *Posibilidad de participación de actores estatales y no estatales.*
2. *Empleo de diferentes modalidades de guerra a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica, unificada y sincronizada.*
3. *Empleo del espacio virtual o ciberespacio para la realización de ciberataques,*
4. *Intensa participación de la población civil ya sea en apoyo o como objetivo en el conflicto.*
5. *Empleo de armamento de alta tecnología y bajo una perspectiva estratégica.*
6. *Empleo en terrenos altamente complejos.*
7. *Existencia de campañas multidimensionales.*

En atención a las cualidades equivalentes establecidas, es oportuno tratar de validar la aplicabilidad y existencias de ellas, con el propósito de robustecer este proceso metodológico. Así, esta ejemplificación se realizará a base del Conflicto del Líbano del 2006, el cual según expertos se constituyó como paradigma de este tipo de conflictos con sus amenazas asociadas y de las situaciones ocurridas hasta la fecha, en la Guerra de Ucrania, la cual producto de sus eventos, también ha sido catalogada dentro de esta topología de conflicto.

2.5 Caso de Estudio “Guerra del Líbano 2006” y relación actual con “Guerra de Ucrania”.

El MDN (2012), manifestó que Frank Hoffman, después de un estudio y análisis de diferentes conflictos para elaborar su teoría, llegó a la conclusión que esta guerra conjugaba en forma integral los ingredientes que la definían.

En otro sentido, también es pertinente expresar, que la guerra de Ucrania no consta de bibliografía, estudios sólidos y experiencias consolidadas, debido a que está en plena vigencia en la actualidad. Sin embargo, algunos informes y artículos realizados por centros de estudios, prensa e informes de gobierno de ambas partes, han cooperado para entender y cimentar una incipiente base contextual y bibliográfica de este conflicto.

Para lo anterior y para validar las cualidades equivalentes establecidas previamente, nos referiremos a las experiencias plasmadas por Anthony H. Cordesman y George y William D. Sullivan, en la publicación “Lecciones del 2006: Guerra Israelí – Hezbolláh” y al artículo escrito por Jorge Schunck “El Diseño Operacional de la Guerra del Líbano 2006”, además de artículos sobre sucesos y experiencias actuales de la Guerra de Rusia y Ucrania, conflicto que se mantiene vigente en la actualidad.

1) "Posibilidad de participación de actores estatales y no estatales":

Conforme a este primer punto, el conflicto implicó la participación de actores estatales y no estatales. Dentro de los estatales se presentaron por parte de Israel las FDI y como contraparte en el Líbano, el Ejército libanés que se involucró en la guerra junto a Hezbolláh en la frontera de ambos países. Por otra parte, en cuanto a la participación de actores no estatales, se desprende la organización política y militar de Hezbolláh y la participación de milicias palestinas la cuales accionaron en apoyo contra las fuerzas armadas y la población israelí. Consecuentemente, Hezbolláh demostró claramente su capacidad para accionar con actores no estatales para estudiar y deconstruir las vulnerabilidades de las fuerzas armadas de estilo occidental y diseñar las contramedidas adecuadas. Entonces, al recoger los fundamentos principales sobre la definición de conflicto y guerra híbrida, los cuales fueron expresados en el punto anterior, sin duda, al revisar estas acciones y experiencias, podemos identificar claramente lo que se postula de esta tipología.

Por otra parte, refiriéndonos a la Guerra de Ucrania, Bargués (2022), indica que actualmente, los enfrentamientos militares convencionales entre el ejército ucraniano y los separatistas prorrusos apoyados por Rusia se combinaban con tácticas irregulares para crear una zona gris y las tácticas híbridas se han intensificado desde el comienzo de la guerra y están haciendo esta contienda más impredecible, menos clara, incluso más brutal.

En tal sentido, en este conflicto se han evidenciado claramente la participación de actores estatales como Ucrania luchando para mantener la integridad territorial del país y defenderse de las fuerzas separatistas en las regiones de Donetsk y Lugansk. Por otra parte, Rusia ha estado involucrada en el conflicto desde el 2014, respaldando a las fuerzas separatistas en el este de Ucrania y proporcionando apoyo militar, logístico y financiero a los grupos separatistas y desplegando fuerzas rusas para la invasión. Asimismo, EE.UU y OTAN, han brindado apoyo político y militar, asistencia no letal, entrenamiento y asesoramiento a las fuerzas de Ucrania, además de imponer sanciones

económicas a Rusia en respuesta a su intervención en Ucrania. Además, también se evidencian la participación de actores no estatales, como los grupos prorrusos del Donetsk y Lugansk, declarando la independencia de estas regiones en el este de Ucrania, Grupo paramilitares y milicias ligados a movimientos nacionalistas ucranianos y prorrusos y finalmente voluntarios extranjeros, uniéndose a las fuerzas separatistas o apoyando a las fuerzas ucranianas.

2) ***"Empleo de diferentes modalidades de guerra a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica, unificada y sincronizada":***

En esta guerra, el mismo bando utilizó de forma simultánea la guerra convencional y la guerra irregular, con una clara tendencia de células altamente disciplinadas, bien entrenadas y distribuidas, las que pudieron competir con las fuerzas convencionales modernas israelitas, por medio de una mezcla de tácticas de guerrilla y tecnología en centros urbanos densamente poblados.

En cuanto a la organización de fuerzas, Hezbolláh estaba organizado horizontalmente, y en términos generales sus fuerzas de sustentaban bajo la existencia de dos tipos de combatientes. Por una lado, combatientes de élite o regulares, los cuales recibían entrenamiento avanzado con armas de alta tecnología, de tiempo completo y altamente disciplinados, y por otro lado, los combatientes de las aldeas y localidades fronterizas, denominados guardias de pueblo, los cuales eran veteranos guerrilleros que tenían experiencia durante la ocupación israelí[5] y se afiliaban vagamente a este grupo armado, no teniendo el mismo tipo de entrenamiento. Así, lo importante de esta organización era que los combatientes eran organizados en pequeños equipos, con una gran capacidad de autonomía y autosuficiencia, dotados para operar en forma independiente y sin la dirección de una alta autoridad durante largos periodos de tiempo, lo que representaba

[5] Guerra del Líbano de 1982: denominada por Israel "Operación Paz para Galilea", también conocida como Primera Guerra del Líbano. Conflicto armado que dio inicio el 6 de junio de 1982 cuando las Fuerzas de Defensa de Israel invadieron el sur del Líbano con el objetivo de expulsar a la OLP (Organización para la Liberación de Palestina), de dicho país.

una estructura de mando descentralizada y un alejamiento de las típicas organizaciones de los ejércitos árabes.

Si bien y conforme al texto, no se puede hablar de terrorismo en el sentido estricto de la palabra, el conflicto estuvo marcado por la presencia de ataques terroristas por parte de ambas partes. En este sentido se comprende que Hezbolláh era considerada una organización terrorista por varios países occidentales y al utilizar cohetes y misiles contra objetivos civiles transfronterizos, se pueden catalogar estos hechos como parte de este mecanismo de acción.

Finalmente, según algunos informes confidenciales, grupos criminales locales estuvieron involucrados en el tráfico de armas y drogas a través de la frontera del Líbano, lo que permitía obtener ganancias significativas en apoyo al financiamiento de los grupos armados. Del mismo modo, también se desprende la existencia de organizaciones criminales rusas que proporcionaron armas, como también, algunos grupos criminales locales involucrados en el saqueo de cuidades y pueblos del sur del Líbano, aprovechando la falta de control gubernamental en importantes áreas del país.

Con respecto a la guerra de Ucrania y producto de las declaraciones de organismos internacionales y principalmente de las altas autoridades ucranianas, se sigue pidiendo a la comunidad internacional, que se reconozca a Rusia como un Estado terrorista. Lo anterior, debido a que según las declaraciones, aterroriza y realiza ataques indiscriminados contra población, amenaza con una catástrofe nuclear y utiliza el suministro de alimentos para negociar (Lutska, 2022).

Asimismo, Cuevas (2023), señala que desde el comienzo de la guerra, el foco ha estado tanto en los ejércitos ucranianos y rusos como en las víctimas del conflicto armado. Sin embargo, existen otros protagonistas que han afectado altamente al transcurso y el desarrollo de la guerra: las empresas de mercenarios, donde destaca el famoso grupo Wagner, quienes han estado involucrados en múltiples batallas en el territorio ucraniano. Sin embargo, en oposición a Wagner y otras compañías militares privadas como el grupo

creado por el conglomerado energético ruso Gazprom y la futura agrupación del líder de Chechenia, se encuentran voluntarios extranjeros que se ofrecieron para alistarse en el Ejército de Ucrania, cuya participación, tanto de veteranos como de soldados principiantes, apunta a un trasfondo complejo y a posibles problemas judiciales dentro de las naciones de Occidente.

Todo lo anterior, deja de manifiesto que los actores en la guerra, utilizan modalidades convencionales e irregulares para llevar a cabo sus operaciones, sumado a otros mecanismos de acción, los que se categorizan dentro de este tipo de conflicto y modalidades del empleo.

3) "Empleo del espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación":

Hezbolláh comprendió que las capacidades obtenidas a partir de operaciones de información con un potente mensaje eran la clave para dominar el ambiente de la información en la guerra. En consecuencia, las publicaciones de Al Jazeera, Abu Dabi TV, Al Arabiya, LBC y Arab News, coincidieron en referirse a Hezbolláh como "La Resistencia" causando un efecto psicológico en la audiencia en contra del "enemigo sionista". Además, los registros de tráfico de internet en Medio Oriente, desde los días previos a las hostilidades, dieron cuenta de lo determinante que fue esta plataforma para expandir la narrativa islámica, la que permitió posicionar a Israel como "un país agresor" en diferentes sitios web oficiales, foros islámicos, blogs, sitios de distribución, grupos mediáticos y redes sociales.

En otro orden de ideas, la guerra del Líbano de 2006 fue un ejemplo temprano de la importancia de la ciberseguridad en los conflictos militares modernos, y destacó la necesidad de desarrollar estrategias efectivas para prevenir y responder a los ciberataques. Así, Uno de los ciberataques más notables fue el ataque a la página web del Ministerio de Defensa de Israel, que fue llevado a cabo por un grupo hacker llamado "K-159". El sitio web fue hackeado y se publicó un mensaje anti-israelí en su página principal.

También se informó de ciberataques a sitios web del gobierno libanés, así como a sitios web de noticias en el Líbano. Se cree que estos ataques fueron realizados por grupos pro-israelíes.

Por otra parte, el ciberespacio, la información y la realización de ciberataques, operaciones de información y desinformación, se han visto representadas por ambas partes en el conflicto de Rusia y Ucrania. Como se señala, la desinformación se ha intensificado desde la invasión rusa, obstaculizando la construcción de normas colectivas. El gobierno ruso ha acusado repetidamente a las fuerzas ucranianas de neonazismo y represión, utilizando estas afirmaciones para justificar su operación contra Ucrania. Estas tácticas de desinformación incluyen la difusión de videos falsos, hackeo de sitios web y ciberataques. En síntesis, el ciberespacio se ha convertido en un escenario clave en este conflicto, con Rusia lanzando ataques cibernéticos no solo en Ucrania, sino también en otros países como Polonia y Estados Unidos. Es así, como la desinformación y los ciberataques continúan generando confusión y complicando aún más la situación. (Bargués, 2022).

4) "Intensa participación de la población civil ya sea en apoyo o como objetivo en el conflicto":

Una de las características que se manifiesta en este tipo de guerras, es el apoyo de la población civil a la causa del conflicto. Por ende, una de las lecciones que se identificaron, fue la ayuda de la población libanesa a las tropas y grupos armados. De este modo, y como se expresa Cordesman y Sullivan (2007), una de las tácticas que utilizó Hezbolláh para fortalecer sus posiciones a lo largo de la frontera fue preparar a las aldeas amigas del sur del Líbano para ser utilizadas como refugios seguros y fortalezas en caso de ataques por parte de Israel. Del mismo modo, Hezbolláh construyó sus instalaciones en pueblos y áreas pobladas, usó instalaciones y viviendas civiles para almacenar armas y llevar a cabo sus actividades, e incrustó sus defensas y armas en áreas urbanizadas, utilizando al pueblo y civiles como armas defensivas y ofensivas.

Con respecto a lo anterior, oficiales de inteligencia de Israel, se quejaron del uso de la infraestructura civil, evidenciándose que en gran parte estas acciones fueron adoptadas sin el consentiminto de los residentes locales, sin embargo, otros analistas sugirieron que los lugareños del sur del Líbano, habián visto, desde el año 2000, una posible invasión israelí como algo inevitable, por lo que apoyaban estas acciones. Así, el mismo texto expresa que después de finalizada la guerra, y en una encuesta realizada por el periódico francés L'Orient-Le Jour, se identificó una división casi pareja entre los ciudadanos libaneses acerca de si Hezbolláh debería ser desarmado. La encuesta descubrió que el 51 por ciento de los encuestados querían que Hezbolá se desarmara, y el 49 por ciento restante se oponía. Sin embargo, en agosto de 2006 otras encuestas revelaron que el 87 por ciento de los libaneses apoyaba la resistencia de Hezbolá contra la invasión, ya que Hezbollah también ayudó a apaciguar reacciones violentas entre sus propios partidarios al enviar ayuda rápidamente a las áreas dañadas, lo cuál beneficiaba a la desprotegida población libanesa.

Refiriéndonos a la Guerra de ucrania, los civiles han sido un factor crucial en el conflicto, ya sea en apoyo o también como objetivos de él. Así, se presenta una situación preocupante en cuanto a la protección de los civiles, en donde Kiev ha sido acusado de poner en peligro la vida de los civiles al establecer instalaciones militares en áreas habitadas, incluyendo escuelas y hospitales. En consecuencia, Amnistía Internacional, señaló que tanto el ejército ucraniano como el ruso han violado el derecho internacional humanitario al convertir bienes civiles en objetivos militares y llevar a cabo ataques en zonas pobladas. Los informes indicaron que las fuerzas ucranianas utilizaron edificios civiles como bases y lanzaron ataques desde el interior de zonas habitadas, lo que resultó en la pérdida de vidas y la destrucción de infraestructura (El Comercio, 2022)

Por otra parte, se señaló que miles de civiles ofrecen sus servicios como voluntarios, muchos de ellos extranjeros, mientras que las autoridades distribuyen armamento. A su vez, otros de manera particular preparan artefactos de circunstancias como bombas molotov coordinando el apoyo. Se menciona además, que en la batalla por Kiev, las tropas rusas se enfrentan no solo a las fuerzas armadas ucranianas, sino también a miles de

civiles. En complementación, el alto mandatario ucraniano en un discurso televisado expresó “Detengan al enemigo en todas partes, donde sea que puedan”, “Quema vehículos enemigos con todo lo que puedas”, dijo el Presidente ucraniano Volodimyr Zelensky en un discurso televisado. (Marson y Hinshaw, 2022).

5) “Empleo de armamento de alta tecnología y bajo una perspectiva estratégica”

La guerra moderna experimentó cambios significativos impulsados por la tecnología, lo que ha permitió a fuerzas más pequeñas y menos equipadas a desafiar a ejércitos modernos basados en el poderío y sus recursos. Hezbolláh, en particular, demostró avances tecnológicos significativos en su armamento, incluyendo misiles y cohetes de diferentes alcances, respaldados por sistemas de mando y control sofisticados y tecnología de inteligencia, vigilancia y reconocimiento (ISR). Estos avances permitieron a Hezbolláh compensar la inferioridad numérica en el campo de batalla y utilizar tácticas asimétricas para enfrentarse a las fuerzas tradicionales de Israel. La sorpresa táctica radicó en el empleo de armamento sofisticado, como misiles, cohetes y armas antiblindajes, que desafiaron las expectativas de las Fuerzas de Defensa de Israel (FDI). Hezbolláh contó con una gran cantidad de unidades de artillería y utilizó drones con capacidad de atacar objetivos aire-tierra, lo cual representaba una capacidad novedosa en comparación a conflictos anteriores. Además, la combinación de pequeños cohetes tácticos y armas más antiguas demostró ser efectiva en la guerra asimétrica.

En lo atingente a la guerra de ucrania, si analizamos desde una perspectiva general el conflicto, se ha utilizado armamento, sistemas de armas y municiones dentro de los desarrollos tecnológicos actuales y propios de cada país. Sin embargo, otros estados han tenido que apoyar a Ucrania con armamento más sofisticado, para operar en diferentes dominios de manera adecuada y con cierta paridad en relación a los medios rusos. Sin embargo, organizaciones no estatales, como grupos separatistas y mercenarios prorrusos también han empleado armamento de mayor capacidad. En este sentido, Ibáñez (2022), menciona que organizaciones no estatales como el grupo Wagner, proporcionaron adiestramiento y asistencia a milicias, instruyéndolas en el empleo de diferentes sistemas

de armas ligadas a la ingeniería de combate, logística, operación de carros blindados y medios técnicos, lo que fundamenta la idea, que estas organizaciones no sólo han empleado y se han supeditado a armamento individual y ligero.

6) "Empleo en terrenos altamente complejos"

En términos de tácticas, Hezbolláh aprovechó las áreas urbanas y los edificios civiles como cobertura y protección, lo que les brindó ventajas en términos de ocultamiento, dispersión y la capacidad de realizar maniobras defensivas asimétricas en profundidad. Esta estrategia guerrillera, les permitió operar de manera efectiva sin depender de grandes instalaciones militares diseñadas para la defensa. En conjunto, el uso de tecnología avanzada, combinado con tácticas asimétricas y el entorno urbano, permitió a Hezbolláh desafiar y contrarrestar las tácticas tradicionales de las FDI en el conflicto. De esta manera, combatir en zonas urbanas y entre la población civil, permitió que estas estrechas áreas de ataque y el terreno proporcionaran a Hezbolláh, el tiempo y la cobertura para preparar emboscadas contra las tropas de las FDI, demostrando estar mejor entrenados y preparados que la mayoría de las fuerzas guerrilleras de la región. De igual forma, la lucha de Hezbolláh mostró cuán bien un actor no estatal puede hacer cuando obtiene armas avanzadas y tiene un fuerte apoyo externo de actores estatales como Irán y Siria.

Por otra parte, en la guerra de Ucrania, tanto las fuerzas ucranianas como las rusas se han visto limitadas por el terreno físico de las ciudades. Es así como Rusia ha tenido enormes dificultades para entrar en las zonas urbanas sufriendo pérdidas inesperadas y ha tenido que recurrir a tácticas de asedio en las ciudades. las batallas urbanas en Ucrania han visto una mezcla más amplia de fuerzas regulares e irregulares con mejores capacidades que en décadas pasadas. Rusia ha empleado tropas regulares, reclutas, fuerzas indirectas, mercenarios como el Grupo Wagner e incluso sirios para llevar a cabo operaciones en zonas urbanas con escasa consideración por las vidas civiles o las infraestructuras. (El Radar, 2023),

7) "Campañas multidimensionales"

Como señala Schunck (2017), conforme al Diseño Operacional elaborado para las operaciones de las Fuerzas de Defensa de Israel, dentro de los PDs sobre las fuerzas de Hezbollah, se establecían las siguientes :

– Ofensiva aérea sobre HVT y destrucción de lanzadores de misiles de largo y mediano alcance logrado, lo que corresponde a (medios aéreos).
– Control del mar, bloqueo de puertos y neutralización de envíos logísticos marítimos y terrestres a las posiciones defensivas lograda, lo que corresponde a medios (marítimos).
– Ofensiva terrestre hasta Bint J´Beil y el sur del Río Litani lograda, lo que corresponde a medios (terrestres).

Asimismo, en la guerra de Ucrania se han podido evidenciar acciones en los diferentes dominios por ambas partes en el conflicto, los que se han presentado tanto para configurar el campo de batalla o como para contribuir a las operaciones decisivas planteadas. Como indicó Muraviev (2022), las fuerzas rusas como parte de su planificación ofensiva, han realizado acciones en todos los dominios, ejemplo de lo anterior, se ejemplifica por la oleada de lanzamientos de misiles crucero, ataque de artillería, ciberataques a gran escala y guerra electrónica, asaltos aéreos y utilización de fuerzas especiales, empleo de grupos paramilitares vinculados al Estado, ataques terrestres con medios y sistemas de armas convencionales, bloqueos navales a los puertos ucranianos, entre otras. Es así y en complementación a lo anterior, que las batallas urbanas se han disputado en múltiples dominios, como el aéreo, el terrestre y el subterráneo, a diferencia de conflictos anteriores en donde predominó el dominio terrestre. (El Radar, 2023).

2.6 Síntesis del capítulo.

El propósito de este capítulo fue determinar que se define por amenaza híbrida. Lo anterior, se realizó a través de un proceso de análisis de contenido, el cual involucró en una primera parte, la descomposición del tópico a base de la fundamentación teórica

definida por ciertos autores, permitiendo con lo anterior, identificar características, particularidades y la evolución de este concepto de manera cronológica, es decir, desde su origen hasta la conceptualización de autores más contemporáneos. Sin duda, se evidenciaron similitudes en los fundamentos, pero también se evidenció una evolución acerca de elementos complementarios que se añadían a los postulados de los autores considerados.

Posteriormente y habiendo organizado las principales características de la amenaza híbrida por autor, se procedió a realizar la misma metodología con los textos directivos nacionales como es el caso del Libro de la Defensa Nacional y la Política de Defensa Nacional, como a su vez, con lo concerniente a la doctrina vigente de países de referencia como es el caso de Estados Unidos, Colombia, España, OTAN y EU, ya que como se explicó en forma precedente, estos países y organizaciones en la actualidad tienen internalizadas el concepto de amenazas hibridas, debido a que sus fuerzas armadas y policías combaten arduamente estas nuevas amenazas, las cuales se manifiestan y actúan a través de una variedad de mecanismos de acción. Gracias al análisis mencionado, se logró establecer ciertos parámetros en común, los cuales según la metodología del capítulo se denominaron cualidades equivalentes, sirviendo posteriormente para analizarlos a base de un estudio de casos y de esta manera poder validarlos para brindar un mayor grado de robustez y objetividad en el análisis de ellos.

En tal sentido, se desarrolló un breve análisis a base de la Guerra del Líbano del 2006 y de sucesos que están ocurriendo actualmente en la guerra de Ucrania, refiriéndonos a algunos factores significativos, ya que como se mencionó con anterioridad, según expertos, la guerra del Líbano se constituyó como paradigma de la guerra híbrida, en donde una parte más débil, accionó a través de acciones convencionales y asimétricas e irregulares. Lo anterior, sumado a lo que está ocurriendo de manera contemporánea en Ucrania, en donde si bien, no existen lecciones y estudios profundos y definitivos para categorizar este tipo de guerra, sin duda, la información que se publica día a día, permite relacionar ciertos sucesos ocurridos con estas acciones y amenazas. Lo anterior, debido a la identificación en el conflicto de actores estatales y no estatales, fuerzas y medios

regulares e irregulares, existencia de campañas multidimensionales y participación de la población civil en apoyo o como objetivos de las contrapartes.

No obstante, y a pesar que en ocasiones no existe un acuerdo robusto entre los autores y sus premisas, cabe resaltar que dejaron una fructífera inquietud en el estudio del conflicto y de igual manera, surgieron factores y fundamentos en común, como es el caso de la importancia de la tecnología, la materialización de acciones convencionales, irregulares y asimétricas, la interacción estatal y de actores no estatales, la inclusión de diferentes dominios como es el caso del espacio y el ciberespacio, como asimismo la participación de nuevos actores como protagonistas.

Finalmente, los antecedentes y la metodología aplicada en la elaboración del presente capítulo, permitieron responder la pregunta específica Nº1: *¿Qué es una amenaza híbrida?.* Lo anterior, como corolario de la indagación bibliográfica acerca de la descripción, análisis y conclusiones de la fundamentación teórica y de exploración de la información existente en nuestras directivas y de la doctrina extranjera. En conclusión y como resultado, se acuñó la siguiente definición de amenaza híbrida, sirviendo de apoyo para el resto de la investigación y de esta manera iniciar la indagación de las características de los procesos de preparación de inteligencia en estudio, siendo esta la siguiente:

"Combinación diversa y dinámica de diferentes modalidades de guerra a través de campañas multidimensionales, realizadas con la participación de actores estatales y no estatales a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica unificada y sincronizada, en terrenos altamente complejos y con el empleo de armamento de alta tecnología, empleando el espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación, complementado con una intensa participación de la población civil, ya sea en apoyo o como objetivo en el conflicto".

CAPÍTULO III
"PREPARACIÓN DE INTELIGENCIA PARA LAS OPERACIONES (IPO)"

3.1 Metodología del capítulo.

En el capítulo anterior, mediante el análisis bibliográfico de expertos en el ámbito de la seguridad y defensa, y de la información obtenida tanto en lo existente en nuestra esfera nacional, como también de diferentes textos doctrinarios de países de referencia, se logró cimentar una definición acerca de este tipo de amenazas. Lo anterior, contribuyendo al presente capítulo, el cual consiste en describir *¿en qué consiste el Proceso de Preparación de Inteligencia IPO?*, y cuál es su pertinencia de análisis en el contexto de amenazas híbridas, para de esta manera, dar respuesta al objetivo específico Nº2 de esta investigación.

Para lo anterior, la metodología capitular se desarrollará por medio del análisis documental, inicialmente a través de la identificación explícita sobre esta tipología de amenazas en la información existente en este proceso. Luego, se definirá y explicará señalando sus objetivos, estructura metodológica y componentes asociados, para finalmente realizar una descripción de sus factores analíticos, con el propósito de identificar la pertinencia de sus recursos evaluativos.

3.2 Revisión de la fundamentación y su relación bibliográfica con el contexto híbrido.

En relación con este segmento, es fundamental comenzar señalando que producto de la revisión bibliográfica, se evidenció que este proceso proporciona recursos valiosos en la evaluación de amenazas del tipo irregular, considerando que fue creado para este cometido. Sin embargo, no aborda de manera evidente el concepto de amenaza híbrida, ya que se centra en el análisis de amenazas del tipo criminal y terrorista, con la particularidad que este concepto no coexistía de manera habitual y de manera determinante en el lenguaje de los expertos en defensa y seguridad de la época. No obstante es de vital importancia analizarla y comprenderla, considerando que no existen

antecedentes de su metodología en nuestro ámbito institucional y el cual es uno de los motivos principales de esta investigación.

3.3 "Preparación de Inteligencia para las Operaciones" (IPO)

IPO fue un concepto y herramienta que surgió y se empleó en los primeros años de la década del dos mil, frente al análisis de amenazas irregulares, las cuales se manifestaron fuertemente en el transcurso y de manera posterior al atentado terrorista del 11 de septiembre del 2001 en Estados Unidos. Para tal efecto, mediante la revisión de la escaza fuente documental encontrada, basada principalmente en artículos escritos por Begert y Lindsay y el texto "Terrorism Early Warning 10 Years of Achievement in Fighting Terrorism and Crime", los cuales proporcionaron información importante sobre este concepto y metodología, se establecerá la estructura teórica sobre los antecedentes generales, surgimiento, fundamentación, objetivos de empleo y su metodología como herramienta de preparación de inteligencia.

3.3.1 Antecedentes Generales

Como se indicó, en forma posterior a los atentados señalados, algunos organismos de seguridad y defensa se percataron que debían establecer como prioridad en asuntos de Estado, medidas concretas de prevención, respuesta e investigación de conspiraciones criminales que apoyaran a movimientos extremistas y grupos terroristas. Es por esta razón, que algunas agencias policiales estadounidenses, fueron pioneras en el estudio de nuevas alternativas para luchar contra el terrorismo, buscando trabajar coordinadamente con instituciones de las fuerza armadas, organismos nacionales, civiles y otras entidades no gubernamentales, con el propósito de comprender la situación acerca de estas amenazas que emergían.

Así, y como manifiesta Martínez (2012), la inteligencia en esta tipología de guerra indudablemente estaría condicionada a nuevos métodos de recolección, análisis y difusión de información. Por lo tanto, a la hora de planificar y diseñar estrategias de inteligencia, se tendría que tener en cuenta principalmente que en un ambiente asimétrico, el esfuerzo de

los medios existentes diferían determinantemente de los empleados en operaciones convencionales. De esta manera, y ante estos nuevos escenarios, es que los medios de inteligencia debían mezclar sus procedimientos militares empleados en forma habitual, con otros relacionados a la investigación criminal y policial, ya que los objetivos habían mutado de las clásicas fuerzas convencionales, a las bandas o grupos, no teniendo una claridad en cuanto a sus organizaciones, ubicaciones, zonas de control, recursos a emplear y medios de financiamiento y sostenimiento; con la particularidad, que la tendencia radicaba en que se manifestaban a través de combatientes insurgentes y terroristas que se mezclaban con la población civil.

3.3.2 Conceptualización, propósitos y fundamentación.

Begert y Lindsay, fueron gestores en el desarrollo del concepto IPO, en un esfuerzo de actualizar la visión de la inteligencia para establecer posibles soluciones basadas en nuevos fundamentos y principios. En tal sentido, identificaron que debían basarse en la implementación de un concepto actualizado que acuñara en forma sincronizada la preparación, observación y el análisis. En esa perspectiva, definieron que IPO es un "sistema de red para la evaluación, análisis, previsión y toma de decisiones, que debía contar con reconocimiento, evaluación, psicología, componentes de análisis y predicción" (Begert y Lindsay, 2002, p. 139).

En este sentido, se comprende que su objetivo estaba relacionado íntimamente con el concepto de defensa activa, el cual se formulaba a través de enérgicas acciones de reconocimiento y vigilancia constante. Si analizamos lo anterior, no dista de las acciones y procedimientos que realizan actualmente y después de casi dos décadas, los organismos de inteligencia, los cuales, a través de diversos medios y recursos de obtención de información, materializados por elementos ISR, acciones HUMINT, OSINT y SIGINT, entre muchos otros, cumplen una labor fundamental en la materialización de estas acciones.

En función de lo planteado, el objetivo final de IPO, era disuadir al adversario por miedo a un cierto fracaso en la materialización de sus acciones. Por consiguiente, esta disuasión

alcanzada a través de la filosofía IPO, se basaba en “una capacidad de recopilación y análisis para prevenir cualquier intento de la acción del enemigo /OPFOR e identificar y derrotar a estos soldados criminales antes que puedan actuar”. (2002, p. 138).

Consecuentemente, se verificó que los analistas de inteligencia militar de aquellos años se centraban vigorosamente al análisis de elementos de los clásicos Órdenes de Batalla (ORBAT), como el tamaño, forma, capacidades, dispositivos, tácticas y procedimientos del adversario, asentándose concisamente en la doctrina de IPB de la década del noventa. Sin embargo, la inteligencia criminal o policial adquirió protagonismo, ya que tenía diferentes enfoques, puesto que se dirigía principalmente a términos de evidencia y pistas, buscando el tiempo de enlace, lugares y acciones a realizar, los que debían estar amparados en altos índices de certeza y oportunidad. Entonces, si profundizamos en su propósito y producto de las consecuencias arrastradas por el terrorismo internacional, el entorno de seguridad requería de enfoques actualizados, es decir, posiciones híbridas a la hora de conducir actividades ligadas a la función. Así, dentro de los propósitos principales de IPO, era tomar lo mejor de la inteligencia militar y policial, y de esta manera, contar con herramientas más adecuadas, ya que las existentes según los expertos, presentaban deficiencias. Lo anterior, se puede reforzar conforme al siguiente fundamento:

> IPO aborda la zona gris entre el crimen y la guerra, y por lo tanto, utiliza algunos elementos de cada uno de estos diferentes conceptos y usos de inteligencia. IPO, debería existir para lograr el objetivo de la detección y eliminación de la amenaza contraria. En su sentido más puro, su más valioso pero elusiva capacidad, es identificar la intención del enemigo / OPFOR antes del hecho, (2002, p. 138).

En este sentido, se comprende que la diversificación profesional y especialización era un factor vital, ya que se buscaba generar organismos multidisciplinarios que aportasen con sus conocimientos específicos a la tarea de comprender este ambiente altamente confuso, en donde expertos en construcción y estructuras, química, ciencias biológicas, salud, epidemiología, tecnología, ciberespacio, seguridad y los acordes al contexto que se requería, eran críticas al momento de planificar las tareas de inteligencia bajo la filosofía

de este concepto. En síntesis, resulta lógico expresar que según lo investigado hasta el momento, la mejor forma para implementar esta metodología, era a través de organismos descentralizados, por lo que se hizo alusión a organismos multidisciplinarios, equipos y entidades en red, los cuales, al igual que en la actualidad, debían poseer las características y capacidades de ejecutar tareas de planificación y de ejecución de tareas de inteligencia de manera íntegra conforme a un Ciclo de Inteligencia[6] bien estructurado, el cual estaba definido básicamente de manera similar al "Ciclo de Inteligencia" que se encuentra plasmado en nuestra doctrina vigente[7], fundamento que se puede observar conforme a las siguientes imágenes.

Imagen 2

"Ciclo de Inteligencia "

Nota: la imagen muestra el ciclo de inteligencia referido en el texto de (Sullivan y Bauer, 2008, p. 101), elaboración propia.

[6] Descripción genérica de las actividades a realizar por organismos de inteligencia independiente del nivel de conducción y situación, el que puede ser táctico, operacional o estratégico.

[7] RDI – 20002, "Reglamento Inteligencia", define Ciclo de Inteligencia, como un modelo funcional que establece la secuencia de actividades por planificar, obtener y procesar la información para que transformada en inteligencia, sea puesta a disposición de los usuarios. Comprende cuatro fases: dirección del esfuerzo de obtención, obtención de la información, análisis de la información y difusión y uso de la información.

Imagen 3

“Ciclo de Inteligencia”

Nota: la imagen hace referencia a nuestro ciclo de inteligencia vigente, establecido en el RDI – 20001 Reglamento de Inteligencia.

3.3.3 Operaciones en Red

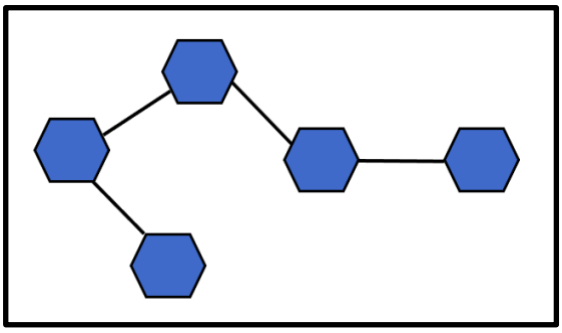
Haciendo alusión a lo anterior, una de las premisas para la implementación de este concepto radicaba en que su mejor adopción, era a través de acciones por medio de una red operativa, en contraposición a un sistema y estructuras altamente formales y jerarquizadas, ya que las organizaciones con un mayor grado de descentralización y bajo una adecuada organización en red, permitían acelerar las acciones de obtención de información, análisis, difusión y adopción de decisiones en beneficio del comandante.

En consecuencia, esta filosofía se generaba a raíz de la necesidad de afrontar las nuevas acciones que se manifestaban en el acontecer nacional y mundial. En concordancia, e indagando en textos más recientes sobre este ámbito, Korybko (2019), manifiesta que autores como John Arquilla y David Ronfeldt, plantearon el advenimiento de un nuevo tipo de conflicto social, en el que redes “sin líderes”, compuestas principalmente por actores no estatales, se aprovecharían de la revolución de la información para librar una lucha amorfa de baja intensidad contra los Estados u otros organismos. En efecto, y como lo señala el autor, se pueden identificar tres tipos de formaciones en red en las organizaciones

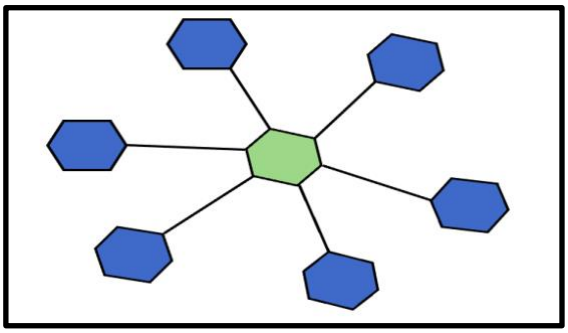
irregulares ligadas al terrorismo, crimen y narcotráfico, las que se ejemplifican de acuerdo con las siguientes imágenes:

Imagen 4

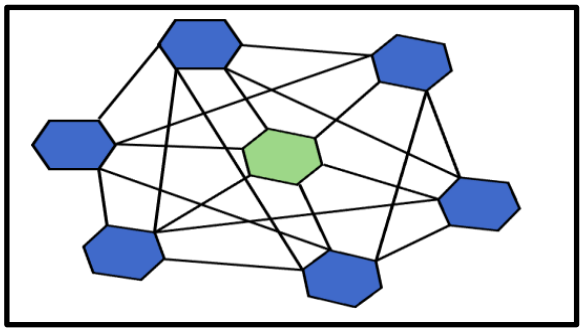
"Tipos de formación en redes"



"Red en Cadena"



"Red en Estrella"



"Red Multicanal"

Nota: las imágenes señalan los diferentes tipos de organizaciones en red, establecidos por el autor del texto. (2019, p. 71).

Con respecto a las imágenes anteriores, las redes en cadena son altamente jerarquizadas y tienen un mando centralizado, lo que se traduce en un funcionamiento controlado de manera descendente, tanto en la toma de decisiones, planificación y ejecución de las operaciones. Por otro lado, las redes en estrella son compartimentadas y podrían llegar a constituir una célula dentro de una mayor. Finalmente, las redes multicanal satisfacen enfáticamente el modelo de descentralización en su más pura concepción, ya que los organismos y miembros no tienen que recurrir a una jerarquía, ya que tienen sus misiones

claras, saben lo que tienen que hacer y tienen un conocimiento pleno de lo que pretende el nivel superior.

Reforzando lo antes descrito, Sullivan y Bauer (2008), aluden a que las guerras del siglo XXI, estarían representadas por organizaciones que metafóricamente funcionarían a base de una especie de enjambres que operarían en redes, oponiéndose a entidades altamente jerárquicas como los ejércitos. Ejemplo de aquello, serían organizaciones como los carteles colombianos y mexicanos, la guerrilla argelina, Cashmera o Chechena y entidades terroristas como Al-Qaeda, entre otros, los cuales se caracterizan por ser actores no estatales y transnacionales, funcionando en términos básicos y simples de la misma manera.

Entonces y como una contramedida a lo expuesto, es que bajo la perspectiva del concepto IPO, se sostuvo el hecho de implementar organizaciones de inteligencia en redes, las cuales tuvieran la capacidad de apoyar a organizaciones superiores y jerarquizadas en el nivel operacional, contribuyendo de dos maneras a estos cometidos: “Apoyar a la recopilación, análisis y difusión de información e inteligencia y también acelerando este proceso para que el sistema de red pueda aumentar el ritmo en el ciclo de decisiones” (Begert y Lindsay, 2002, p. 136). En relación con este tema, el ciclo al cual se hace referencia estaba basado sobre las teorías de Boyd[8], el cual enfatiza en que la interacción de los ciclos OODA, siempre son constantes y complejos, ya que la interacción continua de oponentes es un duelo constante de observación, orientación, decisión y actuación. En consecuencia, IPO también se divisaba como una actividad constante, que se asemejaba al ciclo antes señalado.

Asimismo, y haciendo referencia a lo manifestado en algunos pasajes previos de este trabajo, se pronunció sobre algunos organismos pioneros en la adopción de estas nuevas

[8] Cuando el autor hace referencia al “Ciclo de Decisiones” se refiere al modelo concebido, estudiado y desarrollado por el Coronel de la Fuerza Aérea de Estados Unidos, John Boyd, el cual se representa a través del ciclo (OODA) Observar, Orientar, Decidir y Actuar, en donde describe la interacción de estas actividades en un ciclo continuo y al enfrentarse estos ciclos en entidades opuestas, como resultado se presenta una victoria o una derrota, por lo tanto el que desarrolla un ciclo más rápido tiene más posibilidades de triunfar.

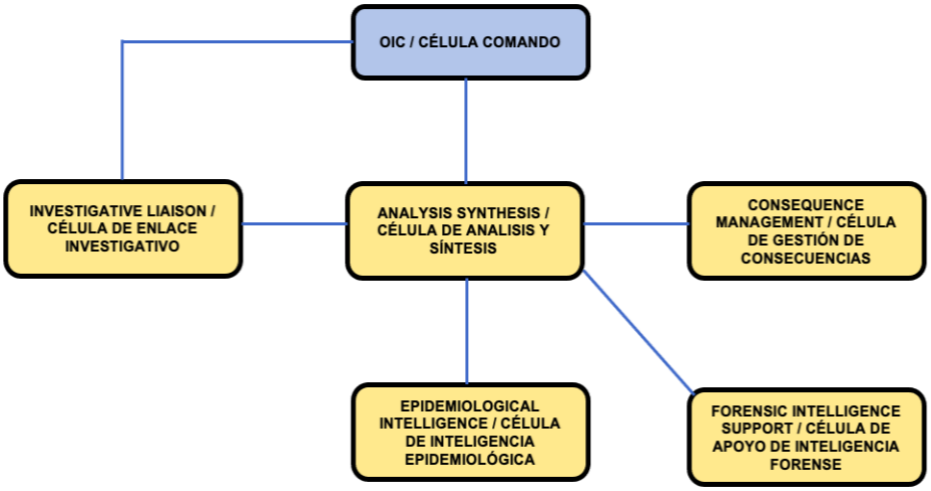
filosofías y métodos ligados a la inteligencia. De esta manera, había surgido cinco años antes de los atentados del 11S, The Ángeles Terrorism Early Warning Group (TEW) o Grupo de Alerta Temprana contra el Terrorismo de Los Ángeles, teniendo la particularidad que contaba con una vasta experiencia en asuntos ligados a la seguridad e invitaban a participar a la comunidad internacional militar, policial, analistas de inteligencia, personas ligadas al mundo empresarial y médico, entre otras muchas disciplinas que estuvieran interesados en trabajar para detener al terrorismo. Como se expresa en el texto Terrorism Early Warning, “este grupo ecléctico formó un grupo cerebro, una especie de “Wikipedia” de lucha contra el terrorismo” (Sullivan y Bauer, 2008, p. 23).

Comenzaron, por lo tanto, materializando acciones centradas en la creación de nuevos puestos de desempeño y de procesos de obtención de información de respuestas ante ciertos objetivos y sucesos, generando carpetas de blancos y análisis e informes de posibles amenazas basados en los estudios realizados.

Si analizamos lo anterior, fácilmente podríamos asemejar y vincular estas acciones, con tareas y procesos que se encuentran plenamente vigentes y que derivan de nuestra doctrina, como es el caso del IPB, JIPOE, Proceso de Adquisición de Objetivos (PAO) y el Proceso de Targeting Conjunto, en donde analistas realizan tareas de inteligencia de blancos y preparan informes y archivos con el propósito de contar con la suficiente información para la toma de decisiones en contribución a las futuras operaciones. De esta manera y con el propósito de poder materializar lo anterior, el TEW vio la obligación de organizarse en seis células como se indica en la siguiente imagen:

Imagen 5

"Organización de empleo del TEW"



Nota: la imagen señala la organización de las células establecidas por el TEW para desarrollar sus tareas de inteligencia. (2008, p. 29).

Tabla 3

"Obligaciones de Células del TEW"

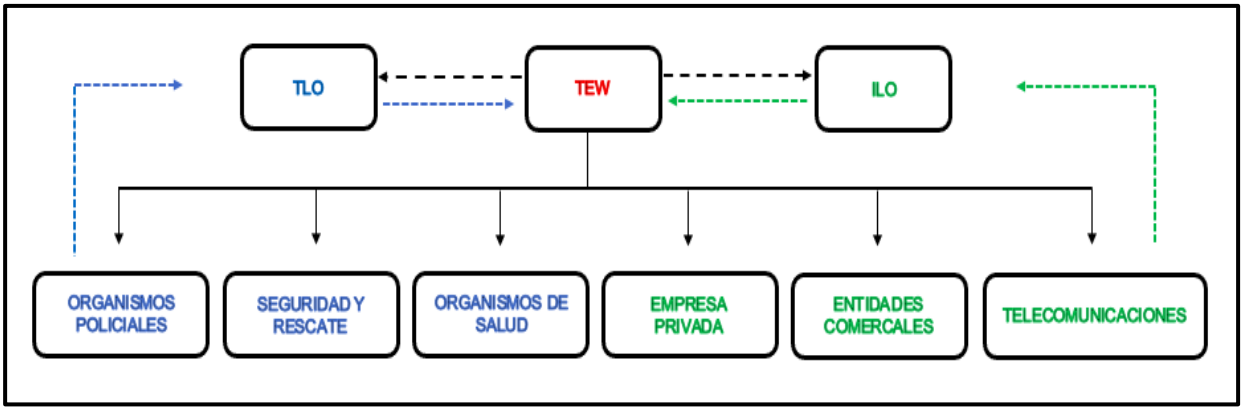
ORGANIZACIÓN	OBLIGACIONES
• ***Célula Comando***	Proporcionaba dirección, estableciendo requisitos de inteligencia y era responsable de interactuar con las autoridades del incidente ocurrido.
• ***Célula Análisis y Síntesis***	Coordinaba las actividades de evaluación y desarrollaba planes de recopilación, tareas de solicitud de información, desarrollo de resultados de análisis en productos de inteligencia.
• ***Célula de Gestión de Consecuencias***	Evaluaba aspectos legales, médicos y de otros organismos de alerta y rescate.
• ***Célula de Enlace Investigativo***	Coordinaba asuntos de inteligencia con entidades de investigación criminal y la comunidad tradicional en asuntos atingentes.
• ***Célula de Inteligencia Epidemiológica***	Responsable del análisis y evaluación de enfermedades, focos de infección e investigación de una enfermedad determinada.
• ***Célula de Apoyo de Inteligencia Forense***	Apoyaba el proceso de fusión en su ámbito, por medio de reconocimientos, uso de sensores y detectores, herramientas geoespaciales y medios cibernéticos.

Nota: la tabla contiene las principales tareas específicas realizadas por las diferentes células constitutivas del TEW. (2008, p. 29).

Con respecto a lo anterior, el TEW desarrolló una red local y pública de Oficiales de Enlace contra el terrorismo (TLO) por medio de organizaciones policiales, de seguridad y rescate, como es el caso de compañías de bomberos, redes de salud, y otras entidades en las distintas áreas de operaciones. En otro sentido, se establecieron también en el sector privado los Oficiales de Enlace de Infraestructura (ILO), quienes eran los encargados de proporcionar información entre los miembros del TEW y las entidades civiles, culturales y de infraestructura crítica en un área determinada. De esta forma, tanto los TLO como los ILO, contribuirían a proporcionar ciertas capacidades de detección para el TEW, y simultáneamente, serían los mismos usuarios de los productos desarrollados por este estamento. Este proceso se pude ejemplificar conforme a la siguiente imagen:

Imagen 6

"Organización y enlace del TEW, con organismos públicos y privados"



Nota: la imagen señala la relación de transferencia de información entre los integrantes del TEW con organismos civiles y privados. (2008, p.29), Elaboración propia.

3.3.4 IPO como herramienta de preparación de inteligencia

Como se ha mencionado con antelación, IPO fue generado como un concepto y filosofía que tenía como propósito reforzar ciertas deficiencias que se evidenciaron de la doctrina IPB vigente de la década de los noventa en Estados Unidos,[9] la cual fue definida como eminentemente convencional. Por lo tanto, si analizamos lo anterior, IPO se constituyó a

[9] Se refiere específicamente al Manual de Preparación de Inteligencia del Campo de Batalla (IPB), publicado en julio de 1996. FM 34-130.

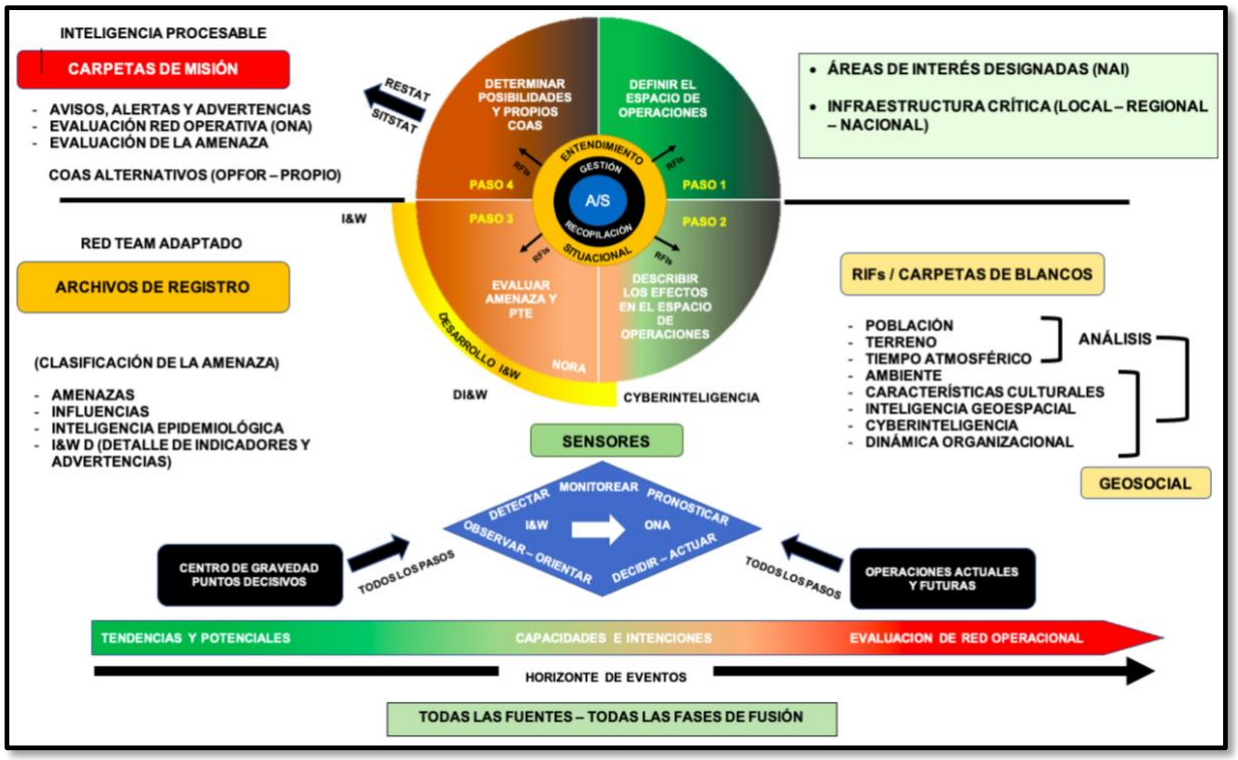
base del modelo de inteligencia desarrollado por el TEW y una adaptación más dinámica del IPB, el cual fue orientado en un plano eminentemente urbano. Lo anterior, complementado con herramientas geoespaciales y geosociales para proporcionar un contexto que contribuyera a anticipar y comprender un conjunto de amenazas no convencionales y de naturaleza irregular.

A su vez, el centro o núcleo de este proceso se amparó en la realización de actividades de análisis y síntesis, el cual se alimentaba por medio de un proceso iterativo de solicitudes o requerimientos de información, proporcionando antecedentes en todos los pasos, los cuales a base de su descomposición en partes constituyentes, permitía el posterior procesamiento e identificación de vínculos con elementos afines, y de esta manera generar las condiciones para sintetizar los resultados del análisis y obtener la inteligencia procesable que se requería.

Como resultado, esta herramienta se desarrolló a base de cuatro etapas secuenciales y dinámicas, las que al estudiarlas, se asemejan indiscutiblemente a las mismas etapas de las metodologías IPB y JIPOE que se encuentran plasmadas en nuestra doctrina vigente. De lo anterior, se presenta a continuación un esquema gráfico que permite entender en una forma más sistemática las etapas, actividades y elementos que sustentan las actividades analíticas de este proceso, siendo complementado con una breve descripción de sus etapas y elementos constitutivos.

Imagen 7

"Esquema general de la estructura del Proceso IPO"



Nota: imagen que representa el esquema genérico del proceso IPO con sus pasos constituyentes, elementos que interactúan con el proceso y productos de cada etapa. (Sullivan & Bauer, 2008)

Paso Nº1 "Definir el Espacio de Operaciones"

En esta etapa, se definía el espacio donde podrían ocurrir acciones de una potencial amenaza en un entorno urbano, a través del estudio y análisis de una serie factores, los que quedan plasmados con mayor detalle en el Anexo Nº2 y 3 de este trabajo. Por lo tanto, se buscaba identificar zonas importantes dentro de un área determinada, obteniendo información sobre la ubicación, dimensiones, infraestructura, importancia táctica, operativa y estratégica, así como las características y distribución de la población existente en ella.

Por otra parte, también se consideraban factores como la economía, la política, la cultura y las tendencias sociales, ya que condicionaban la vida en un área en particular. En consecuencia, en esta etapa, se realizaban evaluaciones desde una perspectiva sistémica local para comprender las relaciones, vínculos y dependencias de los factores en este espacio de operaciones. Además, los análisis estaban enfocados en identificar los diferentes componentes asociados principalmente a la infraestructura crítica (IC) de una localidad y a los lugares de alta significancia, los cuales iluminaban las tareas de recopilación de información y se constituían como el resultado principal del análisis y conclusiones de este paso.

Paso Nº2 "Describir los efectos en el Espacio de Operaciones"

Teniendo como producto la orientación general y la identificación de posibles NAI, representados como nodos de un sistema de IC, se procedía a evaluar una amplia gama de factores que podrían influir en ellos. Se realizaba en consecuencia, un estudio sobre elementos y actividades que podrían repercutir positiva o negativamente en las zonas o posibles lugares de riesgo, estudiando el comportamiento de los sistemas identificados, factores ambientales ligados a la meteorología que los condicionaran, y en definitiva, identificando y estableciendo posibles sistemas de objetivos, los cuales serían los componentes fundamentales de la IC evaluada, permitiendo establecer una lista o inventario de objetivos que servirían para los posteriores análisis del proceso.

Además, y conforme a patrones identificados previamente, se evaluaban las actividades propias y características de ciertas zonas específicas, como es el caso de eventos de reuniones masivas, fechas significativas, concentración de recursos vitales, lugares con significancia simbólica, entre otros, los que contribuían a determinar posibles objetivos adicionales, los que según su grado de importancia, y derivados de los HVT identificados en el proceso, se podían catalogar como HPT.

En consecuencia, el resultado de lo antes realizado, contribuía a definir la naturaleza e identificación de objetivos potenciales en el área de operaciones. En tal sentido, esta

metodología aludía sobre la evaluación del impacto que tenían ciertos factores ambientales, como el estudio del terreno, el tiempo atmosférico y los aspectos geosociales (características demográficas y culturales), complementado con medios tecnológicos asociados a GEOINT y CYBERINT, detallados en el Anexo Nº2 y 4, siendo fundamentales para comprender el entorno y evaluar los impactos en un área específica.

Paso Nº3 "Evaluación de la Amenaza y PTE"

Este tercer paso y como lo indica el Anexo Nº2 y 5, involucraba los estudios relacionados principalmente al adversario o PTE, en donde los analistas de inteligencia debían en primer lugar, identificar individuos, grupos u organizaciones dentro del área de operaciones, quienes por sus características particulares, podrían llegar a constituirse como posibles amenazas. Por esta razón, es que se debía evaluar las relaciones y vínculos entre estos actores y entidades asociadas al crimen y terrorismo. Dado lo anterior, se buscaba responder las preguntas orientadas a ¿Quiénes son las personas involucradas?, ¿Cuáles son las afiliaciones?, ¿Cuáles son las creencias?, entre otras preguntas atingentes. Por lo tanto, se debía evaluar las densidades de población detectadas en estas organizaciones, sus variaciones, movimientos, como asimismo, sus actividades locales, identificando métodos, objetivos, financiamiento, lugares de empleo e interés, lo que proporcionaba una visión importante de la capacidad de accionar del enemigo.

Por consiguiente, las actividades en esta etapa y como lo indica el esquema del proceso IPO, eran apoyadas por un programa activo de identificación o transacciones de "I&W" (indicadores y advertencias), el cual según Sullivan y Bauer (2008), correspondían a una metodología para establecer indicadores y advertencias en la anticipación de amenazas terroristas, basado en la identificación de actividades, tendencias o patrones que indiquen una amenaza específica, es decir, proporcionando alertas previamente planificadas.

Finamente, el análisis de la amenaza en esta etapa por medio del estudio de los factores ORBAT, serían fundamentales para evaluar los fines, modos y medios del adversario, con

el afán de poder comprender y determinar la posibilidad de este tipos de amenazas, las cuales según esta naturaleza, empleaban distintas técnicas en su empleo, como es el caso de armas químicas, biológicas, radiológicas, nucleares, WDM y otras de alta letalidad.

Paso Nº4 "Determinar Posibilidades e insumos para el Desarrollo de COAs"

Conforme a Anexo Nº2 y 6, esta última etapa del proceso, radicaba en la capacidad de determinar las posibilidades del adversario, por medio de la evaluación de las capacidades y opciones dentro de los lugares o áreas conocidas como "Escenarios de Alto Impacto" (HIT), lo que sumado a la inteligencia disponible, permitían establecer la hipótesis del COA más probable y del más peligroso.

No obstante, este proceso se veía inmerso e influenciado por otros factores y elementos como lo indica la imagen 9, los cuales interactuaban permanentemente en las diferentes etapas. De esta manera, las actividades terroristas se desarrollaban con el tiempo, lo que se podía expresar de forma lineal en un horizonte de eventos o también de manera no lineal. De lo anterior, y conforme lo señala la imagen 10, "Ciclo de Análisis de Transacciones", correspondía a un enfoque analítico complementario elaborado específicamente para acciones en un entorno no lineal, cuya finalidad tenía la de discernir sobre la actividad terrorista dentro de un conjunto de datos e información dinámica y confusa, propia de la gran incertidumbre que envuelve este ambiente no convencional. Así, este ciclo surgió para enseñar a los analistas, sobre cómo interpretar las actividades para evaluar las pistas y otros indicativos, mientras desarrollaban planes de obtención de información iterativos en la identificación de patrones sobre posibles cadenas de acciones terroristas.

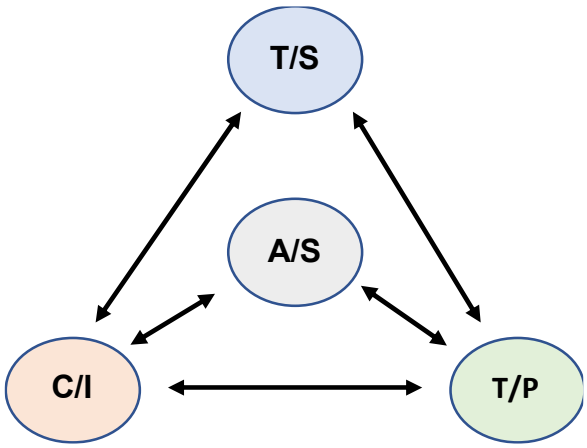
Por lo tanto, este ciclo de transacciones servía como un generador de patrones centrado en actividades de análisis y síntesis (A/S) de información, siendo el núcleo de la fase de 'Orientación' del Ciclo de Decisión del Coronel Boyd o ciclo OODA (Observar-Orientar-Decidir-Actuar). Del mismo modo, el proceso de análisis/síntesis impulsaba los cuatro

pasos de IPO, mediante la emisión de solicitudes o requerimientos de información (RFI), según lo requerían las circunstancias. En efecto, los analistas podían observar actividades realizadas por una variedad de actores que podían constituirse como indicadores o precursores de actividades terroristas o delictivas, pudiendo ser representadas de muchas maneras, como es el caso de, evidencias relacionadas con el financiamiento, adquisición de material, municiones o capacidades, reclutamiento de personas, realización de reconocimientos, ensayos de una misión o la realización de un ataque.

En síntesis y según esta metodología, la acción de identificar estos patrones o actividades previas permitían a los especialistas catalogar estos eventos como firmas, los que cooperaban en la identificación de actos terroristas o criminales. A su vez, estas transacciones y firmas (T/S), podían observarse y combinarse con patrones de actividad, pudiendo ser expresadas como tendencias y potenciales (T/P), las cuales finalmente, podían evaluarse en términos de capacidades e intenciones (C/I) de un actor específico en el proceso analítico. A continuación y en estrecha relación a lo antes señalado, se puede observar la interacción de este ciclo, conforme a la siguiente imagen:

Imagen 8

"Ciclo de Análisis de Transacciones"



Nota: esquema del "Proceso de Análisis de Transacciones" en donde el núcleo corresponde al análisis/síntesis de la información, con los insumos que contribuyen a su desarrollo. (2008, p. 32,58).

3.3.5 Cuadro descriptivo de IPO y su pertinencia en el análisis de amenazas híbridas.

Como una manera de abordar este segmento capitular, se realizó una descripción de algunos factores de este proceso, principalmente a base del paso Nº3 “Evaluación de la Amenaza” y bajo otros antecedentes de los pasos adicionales de esta metodología.

Tabla 4

“Cuadro descriptivo del proceso IPO”

Cuadro descriptivo de Proceso de Inteligencia IPO	
Criterio	**Observaciones**
1. Análisis de la definición del espacio operativo.	• Proceso que busca la definición física del espacio operativo, bajo un entorno de conducción táctica, por medio de la medición de áreas y límites, tanto para el desarrollo de las operaciones, como para las actividades de inteligencia. • Enfocada en determinar las características importantes del entorno. • Procura buscar vacíos de inteligencia, prioridades y déficits de inteligencia. • Orientación en el análisis de zonas urbanas, identificando lugares, sitios específicos, infraestructura, sectores culturales, centros económicos, sistemas de infraestructura crítica.
2. Factores influyentes en el análisis de los efectos del espacio operativo.	• Principalmente del análisis de factores meteorológicos, terreno y consideraciones civiles • Análisis de factores del terreno orientado a infraestructura crítica y obras de arte. • Análisis de tendencias meteorológicas en función de efectos en las estructuras y la potencialización de estos fenómenos en el efecto de las armas. • Análisis de antecedentes de factores geosociales. • Capacidad de análisis desde una perspectiva sistemática enfocada en el área operativa específica y terrestre.
3. Naturaleza, propósito y metodología del paso Nº3 “Evaluación de la Amenaza”.	• Busca determinar las capacidades, limitaciones y vulnerabilidades de un adversario o amenaza. • Pretende comprender las tácticas, técnicas y procedimientos de empleo de una amenaza irregular y la forma en como ha desarrollado sus operaciones con antelación. • Busca a través del análisis de las fortalezas, capacidades, limitaciones y vulnerabilidades del adversario, identificar Centros de Gravedad y Puntos decisivos. • La herramienta principal de análisis de la amenaza son los factores del ORBAT, generados de las bases de datos existentes. • No apoya actualmente ningún proceso de planificación.

Cuadro descriptivo de Proceso de Inteligencia IPO	
	• Herramienta de carácter táctica que contribuye al nivel operacional. • Énfasis en el análisis de fuerzas en un espacio urbano y eminentemente terrestre. • Análisis principalmente de fuerzas irregulares (terrorismo, crimen y delincuencia). • Para su desarrollo, se integra con otros organismos tanto civiles, como militares.
4. Factores del ORBAT	• Emplea las siguientes variables del ORBAT: – Composición. – Fuerza. – Dispositivo – Tácticas, técnicas y procedimientos de empleo. – Entrenamiento. – Logística – Eficiencia de combate. – Características especiales o datos misceláneos. • Considera adicionalmente la variable cultura y variables sociales en su lista de variables de análisis de los factores ORBAT • Enfoca explícitamente el análisis de estas variables a una amenaza irregular, estudiando los siguientes tópicos: – Organización de unidades, grupos religiosos, étnicos y delictuales. – Efectivos, armas y equipamiento ofensivo y no convencional, como armas CBRNE, cuadros o células políticas, apoyo popular de simpatizantes y de sostenimiento, traslado u ocultación de información. – Situación de empleo, movimientos o ubicaciones recientes, actuales o futuras de la amenaza. – Consideraciones políticas, militares, sicológicas y económicas del área operativa. – Formaciones individuales y organizacionales del adversario. – Análisis vertical y horizontal del sostenimiento de organizaciones. – Condicionamiento de la motivación, adhesión popular, aspectos sentimentales, intimidación y cambios en el poder político. – Vínculos de las personalidades claves y sus grupos y asociaciones. – Cultura de organizaciones criminales y terroristas abordando, ideologías, usos, costumbres, patrones de pensamiento, problemas culturales, actitudes militares y de ley y justicia, entre otros.
5. Productos de inteligencia entregados al final del paso.	• Proporciona modelos de amenazas conforme a la base de datos existente e identifica el CoG y PDs con respecto a ellas. • Centra sus actividades en entregar los siguientes productos: – Lista de amenazas. – Elementos de potenciales amenazas. – Modelos de amenazas a través de la evaluación de los fines, modos y medios de una amenaza irregular (terrorismo, delincuencia). – Indicadores y advertencias. – Relaciones de las amenazas y los objetivos establecidos como IC, eventos y

Cuadro descriptivo de Proceso de Inteligencia IPO	
	lugares. – Escenarios de amenazas de Alto Impacto o HIT.
6. Enfoque en análisis relacionado con amenazas no convencionales.	• Herramienta generada para analizar amenazas irregulares. • No entregan de manera profunda una metodología acerca de la elaboración de plantillas doctrinales, sólo las menciona. • Expresa la importancia acerca del estudio sociocultural a través del análisis global de los siguientes factores: – Estructura social: razas y grupos étnicos, redes e instituciones. – Cultura: identidad, creencias, valores, actitudes y percepciones, sistemas de creencias, formas culturales, lenguaje, rituales, símbolos, ceremonias, mitos y narrativas. – Poder y autoridad: fuerza coercitiva, capital social, poder económico, autoridad. – Intereses: seguridad física, servicios esenciales, economía y participación política. – Infraestructura. • Factores ORBAT relacionados a amenazas no convencionales. • Carente de información acerca operaciones en diferentes dominios.

Nota: el presente cuadro describe los principales factores analíticos de IPO en relación al paso Nº3 “Evaluación de la Amenaza” y otras adicionales de los pasos Nº1 y 2 de esta metodología.

No obstante, del presente cuadro descriptivo se infieren y establecen las siguientes fortalezas y debilidades factibles de ser relacionadas con el análisis de amenazas híbridas definidas en el capítulo anterior.

Tabla 5

“Fortalezas y debilidades del proceso IPO en el contexto del análisis de una amenaza híbrida”

Cualidades equivalentes de amenaza híbrida	Fortalezas	Debilidades
1. *Posibilidad de participación de actores estatales y no estatales.*	• Capacidad de realizar un análisis sistémico.	**-.-**
2. *Empleo de diferentes modalidades de guerra a través de capacidades convencionales, tácticas y*	• Herramientas de análisis atingente y específica para el análisis de tácticas, técnicas	• Carencia de recursos analíticos para evaluar amenazas y operaciones

	formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica, unificada y sincronizada.	irregulares asociadas a terrorismo, delincuencia y crimen organizado.	convencionales de fuerzas regulares.
3.	*Empleo del espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación.*	**-.-**	• Enfoque predominantemente del entorno físico.
4.	*Intensa participación de la población civil ya sea en apoyo o como objetivo en el conflicto.*	• Fundamentación para el análisis de factores sociales en el espacio operativo.	**-.-**
5.	*Empleo de armamento de alta tecnología y bajo una perspectiva estratégica.*	• Énfasis en sistemas de armas y en el análisis de sus efectos.	**-.-**
6.	*Empleo en terrenos altamente complejos.*	• Enfocada en el análisis de operaciones en terrenos urbanos y altamente complejos.	**-.-**
7.	*Existencia de campañas multidimensionales*	**-.-**	• Falta de recursos para el análisis de operaciones en diferentes dimensiones, enfocándose solo al dominio terrestre.

Nota: se describen las fortalezas y debilidades del proceso IPO, tomando como referencia el concepto de amenaza hibrida definida en el capítulo anterior.

No obstante, como una manera de contribuir en la calidad y objetividad de los resultados orientados al grado de pertinencia de este proceso, y a reforzar el análisis de fortalezas y debilidades establecidas, durante la investigación se realizaron encuestas a oficiales especialistas en inteligencia que se desempeñan actualmente como comandantes de Agrupaciones de Inteligencia, asesores de inteligencia en UACs y profesores que se desempeñaron impartiendo clases de la doctrina de procesos de inteligencia en la institución, con la finalidad de reforzar la determinación del análisis y conclusiones. De esta manera, y conforme a Anexo Nº7 y 8, se realizaron las siguientes preguntas a los encuestados:

1) *¿Tiene usted algún conocimiento del concepto y metodología de preparación de inteligencia "Intelligence Preparations for Operations" (IPO) utilizado en EEUU en la primera década de los años dos mil?.*

2) *¿Considera que una herramienta no vigente como IPO, podría contribuir a completar ciertos vacíos analíticos, debido a su especificidad en el análisis de amenazas ligadas a la criminalidad, terrorismo y crimen organizado?*

Con respecto a lo anterior, casi la totalidad de encuestados desconoció este proceso. Sin embargo, en la introducción de la encuesta enviada, se plasmaron algunas de las características principales de este proceso, con el propósito que se interiorizaran sobre esta metodología, y ante eso, algunos manifestaron que nuestros procesos actualmente entregan estos factores de análisis por lo que no sería necesario su complementación y otros expresaron que podría contribuir rescatando principalmente sus recursos sobre el análisis de amenazas irregulares.

Finalmente, como resultado del desarrollo de las tareas señaladas en la metodología capitular, podemos establecer las siguientes conclusiones:

Revisión bibliográfica y relación del Proceso IPO con el contexto de amenazas híbridas.

Se pudo identificar que el proceso IPO no aborda explícitamente el concepto de amenaza híbrida, sin embargo, en el ámbito de amenazas no convencionales, presenta herramientas sólidas y específicas para la evaluación de amenazas irregulares, orientadas a adversarios que realizan actos terroristas, delictuales y ligados al crimen organizado.

Definición y explicación del Proceso IPO.

Con respecto a este punto, IPO se caracteriza por ser un proceso de inteligencia obsoleto y desactualizado, que surgió como respuesta a las limitaciones de la doctrina de IPB en Estados Unidos de los años 90, la cual fue categorizada como eminentemente convencional. En efecto, IPO se construyó como un proceso basado en análisis y síntesis, a través de solicitudes iterativas de información, estructurado en cuatro pasos similares al IPB y JIPOE que conocemos actualmente en nuestra doctrina institucional y conjunta, con el objetivo de analizar y contrarrestar amenazas irregulares ligadas al terrorismo y delincuencia con un énfasis especial en terrenos urbanos.

En relación a lo anterior, fue una herramienta de carácter policial y criminal, basado en el concepto de defensa activa, centrada en materializar una secuencia de acciones orientadas a la evaluación, análisis, previsión y toma de decisiones para enfrentar estas amenazas, sostenida a base de la colaboración de diversos organismos multidisciplinarios con conocimiento sobre asuntos de seguridad y defensa.

Pertinencia en el análisis de amenazas híbridas.

Finalmente, IPO proporciona herramientas que son atingentes al análisis de una amenaza híbrida, en lo que respecta principalmente a amenazas irregulares, análisis de terrenos complejos como son los urbanos, análisis de los efectos del entorno en los sistemas de armas, importancias y énfasis en el trabajo integrado y multidisciplinario de organismos ligados a la seguridad y defensa, e importancia en la evaluación de factores sociales y culturales en un entorno operativo y bajo un análisis sistémico. Sin embargo, se constituye como un proceso de inteligencia de nivel táctico, orientado en definir un entorno operativo eminentemente urbano, bajo un análisis especialmente físico y para una amenaza irregular, careciendo de importantes recursos analíticos orientados principalmente a la comprensión de operaciones en los diversos dominios, al análisis de amenazas y operaciones convencionales y a la condicionante privación de factores y variables de información y fundamentos en la evaluación del espacio virtual o ciberespacio.

3.4 Síntesis del capítulo.

El propósito de este capítulo, fue dar respuesta a la pregunta Nº2 *¿En qué consiste el Proceso IPO y cuál es su pertinencia en el análisis de amenazas híbridas?.* En tal sentido, el tema clave analizado fueron aquellos relacionados con el concepto y proceso de inteligencia IPO, los cuales dieron forma y sustento a los respectivos análisis y conclusiones sobre su indagación. Para este cometido, la metodología se sustentó principalmente en la técnica de análisis documental, basada en artículos y textos relacionados con este proceso, básicamente de los primeros años de la década del dos mil, ya que no existieron evidencias actualizadas, experiencias y resultados sobre su empleo. Lo anterior, debido a su

obsolescencia y casi total desconocimiento en nuestro ámbito nacional y también de la escaza bibliografía encontrada extrainstitucionalmente. Es pertinente mencionar, que se desarrollaron dos ejercicios bajo el amparo de esta metodología, siendo estos la *"Operación Talavera"* del 2004, frente a un simulacro de un contraataque radiológico y la *"Operación Quimera"* del 2005, frente al análisis de un escenario contrabiológico, de los cuales no se pudo acceder a su información y experiencias.

Respecto a los hallazgos obtenidos, en primer lugar, se buscó identificar y señalar sobre que abordaba este proceso específicamente sobre el análisis de amenazas híbridas, entregando como resultado, la desconexión explícita con este concepto, ya que IPO fue creado para el análisis de amenazas irregulares conforme a su contexto temporal. Seguidamente, se definió y describió este proceso, el cual permitió obtener información objetiva acerca de su origen, fundamentos, objetivos y metodología de empleo como proceso de inteligencia, indicando sus particularidades. Posteriormente, se realizó un cuadro descriptivo de los factores de análisis de este proceso, principalmente a base del paso Nº3 "Evaluación de la Amenaza", y también de otros criterios de análisis de sus pasos adicionales, con el propósito de determinar la naturaleza de sus recursos analíticos, fortalezas, debilidades y su posible pertinencia en el análisis de esta tipología de amenazas.

Esta acción, fue contrastada con la opinión de algunos oficiales especialistas en inteligencia que actualmente se desempeñan como asesores en UACs, comandantes de AGRINT y oficiales que impartieron la doctrina de IPB y JIPOE en la Escuela de Inteligencia. Lo anterior, con el propósito de robustecer y darle un sentido objetivo al establecimiento de las conclusiones acerca del conocimiento de este proceso y del grado de su posible pertinencia.

Finalmente, con la totalidad de las tareas realizadas durante el presente capítulo, el cual buscó describir en qué consiste el Proceso de Preparación de inteligencia IPO, y cuál es su posible pertinencia en el análisis de amenazas híbridas, se pudo concluir que los resultados del capítulo hacen posible afirmar, que es un proceso desconocido, obsoleto, orientado al nivel físico y táctico. Sin embargo, proporciona algunos recursos y variables atingentes para

el análisis de amenazas irregulares, propios de un ambiente híbrido actual, concluyendo con lo anterior a darle respuesta a la pregunta específica de la investigación y a darle cumplimento al objetivo planteado para este capítulo.

CAPÍTULO IV

IPB Y JIPOE Y SU PERTINENCIA DE SER EMPLEADOS EN EL ANÁLISIS DE AMENAZAS HÍBRIDAS.

4.1 Metodología del capítulo.

El presente capítulo, buscó responder la pregunta específica Nº3 *¿Cuáles son las diferencias analíticas de los procesos IPB y JIPOE, en el contexto de amenazas híbridas?* y con ello dar cumplimiento al objetivo específico Nº3. Para lo anterior, la metodología capitular se ajustará básicamente a un trabajo comparativo del tipo descriptivo, desarrollando para el presente capítulo dos segmentos en particular.

En tal sentido, el primero de ellos, se basará en identificar si es que estos procesos de inteligencia indican o mencionan explícitamente la conceptualización de este tipo de amenazas, ya que es uno de los conceptos claves de esta investigación. Posteriormente, se realizará un análisis comparativo de estos procesos, con el propósito de identificar las semejanzas y diferencias en sus recursos analíticos y vincularlos al análisis de amenazas de naturaleza híbrida.

4.2 Revisión de fundamentos y su relación con el contexto híbrido.

Es pertinente empezar señalando, que en los procesos de preparación de inteligencia existentes en nuestra reglamentación, los principales insumos disponibles para analizar una amenaza, se encuentran plasmados en el paso Nº3 “Evaluación de la Amenaza”, sin perjuicio que existen otros recursos valiosos que complementan y concurren en beneficio de estas evaluaciones. Entonces, ahondado en nuestra reglamentación institucional y conjunta, será innegable dudar que los procesos IPB y JIPOE, entregan elementos y variables sustanciales para poder evaluar a un adversario desde una perspectiva convencional. Sin embargo, la pregunta que debemos hacernos es, ¿mencionan o abarcan fundamentos específicos acerca de lo híbrido?.

En respuesta a lo anterior, nuestro texto institucional RDI – 20005 IPB, “Proceso de Integración del Campo de Batalla”, no nombra y considera explícitamente información acerca de esta tipología de amenazas, identificando preliminarmente, una ausencia de factores o variables analíticas específicas. No obstante, hace referencia de una manera somera a amenazas irregulares o asimétricas. Además, sostiene que para evaluarlas, “será necesario la utilización de herramientas de análisis diferentes a las que se presentan en este reglamento” (2015, p.35). Complementando lo anterior, este reglamento se basa en la doctrina norteamericana de inteligencia. Sin embargo y como hace mención Carter (2016), IPB es deficiente en el desentierro de una naturaleza desconocida y de carácter inestable del conflicto, porque se presume que hay un enemigo/amenaza en un sentido convencional. Por lo tanto, es concebible que en un ambiente operacional complejo, no haya un enemigo, sólo condiciones o sistemas que requieren ajuste para resolver un problema y lograr una misión. De lo anterior, indica que una reestructuración de esta metodología a un diseño sistémico, centrado en múltiples actores que interactúan en un ambiente complejo, serviría mejor a los comandantes en la identificación de las causas de los problemas y no sólo en los síntomas.

Por otra parte, JIPOE aborda este concepto solamente como referencia para introducir los contenidos sobre las operaciones de estabilidad y de guerra irregular, las que son abordadas en el Capítulo III “Consideraciones Especiales” del respectivo texto. De esta forma, nos adentra en el concepto de terrorismo e insurgencia, aunque desde una postura general.

4.3 Análisis comparativo de procesos de preparación de inteligencia empleadas en apoyo a nuestros procesos de planificación de operaciones.

Como una manera de abordar este punto, se plasmaron los antecedentes identificados del estudio de las diferentes metodologías, según la formulación de algunos criterios de comparación que permitieron identificar las semejanzas y diferencias acerca de la naturaleza y recursos existentes de cada proceso. Lo anterior, tomando como referencia y adaptando la herramienta “Esquema de comparación”, la cual se encuentra en (CEEAG,

2017, p. 93). Además, para llevar a cabo este ejercicio, la comparación se enmarcó principalmente en el paso Nº3 “Evaluación de la Amenaza”, y bajo algunos otros antecedentes de los pasos adicionales, ya que, como se señaló, se constituye como la etapa destinada a estudiar y evaluar una amenaza y en donde existe el mayor porcentaje de variables analíticas destinadas para ello.

Tabla 6

“Cuadro comparativo de los procesos IPB y JIPOE”

Cuadro comparativo de procesos de inteligencia (IPB y JIPOE)	
Criterio de comparación	**Observaciones**
1. Análisis de la definición del campo de batalla y ambiente operacional.	**Semejanzas:** • Ambos procesos buscan la definición física del espacio de operaciones por medio de la medición de áreas y límites tanto para el desarrollo de las operaciones como para la inteligencia. • Determinación de características importantes del entorno. • Búsqueda de vacíos de inteligencia, prioridades y déficits de inteligencia. **Diferencias:** **IPB** • Análisis de campo de batalla centrado básicamente a un espacio físico y de nivel táctico. **JIPOE** • Análisis del ambiente operacional centrado en áreas físicas y no físicas, buscando determinar áreas y límites de un área operacional conjunta.
2. Factores influyentes en el análisis de los efectos en el campo de batalla y ambiente operacional.	**Semejanzas:** • Análisis de factores meteorológicos, terreno y consideraciones civiles **Diferencias:** **IPB** • Análisis de campo de batalla, bajo la orientación de los factores METTTC. • Análisis de los factores militares del terreno (TOCOD). • Análisis de consideraciones civiles por medio de factores ASCOPE. **JIPOE** • Análisis del ambiente operacional desde una perspectiva geográfica (física y no física) • Análisis de un entorno multidominio, terrestre, marítimo, aéreo, espacial y ciberespacio. • Antecedentes del ambiente desde una perspectiva de la información y cognitiva.

Cuadro comparativo de procesos de inteligencia (IPB y JIPOE)	
	• Análisis de ambiente operacional desde una perspectiva sistémica por medio de las variables (PEMSII).
3. Naturaleza, propósito y metodología del paso Nº3 "Evaluación de la Amenaza".	**Semejanzas:** • Ambas metodologías buscan determinar las capacidades, limitaciones y vulnerabilidades de un adversario o amenaza. • Tienen la particularidad que no solamente pueden ser empleadas por organizaciones militares, sino a todas aquellas que deban tomar una decisión, ya sea para contrarrestar a una amenaza como también para planificar. • Buscan comprender las tácticas, técnicas y procedimientos de empleo del adversario y la forma en como han desarrollado sus operaciones con antelación. • Buscan a través del análisis de las fortalezas, capacidades, limitaciones y vulnerabilidades, identificar el Centro de Gravedad del adversario y Puntos decisivos. • La herramienta principal empleada, es el análisis de los factores del ORBAT extraídos de la doctrina y de las bases de datos existentes. • Emplean dentro de su metodología la técnica de elaboración de modelos y plantillas doctrinales de empleo de una amenaza. **Diferencias:** **IPB** • Apoya los procesos PCT y PPM • Herramienta de nivel táctico. • Énfasis para el análisis de fuerzas adversarias en la dimensión terrestre. • Análisis principalmente de fuerzas regulares o convencionales. • Análisis funcional por medio de factores del ORBAT, pudiendo complementarse con factores ASCOPE y otros factores según las circunstancias. • En el análisis de una fuerza regular, análisis por funciones de combate. • En el análisis de una fuerza no convencional, por medio del análisis de bases de datos y patrones de acciones previos. **JIPOE** • Apoya el PPO • Herramienta de nivel operacional, en beneficio de operaciones conjuntas. • Herramienta de análisis para fuerzas que operan en operaciones multidominio (aire, tierra, mar, espacio y ciberespacio). • Analiza los factores del ORBAT, pudiendo complementarse con los factores ASCOPE, PEMSII y otros factores según las circunstancias.
4. Factores del ORBAT	**Semejanzas:** • Ambos procesos, emplean las siguientes variables del ORBAT: – Composición. – Fuerza. – Dispositivo

Cuadro comparativo de procesos de inteligencia (IPB y JIPOE)	
	– Tácticas, técnicas y procedimientos del empleo. – Entrenamiento. – Logística – Eficiencia de combate. – Características especiales o datos misceláneos. • El análisis de estas variables, se asocian principalmente a fuerzas regulares o convencionales en el nivel táctico. **Diferencias:** **JIPOE** • considera adicionalmente la variable cultura en su lista de variables de análisis.
5. Productos de inteligencia entregados al final del paso.	**Semejanzas:** • Elaboración de: – Modelos de amenaza (Plantillas doctrinales de adversario). – Descripciones de la plantilla doctrinal. – Descripción de las TTP de la amenaza. – Elaboración de una lista de HVT y posibles HPT. – Identificación del CoG y PDs. **Diferencias:** **IPB** • Análisis de las capacidades adversarias por medio de las funciones de combate (maniobra, mando y control, apoyo de fuego y técnico, inteligencia, seguridad, apoyo al combate y guerra electrónica). **JIPOE** • Realiza tareas asociadas a establecer el diseño operacional (DO) del adversario.
6. Enfoque de análisis relacionado con amenazas no convencionales.	**Semejanzas:** • Ambos procesos hacen mención acerca de amenazas y operaciones irregulares, aunque con una notoria diferencia en el grado de profundización. • No entregan de manera profunda una metodología de elaboración de plantillas doctrinales para estas amenazas. **Diferencias:** **IPB** • Señala las implicancias e importancia de analizar amenazas de naturaleza asimétricas, irregulares o desconocidas, con énfasis en el empleo de una fuerza en MOOTW. • Para la evaluación de estas amenazas, complementación con herramientas adicionales, en donde los medios de obtención serán vitales para obtener información e integrarla para establecer los patrones y procedimientos de empleo del adversario. **JIPOE** • Única herramienta que hace referencia al concepto de guerra híbrida, no entregando fundamentos específicos para abordarlos. • Establece que para enfrentar enfoques asimétricos, se requerirá de

Cuadro comparativo de procesos de inteligencia (IPB y JIPOE)	
	técnicas y productos que se deberán adaptar al tipo de operaciones conjuntas. • Señala que las técnicas existentes en su manual se pueden aplicar a adversarios de carácter irregular. • Hace mención acerca de operaciones de estabilización e irregular (insurgencia, terrorismo, desinformación, propaganda, crimen organizado) pero con deficiente información. • Enfatiza en la utilización de esta herramienta, no sólo destinado a derrotar a un adversario militar, si no que, en el apoyo a las operaciones que se centren en la población civil. • Señala sobre la importancia del intercambio de información con medios de contrainteligencia en beneficio del análisis de la amenaza. • Expresa sobre la importancia acerca del estudio sociocultural a través del análisis global de los siguientes factores: – Estructura social: razas y grupos étnicos, redes e instituciones. – Cultura: identidad, creencias, valores, actitudes y percepciones, sistemas de creencias, formas culturales, lenguaje, rituales, símbolos, ceremonias, mitos y narrativas. – Poder y autoridad: fuerza coercitiva, capital social, poder económico, autoridad. – Intereses: seguridad física, servicios esenciales, economía y participación política. – Infraestructura. – Mayor intercambio de información y explotación de otras fuentes.

Nota: el presente cuadro comparativo señala las principales semejanzas y diferencias identificadas del análisis de las herramientas de inteligencia IPB y JIPOE en el paso Nº3 “Evaluación de la Amenaza”.

Del mismo modo y al relacionar las características plasmadas en el cuadro comparativo con la definición de amenaza híbrida establecida, se señalan las siguientes fortalezas y debilidades de los factores analíticos con respecto a esta conceptualización.

Tabla 7

"Fortalezas y debilidades identificadas de los procesos IPB y JIPOE relacionadas y pertinentes de ser consideradas para el análisis de amenazas híbridas"

IPB		
Cualidades equivalentes de amenaza híbrida	**Fortalezas**	**Debilidades**
1. *Posibilidad de participación de actores estatales y no estatales.*	• Análisis factores ORBAT y ASCOPE. • Se puede complementar con otros factores de análisis.	-.-
2. *Empleo de diferentes modalidades de guerra a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica, unificada y sincronizada.*	• Entrega fundamentos sólidos para analizar amenazas convencionales. • Señala las implicancias e importancia de analizar amenazas de naturaleza asimétricas, irregulares o desconocidas, con énfasis en el empleo de una fuerza en MOOTW, entregando significativos recursos de análisis para una amenaza no regular como calco de incidentes, matriz radial de análisis de patrones, tabla de relación tiempo evento – tiempo, matriz de asociación, matriz de actividades, diagrama de vínculos, análisis nodal.	• No entrega de manera profunda una metodología acerca de plantillas doctrinales para estas amenazas. • Análisis principalmente de fuerzas regulares o convencionales.
3. *Empleo del espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación.*	-.-	• Deficiencia para analizar amenazas que actúan en el ambiente de la información y ciberespacio.
4. *Intensa participación de la población civil ya sea en apoyo o como objetivo en el conflicto.*	• Análisis de factores ASCOPE.	• Deficiencia con respecto al análisis de aspectos geosociales.
5. *Empleo de armamento de alta tecnología y bajo una perspectiva estratégica.*	• Análisis de factores ORBAT.	-.-
6. *Empleo en terrenos altamente complejos.*	• Énfasis en análisis de terrenos convencionales.	-.-

	• Entrega recursos gráficos para comprensión del campo de batalla y amenaza en zonas urbanas.	
7. *Existencia de campañas multidimensionales*	-.-	• Herramienta de nivel táctico. • Análisis centrado mayoritariamente a un espacio físico y convencional. • Deficiente para analizar operaciones y amenazas multidominios. • Énfasis para el análisis de fuerzas adversarias en la dimensión terrestre.

JIPOE		
Cualidades equivalentes de amenaza híbrida	**Fortalezas**	**Debilidades**
1. *Posibilidad de participación de actores estatales y no estatales.*	• Análisis desde una perspectiva de sistemas para comprender el ambiente operacional y actores presentes en él. • Análisis de factores del ORBAT, pudiendo complementarse con ASCOPE, PEMSII y otros factores según las circunstancias.	• No considera dentro de los factores PEMSII, las variables PT (entorno físico y tiempo).
2. *Empleo de diferentes modalidades de guerra a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica, unificada y sincronizada.*	• Proceso que puede ser aplicado tanto a adversarios de carácter regular como irregular. • Referencia operaciones de estabilización e irregular (insurgencia, terrorismo, desinformación, propaganda, crimen organizado).	• Deficiencia metodología acerca de plantillas doctrinales para estas amenazas. • Deficiencia gráfica de herramientas para analizar áreas específicas y de nivel táctico.
3. *Empleo del espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación.*	• Análisis de un entorno multidominio, terrestre, marítima, aérea, espacial y del ciberespacio.	-.-
4. *Intensa participación de la*	• Enfatiza en el análisis de la	-.-

población civil ya sea en apoyo o como objetivo en el conflicto.	variable cultura. • Herramienta, no sólo destinada para el análisis de un adversario militar, sino que también, a operaciones que se centren en la población civil. • Importancia acerca del estudio sociocultural.	
5. *Empleo de armamento de alta tecnología y bajo una perspectiva estratégica.*	• Análisis mediante los factores ORBAT.	-.-
6. *Empleo en terrenos altamente complejos.*	-.-	• Énfasis en análisis de entornos multidimensionales convencionales. • Carencia de fundamentos para analizar escenarios urbanos y de nivel táctico.
7. *Existencia de campañas multidimensionales*	• Análisis del ambiente operacional desde una perspectiva geográfica (física y cognitiva). • Perspectiva de análisis en el dominio de la información.	-.-

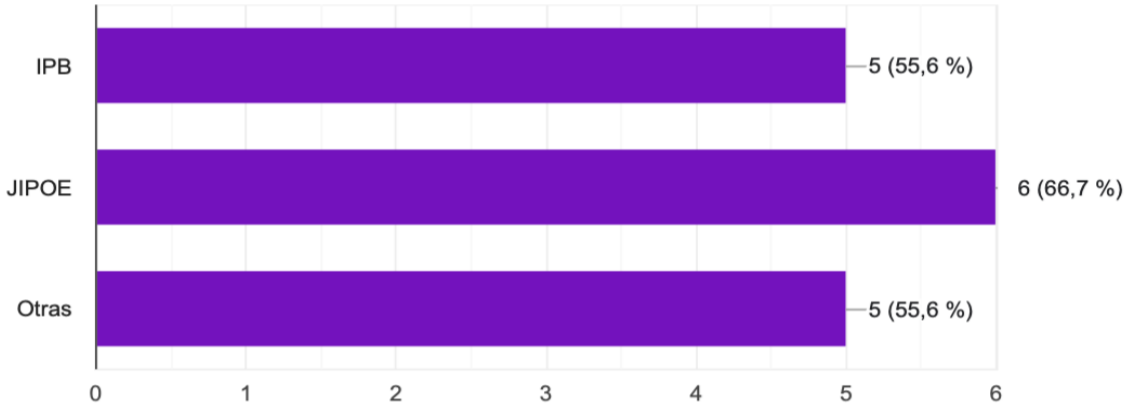
Nota: se describen las fortalezas y debilidades de los procesos IPB y JIPOE, con respecto a su posible pertinencia de ser utilizadas en el análisis de una amenaza hibrida.

Como una manera de brindar un mayor grado de solidez a estos resultados, se presenta una síntesis de las opiniones recopiladas de personal encuestado, quienes se han desempeñado o actualmente se desempeñan en tareas asociadas a preparación de inteligencia en MOOTW y en los últimos EEC, en donde las amenazas identificadas, rápidamente se han asociado en un mayor grado a amenazas no convencionales e híbridas.

1) *¿Durante los EEC o en las tareas operativas propias de la función, cuáles han sido las herramientas de inteligencia que ha utilizado con mayor preponderancia en apoyo a los procesos de planificación? ¿IPB, JIPOE u otras?.*

2) *¿Cuál fue el motivo de esa elección y los recursos fueron eficientes para el análisis del campo de batalla o ambiente operacional y de las amenazas identificadas?*

Con respecto a estas preguntas, los encuestados manifestaron que durante las tareas propias de la función inteligencia que han tenido que desempeñar en operaciones enmarcadas en EEC, han utilizado ambos procesos existentes en nuestra doctrina, lo anterior, directamente condicionado por las circunstancias propias del empleo de las unidades y en directa relación al entorno operacional propio de cada empleo de las fuerzas, conforme lo señala el gráfico de empleo de los procesos de inteligencia.



Además, sostienen que el motivo principal del empleo de estos procesos se da porque son las herramientas doctrinarias ya existentes a disposición en apoyo a los procesos de planificación institucionales, y que en ocasiones la tendencia radica en la complementación entre ambas y en la utilización de herramientas adicionales. No obstante, se destaca que el proceso JIPOE, se presenta con mayor grado de utilización, destacando que según los encuestados entrega las herramientas más adecuadas para analizar un ambiente multidimensional.

3) *¿Considera que el IPB, y específicamente el paso Nº3 "Evaluación de la Amenaza", es parte de un proceso metodológico y herramienta útil para el análisis de amenazas de naturaleza híbridas?.*

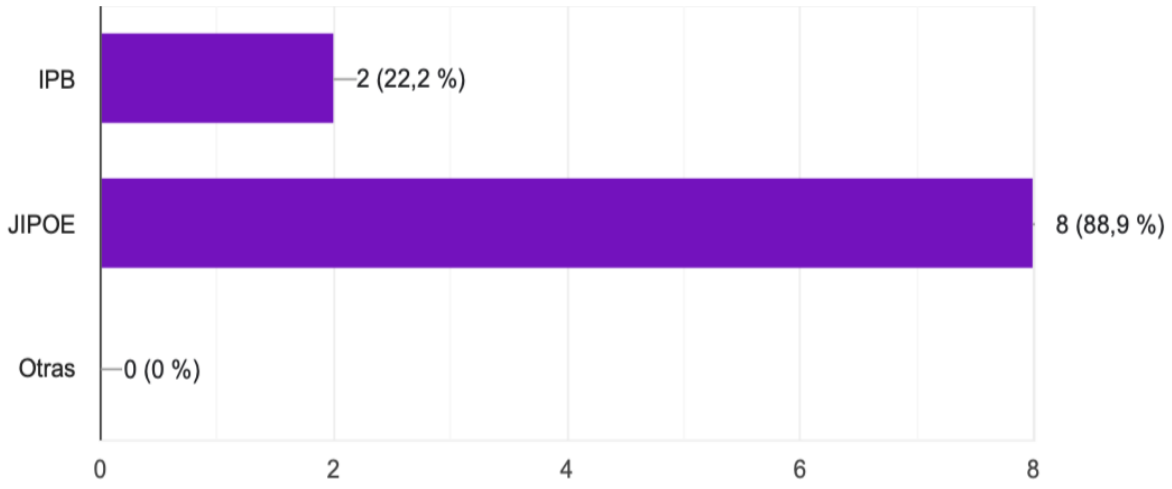
Según la información proporcionada por los encuestados, se concluye que IPB, no sería la mejor opción para analizar amenazas de naturaleza híbrida. Lo anterior, debido a que su origen y concepción está específicamente dirigido a una naturaleza de amenazas más tradicionales o convencionales y puede caer en la poca flexibilidad en situaciones que se requieren de un mayor grado de adaptabilidad de sus factores analíticos. Además, dado que las amenazas híbridas carecen de información doctrinaria en la reglamentación, no cuenta con todas las herramientas necesarias para definirlas y analizarlas correctamente. Por lo tanto, según el análisis de los especialistas en inteligencia, se sugiere ampliar esta herramienta para evaluar adecuadamente estas amenazas, complementándolas con otras metodologías como el JIPOE y otras utilizadas por organismos de inteligencia asociados a la seguridad interior, principalmente orientado a información existente en base de datos como es el caso de las instituciones de orden y seguridad. Por último, se pueden complementar con doctrinas similares como EE.UU. ya que están actualizadas y consideran variables o amenazas de naturaleza híbrida.

4) *¿Considera que JIPOE ofrece factores y variables de análisis suficientes y precisas para analizar un ambiente operacional complejo y amenazas de naturaleza híbridas?. ¿Si no es así, cuál serían los vacíos doctrinales y analíticos que usted evidencia de este proceso?.*

Según lo expresado por los encuestados, el JIPOE proporciona herramientas de análisis necesarias para comprender el ambiente operacional y las variables en todos los dominios, siendo incluso con sus deficiencias, la mejor opción hasta el momento para abordar posibles amenazas de naturaleza híbrida. No obstante, se señala que JIPOE es una herramienta de nivel operacional y carecería de cobertura táctica, especialmente cuando se enfrenta a amenazas híbridas y en la denominada "zona gris". En efecto, para subsanar lo anterior, se sugiere agregar más factores de análisis y considerar el cómo otras instituciones y países abordan este tipo de amenazas, como es el caso de los organismos policiales en nuestro país, DIRECTEMAR y DGAC, así como la doctrina de inteligencia de países como Colombia y Perú. En resumen, aunque el JIPOE brinda

herramientas importantes, se requiere una mayor integración de variables para abordar amenazas híbridas y complejas.

5) *¿Cuál es el proceso o herramienta de inteligencia que actualmente ostenta de mayores recursos para analizar amenazas de naturaleza híbridas?*



Conforme al gráfico, el gran porcentaje de encuestados manifestó que el JIPOE, es el proceso que ostenta de mayores recursos analíticos para poder evaluar una posible amenaza híbrida. Lo antes mencionado, debido a que ofrece herramientas analíticas más adecuadas para comprender el ambiente operacional considerando actores de naturaleza híbrida en todas las dimensiones. Esto, se debe a que abarca más variables y dispone de herramientas disponibles para apoyar el proceso de toma de decisiones. Además, debido a su capacidad para analizar una amplia variedad de ambientes, permite analizar el problema de una manera sistémica, lo que proporciona más herramientas para identificar diversas amenazas, independientemente de su naturaleza. En resumen, su enfoque ofrece una perspectiva más completa para el análisis de inteligencia, en comparación con otras herramientas disponibles.

6) *¿Qué otras variables de análisis deberían abordar los procesos de inteligencia presentes en nuestra doctrina institucional y conjunta, para analizar amenazas de naturaleza híbridas?*

Se concluye, que dentro de las variables de análisis que se deberían considerar con un mayor grado de profundidad en refuerzo a los factores establecidos en ambas metodologías, estarían los relacionados con el estudio de factores del espectro electromagnético, amenazas cibernéticas, aspectos socio culturales como las personalidades, liderazgo de sujetos claves y estudio de la población, ya que, el centro de gravedad de estas amenazas estaría condicionado por el entendimiento de estos factores.

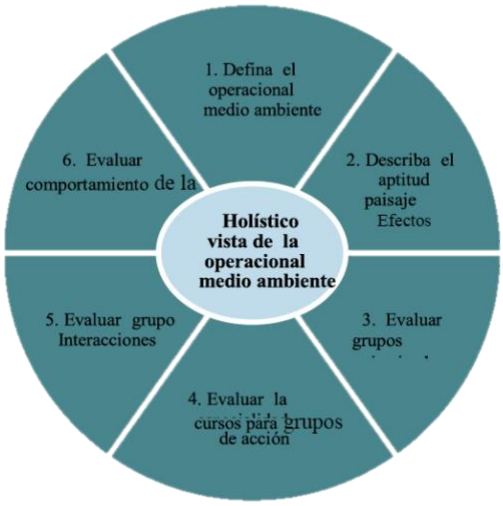
Adicionalmente y en respuesta a los resultados y opiniones del personal encuestado, en donde de manera importante se identificó sobre las orientaciones dirigidas a la revisión de nuevos textos doctrinarios y del énfasis en el análisis de nuevas variables para entender y evaluar estas amenazas, como es el caso de factores sociales y población, se expresan los siguientes fundamentos complementarios al desarrollo capitular.

4.4 IPB Complejo

Profundizando en herramientas más recientes, Morris al adaptar el IPB empleado en el Ejército de Estados Unidos a un IPB complejo, como él lo denominó, cuyo propósito tenía el de capacitar a personal de inteligencia ucraniano como parte del programa de cooperación del Centro Internacional de Mantenimiento de la Paz y Seguridad (IPSC), enfatizó sobre el estudio de la integración holística de las consideraciones civiles, considerando la interconexión multigrupal y la evaluación del comportamiento de la población, es decir, un análisis centrado en el ser humano, por sobre el análisis de un enemigo. Así, “esta adaptación en lugar de identificar y evaluar principalmente al enemigo o la amenaza, ayuda al personal de inteligencia a analizar múltiples grupos y cómo interactúan y se comportan colectivamente” (2017, p. 59). En tal sentido, una de sus grandes particularidades radica en la estructura de su metodología, la cual dista de los cuatro clásicos pasos de la mayoría de los procesos y se representa por medio de la siguiente imagen.

Imagen 9

“Estructura General del Proceso IPB Complejo”



Nota: Esquema que explica el proceso genérico de IPB Complejo, Antecedentes extraídos de (2017, p. 61).

Por su parte, IPB Complejo se aplicó en el contexto de Ucrania para comprender el movimiento separatista y las amenazas híbridas, identificando tanto los actores de las amenazas, como las estructuras de incentivos que impulsaban sus comportamientos. Se reconoció que las amenazas híbridas requerían una respuesta integral que debía ir más allá de la fuerza militar y que el análisis realizado a través de este proceso, proporcionaba una comprensión más completa de la situación operativa y de las operaciones antiterroristas.

En síntesis, se puede manifestar que esta adaptación enfatizó sobre el estudio de los aspectos socio-culturales y político-poblacionales dentro de un ambiente operativo. Por su parte, este enfoque buscó comprender cómo las decisiones individuales interactuaban y afectaban la dinámica de un grupo, destacando la importancia de considerar las interacciones entre individuos, poblaciones y Estados, así como los efectos vinculantes de las interacciones más pequeñas y directas.

4.5 IPB ATP 2-01.3

Por otra parte, el actual reglamento de proceso IPB del Ejército estadounidense, ATP 2-01.3, conforme lo representa la imagen, incluye y proporciona fundamentos actualizados para el análisis de nuevas tipologías de amenazas.

Imagen 10

"Estructura General de actual Proceso IPB en doctrina Estadounidense"

Nota: Esquema que explica el proceso genérico de IPB, Antecedentes extraídos de (ATP 2-01.3, 2019, p. 1-3).

Es así, que como una manera de indagar sobre sus fundamentos, se estableció su revisión a base de los mismos criterios definidos en la comparación realizada de manera precedente.

Tabla 8

"Fundamentos paso Nº3 "Evaluación de la Amenazade IPB (ATP 2-01.3), edic. 2019"

Criterio	Observaciones
1. Naturaleza, propósito y metodología del paso Nº3 "Evaluación de la Amenaza".	• Determinar las capacidades de la amenaza, sus principios doctrinales, fuerza y sus TTP preferibles de empleo, representadas por (fuerzas regulares, irregulares, terroristas y elementos criminales). • Utilización de tácticas tradicionales y no tradicionales. • Las amenazas se dividen en regulares, irregulares e híbridas. • Identificación de características del adversario, a través del análisis de los factores ORBAT. • Creación o refinamiento de modelos de amenazas, por la conversión

	doctrinal o la realización de gráficos de patrones de operaciones. • Establecimiento de HVTs y posibles HPT.
2. "Factores ORBAT"	• Este proceso emplean las siguientes variables del ORBAT: – Composición. – Fuerza. – Dispositivo. – Doctrina y tácticas o procedimientos de empleo. – Logística. – Eficiencia de combate. – Características especiales. • En su Apéndice C "Características de la Amenaza", entrega factores del ORBAT relacionados específicamente a una amenaza híbrida.
3. Productos de inteligencia entregados al final del paso.	1. Archivos de datos de amenaza. 2. Plantilla de amenaza. 3. Lista de HVT. 4. Declaración de la capacidad de la amenaza.
4. Enfoque en análisis relacionado con amenazas no convencionales.	Este nuevo texto, a diferencia de nuestro IPB edic. 2015, presenta las siguientes diferencias. **Paso Nº1** • Analiza el AO y no se limita solamente al campo de batalla. • Considera el concepto y fundamentos de operaciones multidominios. **Paso Nº2** • Amplia el análisis de los factores ASCOPE a los PMESII-PT y los relaciona a través de una matriz de impacto cruzado. • Ejemplificación del estudio militar del terreno para zonas urbanas. • Integración del IPB y ciberespacio. • Hace referencia sobre el análisis del entorno físico, temporal, cognitivo y virtual. **Paso Nº3** • Describe características de amenazas regulares, irregulares e híbridas. • Factores ORBAT con especificación híbrida. • Complementa las herramientas de análisis a través de la matriz CARVER (Criticidad, Accesibilidad, Recuperabilidad, Vulnerabilidad, Efecto y Reconocimiento) para el análisis de objetivos e identificación de riesgos. **Paso Nº4** • Ejemplificación de plantillas de situación para fuerzas regulares e irregulares. • Ejemplificación de plan de obtención de información. **Otros** • Consideración de operaciones de estabilidad. • Fundamentación para inteligencia de seguridad civil. • Evaluación para organizaciones de amenazas internas. • Orientaciones para operaciones de crisis humanitarias. • Antecedentes para evaluación de desarrollo económico.

	• Antecedentes para evaluación de desarrollo de infraestructura. • Antecedentes de ambientes únicos (entornos litorales y entornos urbanos).

Nota: Esta tabla muestra los fundamentos doctrinales del paso Nº3 “Evaluación de la Amenaza” del nuevo reglamento IPB utilizado por el Ejército de EE.UU. en la actualidad.

Del mismo modo, al analizar el actual Reglamento de Preparación de Inteligencia del Campo de Combate del Ejército de Colombia, MTE 2-01.3 (2019), se evidenció que tiene los mismos fundamentos que el actual IPB estadounidense, por lo cual, se infiere que su actualización fue producto de un proceso de traducción por parte de su centro de doctrina institucional.

En conclusión y en relación a las actividades realizadas en cumplimiento a la presente metodología capitular, se obtienen los siguientes resultados:

Revisión bibliográfica y relación del Proceso IPB y JIPOE bajo el contexto de análisis de amenazas híbridas.

Nuestros procesos de inteligencia, IPB y JIPOE carecen de fundamentos explícitos y específicos sobre esta tipología de amenazas, ya que no se consideran en la reglamentación y no se identifican factores de análisis específicos para ellos, sometiéndose simplemente a operaciones y amenazas irregulares asociadas principalmente a insurgencia y operaciones de estabilidad.

Pertinencia de IPB y JIPOE en el análisis de amenazas híbridas.

IPB, se sintetiza como un proceso de inteligencia de nivel táctico, que se direcciona en definir y comprender un campo de batalla basado en un entorno físico, analizando una amenaza de carácter predominantemente convencional o regular. Sin embargo, entrega interesantes recursos analíticos en la etapa final de su texto, en relación con el empleo de fuerzas en MOOTW, y en como algunos recursos de inteligencia existentes ligados al análisis del terreno y amenazas en zonas urbanas y en donde adquiere importancia la

población, apoyan el entendimiento de un entorno operativo más complejo y de posibles amenazas no convencionales. No obstante, el personal encuestado manifestó que no sería el proceso más adecuado para analizar un entorno y una amenaza que fluctúa en los diferentes niveles y el cual emplea métodos convencionales como irregulares, representados por una variada lista de alternativas en su empleo. Por lo tanto, la complementación con otras herramientas como el JIPOE, vendría a suplir esta deficiencia.

En otro sentido, JIPOE se establece como un proceso de inteligencia de nivel operacional con la capacidad de complementarse con las tareas y resultados realizados en el nivel táctico, los cuales, no están profundizados. Así, se orienta a definir y describir un ambiente operacional conjunto, bajo un análisis físico, de información y cognitivo, en donde las operaciones se pueden ver representadas a través de operaciones en diferentes dominios, con la particularidad que proporciona adicionalmente factores de análisis altamente valiosos como los PEMSII, los cuales permiten entender el ambiente operacional desde una perspectiva sistémica, permitiendo relacionar actores, eventos, vínculos, enlaces de organismos tanto internos como interagenciales, entre otros, entidades propias de un ambiente complejo y en donde las amenazas híbridas sacan su mayor provecho y rendimiento. Además, dentro de las fortalezas identificadas, se destaca los recursos entregados, los cuales, permiten analizar a una amenaza tanto regular como irregular, mencionando principalmente las acciones ligadas al (terrorismo, insurgencia), enfatizando que este proceso puede ser adaptado de acuerdo con la amenaza y ambiente específico requerido y se puede complementar con herramientas adicionales más específicas.

4.6 Síntesis capitular

El propósito de este capítulo, fue dar respuesta a la pregunta Nº3 *¿Cuáles son las diferencias analíticas de los procesos IPB y JIPOE, en el contexto de amenazas híbridas?.* En efecto, los temas claves analizados para el desarrollo de este capítulo, fueron los concernientes a los procesos IPB y JIPOE, aspirando a identificar sus fundamentos, particularidades y sus factores de análisis de una amenaza, en una relación directa con la evaluación de amenazas híbridas, complementando la información descrita, con el estudio

general de otros procesos más actualizados y que incluyen factores de análisis más sólidos en la comprensión de un ambiente operacional complejo y en donde interactúan otras amenazas no convencionales y contemporáneas. En este sentido, la metodología capitular se sustentó principalmente en un trabajo comparativo del tipo descriptivo, sustentado en la revisión de contenidos propios de la reglamentación de ambas metodologías de inteligencia. Respecto de los hallazgos conseguidos, al igual que en el capítulo anterior, inicialmente se buscó identificar la relación directa y manifiesta de estos procesos y su vinculación con el concepto híbrido. En consecuencia, se evidenció sobre la falta de fundamentos explícitos, sumado a la ausencia de factores de análisis específicos para abordarlas, circunscribiéndose a la existencia de información ligada a operaciones y amenazas irregulares, representadas principalmente por la insurgencia y operaciones de estabilidad.

Así mismo, se realizó un estudio comparativo de los factores de análisis, principalmente enmarcados en el paso Nº3 “Evaluación de la Amenaza”, y adicionalmente por medio de otros criterios de comparación, con el propósito de determinar las semejanzas y diferencias de las variables y factores evaluativos de cada metodología, permitiendo con lo anterior, establecer ciertas fortalezas, debilidades y su posible pertinencia en el análisis de estas amenazas. Del mismo modo, esta información fue complementada con las opiniones de personal idóneo en el ámbito de la función, con la finalidad de contribuir a robustecer las conclusiones realizadas, principalmente en la determinación del grado de pertinencia en el análisis de estas amenazas, las cuales, rápidamente han adoptado mecanismos propios de esta naturaleza.

Es pertinente mencionar, que existen muchas discrepancias en las opiniones de los encuestados, evidenciándose una falta de lineamientos con respecto a la opinión, enfoque, utilización y experiencias obtenidas en el empleo de estos procesos, infiriéndose que estos procesos son metodologías que entregan herramientas, y el rendimiento y uso adecuado, se circunscribe en muchas ocasiones, al conocimiento, experiencia y habilidad del analista.

No obstante, por medios de las acciones realizadas, se pudo concluir que nuestro actual IPB es un proceso de inteligencia dirigido principalmente al análisis de amenazas convencionales y de nivel táctico, con una notoria carencia de factores importantes para analizar un ambiente operacional más complejo, multidimensional, y bajo una perspectiva física y cognitiva, entorno propio en donde coexisten estas amenazas. Sin embargo, conforme al nivel de la conducción que lo caracteriza, presenta recursos específicos importantes y adaptables para analizar amenazas no convencionales principalmente en MOOTW, por medio de algunas herramientas teóricas y graficas para evaluar entornos urbanos y el posible empleo de amenazas no convencionales en él, necesitando la complementación con el JIPOE, para a través de ambas, subsanar las deficiencias enfocadas principalmente en la comprensión del ambiente operacional y de todos los elementos que interactúan de manera compleja y por medio de acciones multidimensionales.

En el mismo sentido, JIPOE, se presenta como un proceso más íntegro y completo, representado por recursos adicionales que permiten evaluar a una amenaza que interactúa en los diferentes niveles de la conducción y por medio de operaciones multidominios, en el ambiente de la información, cognitivo y físico, sumado a factores de análisis que permiten entender un complejo ambiente operacional desde una perspectiva sistémica, dando un alto grado de flexibilidad y adaptación a los recursos disponibles. Sin embargo, también presenta deficiencias por si sola, para analizar eventos y amenazas que operan en terrenos altamente complejos, como los urbanos, selváticos, boscosos y para el análisis de amenazas que operan en el nivel táctico. De lo anterior, se desprende que, para analizar amenazas híbridas, considerando todas sus características definidas, también debe ser complementada con otros procesos de nivel táctico, en nuestro caso y bajo nuestra doctrina con el IPB.

Adicionalmente, y como resultado de la indagación de otros procesos y herramientas de inteligencia, se evidenció que algunas instituciones han actualizado su reglamentación con el propósito de incluir mayores fundamentos acerca del entendimiento del ambiente operacional y de las distintas amenazas que interactúan en él, por medio del

establecimiento de información más específica e integral en beneficio de los analistas. Finalmente, y concluyendo con lo anterior, las acciones realizadas permiten cumplir con el objetivo específico de este capítulo, el cual es, describir sobre las diferencias analíticas de los procesos IPB y JIPOE y su pertinencia de análisis en el contexto híbrido.

CAPÍTULO V

CONCLUSIONES Y PROPUESTAS

5.1 Conclusiones

Durante el desarrollo del presente capítulo, se exponen las conclusiones establecidas como parte de los resultados alcanzados durante este trabajo de investigación. Para lo anterior, se realizó una síntesis enlazada con cada uno de los objetivos parciales, dando respuesta a las preguntas específicas, y consecuente con ello, al objetivo general de este trabajo. Asimismo, en esta síntesis, se consideró pertinente expresar los aspectos tanto positivos y negativos que repercutieron y condicionaron el desarrollo de las actividades realizadas, las cuales, influyeron en la determinación de los resultados finales. Finalmente, se realizarán algunas propuestas derivadas de los resultados obtenidos.

5.2 Síntesis

En el capítulo I *"Problema de investigación",* se estableció la problematización, como consecuencia de una breve síntesis del estado del arte realizado respecto a los conceptos relacionados con la amenaza híbrida y con los procesos de preparación de inteligencia, específicamente enfocado en lo que definió DIPLINE al generar la necesidad del estudio y análisis de la metodología IPO, la cual según este estamento, se erigía como una metodología vanguardista y específica para analizar nuevas amenazas emergentes como son las híbridas.

En este contexto, se dio origen al cuestionamiento acerca de que si el proceso IPO, se podría constituir como una metodología pertinente para el análisis de estas amenazas. No obstante, al indagar en su fundamentación se pudo dilucidar que era un proceso obsoleto, pero que sin embargo, proporcionaba un enfoque específico para el estudio de amenazas irregulares. Por otro lado, conforme a la opinión de expertos en la materia, se planteó del mismo modo, la inquietud sobre la pertinencia de los procesos vigentes en nuestra doctrina y reglamentación, cuestionando si es que era necesario indagar en esta metodología extrainstitucional, lo que conllevó finalmente a plantear el problema de investigación a base de que si IPO, IPB y JIPOE podrían ser atingentes de analizar estas amenazas más complejas.

En consecuencia, el desarrollo de los capítulos posteriores se enfocó en dar respuesta a los objetivos específicos, los cuales fueron desarrollados durante esta investigación. En efecto, este capítulo además de establecer el problema de investigación, recorre de manera estructurada el proceso metodológico, dando validez a la metodología desarrollada posteriormente, estableciendo claramente los límites del trabajo, así como los procedimientos para dar cumplimiento al rigor científico exigido.

El capítulo II *"Amenaza Híbrida*" tuvo por finalidad definir que es una amenaza híbrida, en consideración a que en nuestra reglamentación no existe una definición formal de esta tipología de amenaza, supeditándose exclusivamente a lo que manifiestan algunas directivas del nivel político, cuya información se centra básicamente a entregar algunas orientaciones dirigidas a las capacidades que se deben alcanzar para contrarrestarlas.

Para este cometido, la metodología utilizada fue a base de análisis de contenido, indagando sobre este concepto a través de la clasificación de tres orígenes de fuentes en particular. La primera de ellas, por medio de la revisión documental de fuentes bibliográficas escritas por teóricos expertos en seguridad y defensa de nivel nacional e internacional. Seguidamente, por la indagación de textos de carácter directivo del nivel político como fue el caso del Libro de la Defensa Nacional y la Política de Defensa Nacional de Chile, y finalmente, por la revisión bibliográfica doctrinaria de países de referencia y de otras instituciones, las cuales tienen internalizados formalmente el concepto y existencia del contexto híbrido, como es el caso de EE.UU., España, Colombia, UE y OTAN.

Lo anterior, permitió recopilar importante información sobre aquellas características, semejanzas, diferencias y cualidades de estas amenazas, antecedentes que fueron definidos, categorizados, interpretados y analizados, permitiendo generar esquemas que facilitaron el establecimiento de cualidades equivalentes con el propósito de establecer una definición más objetiva. Como resultado de señalan las siguientes cualidades obtenidas, las cuales se circunscriben desde una perspectiva del nivel de la conducción operacional y táctico.

1. *Posibilidad de participación de actores estatales y no estatales.*
2. *Empleo de diferentes modalidades de guerra a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica, unificada y sincronizada.*
3. *Empleo del espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación.*
4. *Intensa participación de la población civil ya sea en apoyo o como objetivo en el conflicto.*
5. *Empleo de armamento de alta tecnología y bajo una perspectiva estratégica.*
6. *Empleo en terrenos altamente complejos.*
7. *Campañas multidimensionales.*

Sin embargo, es pertinente mencionar, que para instaurar un mayor grado de solidez en las conclusiones y en esta definición, se realizó un estudio de casos a base de la Guerra del Líbano del 2006, la cual fue considerada por expertos como paradigma de la guerra híbrida y los acontecimientos que están ocurriendo actualmente en la guerra de Ucrania.

Finalmente, y una vez habiendo realizado la totalidad de las acciones señaladas en la metodología capitular, las cuales permitieron dar cumplimiento al primer objetivo específico de esta investigación, se definió amenaza híbrida como la:

> *"Combinación diversa y dinámica de diferentes modalidades de guerra a través de campañas multidimensionales, realizadas con la participación de actores estatales y no estatales a través de capacidades convencionales, tácticas y formaciones irregulares, terrorismo y crimen organizado bajo una visión estratégica unificada y sincronizada, en terrenos altamente complejos y con el empleo de armamento de alta tecnología, empleando el espacio virtual o ciberespacio para la realización de ciberataques, operaciones de información y desinformación, complementado con una intensa participación de la población civil, ya sea en apoyo o como objetivo en el conflicto"*[10].

[10] Definición elaborada por el autor.

Lo anterior, como base de esta conceptualización, permitiendo seguir dando curso a los capítulos posteriores.

El capítulo III *"Proceso de Preparación de inteligencia para las Operaciones IPO*" tuvo como propósito describir en qué consistía este proceso de preparación de inteligencia, y cuál era su pertinencia de análisis en el contexto de amenazas híbridas. Para el desarrollo de este capítulo, se estimó necesario descomponer el trabajo de indagación en tres segmentos diferenciados, siendo la metodología empleada la de análisis de contenido.

En consecuencia, inicialmente se buscó identificar por medio de la revisión de este proceso, su relación directa y explícita con el contexto híbrido. El resultado obtenido arrojó que IPO no abordaba de manera evidente este concepto. Sin embargo, en el ámbito de amenazas no convencionales, presentó información sólida y específica para la evaluación de amenazas irregulares, ligadas a la materialización de actos terroristas, delictuales y al crimen organizado, propios del contexto nacional de EE.UU. en los primeros años de la década del dos mil.

Posteriormente, se buscó describir sus antecedentes generales, conceptualización, propósitos y fundamentación. De lo anterior, se pudo concluir que este proceso surgió como una alternativa a las limitaciones identificadas de la doctrina de IPB en Estados Unidos de los años 90, específicamente del Manual de Preparación de Inteligencia del Campo de Batalla IPB (FM 34-130), publicado en julio de 1996. En tal sentido, IPO fue una herramienta de carácter policial y criminal, basado en el concepto de defensa activa, centrada en materializar una secuencia de acciones orientadas a la evaluación, análisis, previsión y toma de decisiones para enfrentar amenazas del tipo irregular, con un énfasis especial a la materialización de acciones en terrenos altamente complejos como son los urbanos. Lo anterior con la particularidad que este proceso se sustentó a base de la colaboración de diversos organismos multidisciplinarios con conocimiento sobre asuntos de Seguridad y Defensa. En efecto, IPO se construyó como un proceso basado en análisis y síntesis de información, a través de solicitudes iterativas de información, estructurado en cuatro pasos similares al IPB y JIPOE que conocemos actualmente en nuestra doctrina

institucional y conjunta, conforme a lo plasmado específicamente en los Anexos Nº1,2,3,4,5 y 6 de esta investigación.

Por último, el tercer segmento, buscó realizar un cuadro descriptivo con las principales características de sus factores analíticos, propendiendo a dilucidar acerca de su vinculación y pertinencia en el análisis de las amenazas señaladas. En efecto, y producto del contraste de sus factores evaluativos con la definición de amenaza híbrida realizada en el capítulo II, y de la complementación de las opiniones de especialistas en inteligencia que actualmente se desempeñan como comandantes de AGRINT, asesores de inteligencia en cuarteles generales de UACs y de oficiales que impartieron la doctrina de procesos de inteligencia institucionales y conjuntos en la Escuela de Inteligencia, se logró establecer que este proceso, si bien, entrega ciertos fundamentos atingentes para evaluar estas amenazas emergentes, carece de variables fundamentales para analizar entornos complejos, multidimensionales y en donde los actores del conflicto, se caracterizan por transitar activamente en los diferentes niveles de la conducción, por medio de variados mecanismos convencionales y no tradicionales de acción, en el ambiente, físico, informativo y cognitivo.

Es oportuno mencionar, que el actual manual de IPB en nuestra doctrina entrega fundamentos para analizar amenazas irregulares en terrenos urbanos, y la última actualización del Ejército de EE.UU. y Colombia, proporcionan información y recursos para evaluar amenazas irregulares e híbridas, lo que se traduce en que, a pesar de los posibles aportes que podría proporcionar el proceso IPO, actualmente los procesos de inteligencia consideran también variables para analizar amenazas irregulares en estos escenarios.

Finalmente, el capítulo IV *"IPB y JIPOE y su pertinencia de ser empleados en el análisis de amenazas híbridas"*, buscó describir cuales son las diferencias analíticas de los procesos IPB y JIPOE en el contexto de la evaluación de lo híbrido. Para el desarrollo capitular, la metodología se ajustó a la realización de un análisis comparativo del tipo descriptivo entre ambas metodologías. De esta forma y al igual que en el capítulo anterior, primero se consultó en la fundamentación general de estos procesos en relación con lo

que proporcionaban sobre el análisis de un entorno híbrido. En este sentido, ambas metodologías no consideraron de una forma manifiesta esta conceptualización, haciendo solamente referencia en grandes rasgos, a operaciones y amenazas irregulares y asimétricas, ligadas a la insurgencia y operaciones de estabilidad. No obstante, JIPOE menciona otro tipo de acciones como el terrorismo, crimen organizado, pero desprovisto de información específica al respecto.

Seguidamente, se realizó un análisis comparativo de ambas metodologías, señalando las semejanzas y diferencias de sus recursos analíticos bajo criterios de comparación cimentados principalmente a base del paso Nº3 “Evaluación de la Amenaza” y de otros ciertos criterios circunscritos en los pasos Nº1 y 2 de estos procesos. Como resultado, se logró establecer una diferenciación sólida, en lo que respecta al entendimiento del ambiente operativo, como también al análisis de un posible adversario.

En tal sentido, como corolario de las conclusiones del investigador y de la opinión de especialistas en inteligencia, ambas metodologías presentan fortalezas y limitaciones, sin embargo, el proceso IPB se enfoca principalmente en definir y comprender un campo de batalla bajo un entorno físico en el nivel de la conducción táctica, analizando amenazas en un mayor énfasis convencionales, con la peculiaridad que ofrece ciertos recursos analíticos para el empleo de fuerzas principalmente en MOOTW. Por otro lado, JIPOE se establece como un proceso de inteligencia del nivel de la conducción operacional, que permite definir un ambiente operacional conjunto, considerando diferentes dominios, y ofrece factores de análisis valiosos como lo son las variables PMESII, los cuales contribuyen a comprender un entorno operativo de manera sistémica.

Ahora bien, según los especialistas, IPB no sería la mejor opción para analizar amenazas híbridas, ya que su enfoque está dirigido a amenazas más tradicionales y carece de las herramientas necesarias para abordarlas correctamente, por lo tanto, sugieren ampliar los recursos de esta metodología y complementarla con otras utilizadas en nuestra doctrina militar y en acciones propias de seguridad interior, como es el caso de organismos de orden y seguridad. En cambio, según los encuestados, JIPOE ofrece una mayor cantidad

de recursos analíticos y una perspectiva más completa para el análisis de inteligencia en comparación con otras herramientas, por lo que se considera la mejor opción hasta el momento, para abordar amenazas híbridas, aunque señalan que carece de cobertura táctica en la "zona gris". Además, se sugiere complementar este proceso con otras de nivel táctico y agregar más factores de análisis, como los asociados al espectro electromagnético, aspectos socioculturales y amenazas cibernéticas y considerar adicionalmente, cómo otras instituciones y países abordan estas amenazas.

Finalmente, con todo lo anteriormente expuesto, fue factible dar cumplimiento al propósito del capítulo, quedando identificadas las diferencias y semejanzas de cada metodología y estableciendo que actualmente el proceso de inteligencia, por si sólo, que mejor apoyaría la evaluación de un ambiente complejo y de amenazas de naturaleza híbrida en apoyo a los procesos de planificación de operaciones en nuestro contexto nacional, se representaría a través del proceso JIPOE. Sin embargo, para un análisis integral necesitaría la complementación con procesos de nivel táctico que presenten factores y variables de análisis en terrenos altamente complejos.

5.3 Valoración

Durante el desarrollo de la presente investigación, se consideró de gran valor algunos aspectos positivos del proceso de análisis de la información, pero también es pertinente reconocer aspectos deficientes identificados en el transcurso del desarrollo de los respectivos capítulos.

En tal sentido, la primera fortaleza observada fue la estructuración del problema de investigación y la delimitación establecida, puesto que el proceso IPO, fue definido de una manera errónea al precisarla como una metodología actualizada y vanguardista para el análisis de amenazas híbridas. En este contexto, se esclareció que fue una herramienta empleada hace casi veinte años atrás, cuya formulación se dirigía a la evaluación de amenazas irregulares, ya que no se manejaba con solidez en el ámbito de la defensa y seguridad, el concepto del conflicto y amenaza híbrida.

Por otro lado, fue positivo la capacidad de poder desarrollar a base de la indagación bibliográfica y doctrinaria de países de referencia, el concepto de amenaza híbrida y las

características e implicancias que ello conllevó. Lo anterior, permitiendo construir una definición objetiva y desde un ámbito militar, la que permitió vincular estas características con los procesos de preparación de inteligencia abordados posteriormente.

Otro aspecto beneficioso, fue la indagación realizada a la doctrina actualizada de inteligencia, como fue el caso de la última edición del IPB estadounidense ATP 2-01.3, y del manual de Preparación de Inteligencia de Campo de Combate MTE 2-01.3, del Ejército Nacional de Colombia, las que permitieron evidenciar que actualmente sus instituciones armadas cuentan con fundamentos renovados y con una información más consistente para analizar fenómenos que se ven representados en el acontecer internacional, regional y nacional.

Al mismo tiempo, se destaca la posibilidad de poder contar con la opinión de especialistas en inteligencia, los cuales a través de sus experiencias en tareas propias de la función en el análisis de un entorno operativo y de las amenazas presentadas en los últimos EE-C, contribuyeron a reforzar y de cierta manera a validar las conclusiones obtenidas del análisis de contenidos, comparaciones y descripciones de los factores y variables analíticas de los distintos procesos, con una especial vinculación a la naturaleza y modos de acción de estas amenazas.

En otro sentido, dentro de las limitaciones identificadas, se señala la falta de información, experiencias en el empleo y resultados del proceso IPO, al ser una metodología obsoleta y de total desconocimiento en nuestro ámbito nacional. Lo anterior, radicó en que las conclusiones se sujetaron específicamente a la escaza documentación obtenida y principalmente a los análisis y proposiciones realizadas por el investigador producto de la revisión documental.

Del mismo modo, no fue posible acceder a resultados empíricos y formales del empleo de nuestras metodologías institucionales y conjuntas por parte de los especialistas en inteligencia, ya sea por el carácter de confidencialidad de la información o porque estos procesos no son un fin en sí mismos e insumos definitivos, sino que se basan en tareas que apoyan a la toma de decisiones del comandante en contribución al empleo de la fuerza, por lo que están sujetas a modificaciones y actualizaciones, con la principal característica, que en forma constante se complementan y muchas veces son reemplazadas por otros recursos informales más idóneos y propios de las circunstancias.

Finalmente, lo antes señalado obligó a mantener el desarrollo de la investigación muy adherido a la revisión doctrinal y conceptual, más que a la obtención de datos concretos y fundamentos estadísticos del resultado del empleo de estos procesos.

5.4 Propuestas.

Como punto de término de las conclusiones, se estima conveniente incluir algunas proposiciones dada la naturaleza de los hallazgos. En este sentido se evidenciaron ciertas deficiencias, las que se podrían convertir en oportunidades al momento de considerarlas y abordarlas por los organismos pertinentes:

1) Se estima conveniente, enviar este informe a través del CEEAG a DIPLINE, ya que fue el estamento que generó este tema de investigación, con el propósito de presentar los resultados de los temas planteados y establecer las aclaraciones pertinentes del proceso de inteligencia bajo estudio.

2) Incorporar a la doctrina de inteligencia institucional, el concepto de amenazas híbridas y especificaciones propias de los factores del ORBAT en relación con sus fundamentos atingentes, como es el caso de Estados Unidos y Colombia, instituciones armadas que actualmente han actualizado su reglamentación de IPB incorporando factores de información y análisis específicos para entender y evaluar estas amenazas.

3) Implementar las herramientas existentes en nuestra doctrina, ya que si bien, JIPOE e IPB, constan de recursos analíticos pertinentes para evaluar amenazas regulares e irregulares de manera particular, no se han implementado sobre el análisis de amenazas híbridas, ya sea porque no se han realizado ejercicios en donde se defina e instaure este tipo de amenaza, o porque en la realidad no se han analizado amenazas categorizadas íntegramente dentro de esta tipología, supeditándose sólo a lo irregular.

4) Realizar un proceso de estandarización de criterios doctrinarios en la ESCINT en conjunto con otros estamentos como el CEDOC, y especialmente la ACAGUE. Complementariamente, elaborar nuevos ejercicios de planificación a los alumnos, con

el propósito de implementar los diferentes procesos y obtener resultados del análisis de nuevos escenarios y amenazas híbridas.

5) Otra propuesta radica en que a través del CEAAG, se generen otras líneas de investigación, en el sentido de analizar la pertinencia e integración de otros procesos doctrinarios como el Proceso de adquisición de blancos, frente a amenazas híbridas.

REFERENCIAS BIBLIOGRÁFICAS

Arteaga, M. (2020). *El Conflicto Híbrido, Una contribución para la incertidumbre*. En CEEAG, *El Conflicto Híbrido y sus efectos en la Conducción Operacional y Táctica* (págs. 19 - 43). Santiago: Centro de Estudios Estratégicos de la Academia de Guerra.

ATP 2 - 01.3. (2019). *"Intelligence Preparation of the Battlefield".* Washington: Department of the army.

Bargués, P. (2022). *Conflicto Híbrido, Guerra total.* https://www.cidob.org/publicaciones/serie_de_publicacion/opinion_cidob/2022/conflicto_hibrido_guerra_total

Begert, M., & Lindsay, D. (2002). *"Intelligence Preparation for Operations". Small Wars and Insurgencies*, 133 - 143.

Bowers, C. O. (2014). *¿Cómo identificar los adversarios híbridos emergentes? Military Review*, 30 - 40.

Cárdenas, M. (2022). *Cómo la OTAN lucha contra las amenazas híbridas. LISA News. https://www.lisanews.org/ciberseguridad/como-la-otan-lucha-contra-las-amenazashibridas/*

Carter, D. (2016). *Nubes o relojes: Las limitaciones de la Preparación de Inteligencia del Campo de Batalla en un mundo complejo*. *Military Review*, 10-15.

Castro, M. (2022). *¿Cuáles son las tácticas de combate ucranianas que ponen en peligro a los civiles según amnistía Internacional?.* https://elcomercio.pe/mundo/actualidad/guerra-ucrania-rusia-cuales-son-lastacticas-de-combate-ucranianas-que-ponen-en-peligro-a-los-civiles-segun-amnistia internacional-dombas-jarkov-y-mykolaiv-vladimir-putin-volodymyr-zelensky-ecpm-noticia/?ref=ecr

CEEAG. (2017). *Investigación en Ciencias Militares claves metodológicas.* Santiago.

CEEAG. (2020). *El Conflicto Híbrido y sus efectos en la conducción Operacional y Táctica.* Santiago: Centro de Estudios Estratégicos de la Academia de Guerra.

Cervantes, D. (2017). *Métodos de investigación en Ciencias Militares*. En C. d. CEEAG, *Investigación en Ciencias Militares: Claves metodológicas* (pág. 88). Santiago: CEEAG.

Cervantes, D. (2019). *"Clase de metodología de la Investigación"*. Santiago: Academia de Guerra.

CESIM III SIDE (R) Nº 6030/2359.

Collier, D. (2010). *Rethinking Social Inquiry: Diverse Tools, Shared Standars.* New York: Rowman and Littlefield Publishers.

Colom, G. (2019). *La amenaza híbrida: mitos, leyendas y realid*ades. *ieee.es*, 1-14.

Cordesman, A., Sullivan, G., & Sullivan, W. (2007). *Lesson ofe the 2006 Israeli - Hezbollah War.* Washington, DC: Centro de Estudios Estratégicos e Internacionales.

Cuevas, I. (2023). *Mercenarios y voluntarios: los otros protagonistas de la Guerra de ucrania.* https://www.latercera.com/earlyaccess/noticia/mercenarios-y-voluntarios-los-otros-protagonistas-de-la-guerra-ucrania/ZTJJ3FEMJRB4DEDWUR7UP7NK3E/

DD – 10001 (2019). *La Fuerza Terrestre.* Santiago. DIVDOC.

DNC 2-04. (2022). *Preparación de Inteligencia del Ambiente Operacional Conjunto (JIPOE).* Santiago: Ministerio de Defensa.

Ejército de Chile, (2012). *Reglamento Inteligencia.* Santiago: DIVDOC.

El Radar, (2022). *El combate urbano está cambiando. La Guerra de Ucrania lo demuestra.* https://www.elradar.es/el-combate-urbano-esta-cambiando-la-guerra-de-ucrania-lo-demuestra/

Gaete, A. (2017). Análisis e interpretación de datos cualitativos. En C. d. CEEAG, *Investigación en Ciencias Militares: Claves metodológicas* (pág. 151-165). Santiago: CEEAG.

Gómez, L. E. (2011). *Un espacio para la investigación documental*. *Vanguardia Psicológica Clínica Teórica y Práctica*, 226-233.

Grisales, O. E. (2015). *Evolución de las nuevas amenazas a la Seguridad Nacional*. Recuperado de: http://hdl.handle.net/10654/13870.

Herrera, M. (2017). *Técnicas e instrumentos de recolección de datos en Ciencias Militares*. En CEEAG, *Investigación en Ciencias Mlilitares: Claves Metodológicas* (págs. 100 - 114). SAntiago: CEEAG.

Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

Hoffman, F. (2009). *Hybrid vs Compound War*. *Armed Forces Journal*. Obtenido de http://armedforcesjournal.com/hybrid-vs-compound-war/.

Ibáñez, L. (2022). *¿Qué sabemos sobre el Grupo Wagner?.* https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEEINV04_2022_LUICOR_Wagner.pdf

Korybko, A. (2019). *Guerras Híbridas: Revoluciones de Colores y Guerra No Convencional. El Enfoque Adaptativo Indirecto para el cambio de régimen.* Argentina: Batalla de Ideas.

Liang, Q., & Xiangsui, W. (1999). *"Unrestricted Warfare".* Beijing: PLA Literature and Arts Publishing House.

Lutska, V. (2022). *Rusia es un Estado terrorista y debe ser reconocido como tal a nivel internacional*. https://war.ukraine.ua/es/articles/rusia-es-un-estado-terrorista-y-debe-ser-reconocido-como-tal-a-nivel-internacional/

Martínez, F. (2012). *La Inteligencia en los Conflictos Híbridos*. En C.S. Nacional, *El Enfoque Multidisciplinar en los Conflictos Híbridos* (págs. 65 -70). Madrid: Ministerio de Defensa.

Marson, J. Hinshaw, D. (2022). *Civiles Ucranianos se unen para defender la patria de la amenaza rusa*. https://www.latercera.com/mundo/noticia/civiles-ucranianos-se-unen-para-defender-la-patria-de-la-amenaza-rusa/46TS5HC3PRCFTFF4Z5EOZLVSB4/

MCE 3-24.0. (2021). *MCE 3-24.0 "Amenaza Híbrida en un Ambiente Operacional".* Bogotá: DIPOE.

MDN. (2012). *El Enfoque Multidisciplinar en los Conflictos Híbridos*. Madrid: Ministerio de Defensa Nacional.

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

MDN. (2020). *Política de Defensa Nacional de Chile.* Santiago: Ministerio de Defensa Nacional.

Morris, V. (2017). *Complex Intelligence Preparation of the Battlefield in Ukrainian Antiterrorism Operations*. Military Review 2017, 58-65. https://www.armyupress.army.mil/Portals/7/militaryreview/Archives/English/MilitaryReview_2017228_art012.pdf

MTE 2 – 01.3, (2019). *Preparación de Inteligencia del Campo de Combate.* Bogotá: Centro de Doctrina del Ejército.

Muraviev, A. (2022). Rusia y Ucrania; cuál es la estrategia militar rusa y qué lecciones aprendió el país tras la caída de la URSS y la Guerra de Georgia. https://www.bbc.com/mundo/noticias-internacional-60589483

Pérez, G. (2011). *Investigación Cualitativa: Retos e Interrogantes. Tomo II, Técnicas y Análisis de Datos*. Madrid: La Muralla.

PD3-308 (2014). *Reglamento de "Inteligencia"*. Ejército de Tierra. Madrid: MADOC

Quiñones de la Iglesia, F. (2020). *Una revisión del concepto "Guerra híbrida/actor híbrido".* www.ieee.es:http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO153FRAQUI.guerrahíbrida.pdf.

RDI - 20005. (2015). *RDI - 20005 "Proceso de Integración del Campo de batalla".* Santiago: DIVDOC.

Sullivan, J., & Bauer, A. (2008). *Terrorism Early Warning "10 Years of Achievement in Fighting Terrorism and Crime.* Los Angeles, Califonia: Los Angeles County Sheriffs Department.

Sánchez García, F. (2012). *El Conflicto híbrido ¿Una nueva forma de guerra?* En C. S. Nacional, *El enfoque multidisciplinar en los conflictos híbridos* (págs. 11-23). Madrid: Miniaterior de Defensa.

Schunck, J. (2017). *El Diseño Operacional: Guerra del Líbano". Estrategia*, 11-17.

Anexo Nº 1 – "Pasos de Metodología IPO"

PASOS	ANTECEDENTES
• ***PASO Nº1 "DEFINIR EL ESPACIO DE OPERACIONES"***	En este paso se identifica las Áreas de Interés Nombradas (NAIs), los cuales pueden ser los blancos elegidos por terroristas, los cuales estarán cubiertos por los medios de recopilación de inteligencia y la determinación de la infraestructura crítica en el área. Incluye la evaluación de los factores locales a través de la complementación de la información general, ya que al ser interconectados, los aspectos de infraestructura crítica pueden residir en una escala superior o global o incluso en varios dominios espaciales interrelacionados.
• ***PASO Nº2 "DESCRIBIR LOS EFECTOS EN EL ESPACIO DE OPERACIONES"***	Se analizan las carpetas de información de respuestas (RIFs)[11] de lugares claves, infraestructura, puntos culturales, además de la población, terreno y clima, y las características socioculturales de una zona de operaciones. Para lo anterior, se incluye Inteligencia Cultural (CULTINT), Inteligencia Geoespacial (GEOINT) y Ciberinteligencia (CyberINT), con el propósito de analizar características culturales de la población, el impacto e interacciones de infraestructura, dinámicas organizacionales, explotación de sistemas de información y análisis de redes sociales. El objetivo será comprender todas estas dinámicas que influyen en las operaciones.
• ***PASO Nº3 "EVALUAR FUERZAS ADVERSARIAS, AMENAZA Y ELEMENTOS DE POTENCIAL AMENAZA"***	Este paso se fundamentará en el análisis de las fuerzas adversarias (OPFOR) o elementos de amenazas potenciales (PTE), las posibles armas a emplear diferenciadas por tipología (químicas, biológicas, radiológicas, nucleares, bombas suicidas, etc.), siendo el objetivo principal determinar "indicaciones y advertencias" (I&W)[12] en profundidad, impulsadas por la evaluación de una variedad de antecedentes de las OPFOR.
• ***PASO Nº4 "DETERMINAR POSIBILIDADES E INSUMOS PARA EL DESARROLLO DE COAS"***	El cuarto paso se basa en el análisis y evaluación de los puntos anteriores, con el propósito de desarrollar posibilidades e insumos que contribuyan a desarrollar COAs para contrarrestar las acciones del adversario. Deberá Incluir una comprensión detallada de la

[11] Carpetas de Información de Respuestas (RIF), son referencias completas y específicas de sitios, lugares, puntos, que sirven como ayuda para la toma de decisiones para guiar una respuesta a un NAI específico (HVT o HPT). Así el TEW, utiliza plantillas estandarizadas para el desarrollo de estas RIFs, definiendo campos de información requeridos para completarlas, como es el caso de planos de sitio, análisis del terreno, tendencias meteorológicas, mapas de puntos vulnerables y sitios potenciales para actividades de incidentes, entre otras.

[12] Indicaciones y advertencias (I&W), se define como un proceso riguroso de análisis que incluye información definida de las amenazas, como también de los elementos de posibles amenazas contra un punto, sitios, o lugares de un probable objetivo. El resultado será un conjunto de previsiones de la amenaza, cuyos pronósticos se desglosan en probables indicadores los cuales pueden ser monitoreados por medio de un proceso de análisis y síntesis.

	situación actual de los recursos disponibles, información deficiente, medios de obtención de información y de inteligencia para determinar vacíos e identificar recursos adicionales. Será el paso en donde se difunden los productos de inteligencia finales y completos, como es el caso de carpetas de misión, avisos, alertas, y otros productos específicos.

Anexo Nº 2 – Proceso IPO (Desarrollo modelo de inteligencia)

Paso Nº1 "Definir el Espacio de Operaciones"

Actividad	Descripción	Producto
I - I	Evaluación del Área de Operaciones	Orientación del Espacio de Operaciones
I - II	Identificar Infraestructura Crítica (local – regional - nacional)	Áreas de Interés Designadas (NAIs).

Paso Nº2 "Describir los efectos en el Espacio de Operaciones"

Actividad	Descripción	Producto
II - I	Inventario de objetivos	Contorno de objetivos – Identificación de objetivos potenciales
II - II	Blancos – Modelo de Respuesta	Carpetas de Información de Respuestas (RIFs).
II – III	Identificación de Factores Ambientales	Estudio de Factores Ambientales.
II - IV	Identificación de Efectos Combinados	Evaluación de Factores y Efectos Combinados

Paso Nº3 "Evaluar fuerzas adversarias, amenazas y elementos de potencial amenaza"

Actividad	Descripción	Producto
III - I	Lista de Amenazas	Vectores de Amenazas Complejas y PTE
III - II	Modelos de Amenazas	Estructura de Amenaza y manuales
III – III	Integración de Amenazas (Combinación de Amenazas Complejas)	Escenarios de Amenazas de Alto Impacto (HIT)

Paso Nº4 "Determinar posibilidades"

Actividad	Descripción	Producto
IV - I	Pronóstico de Amenazas	Posibilidades alternativas, hipótesis en competencia.

Anexo Nº3 – Paso Nº1 “Definir el Espacio de Operaciones”

(I – I): Evaluación del Área de Operaciones

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. Definición panorámica del Espacio de Operaciones.	1.1 Orientación básica	Ubicación - posición simbólica - importancia estratégica - organización administrativa local - estadísticas de población - detalle de sectores culturales, económicos y políticos claves.	Orientación del Espacio de Operaciones.
	1.2 Composición del área	Alcance y magnitud – longitud – infraestructura – información geosocial – distribución – centros económicos e industriales – organización y organismos de autoridades jurisdiccionales.	
	1.3 Disposición del área	Sistemas culturales – sistemas económicos e industriales – entradas y salidas críticas – estadísticas de influencia y concurrencia.	
2. Definición de Perspectivas Divergentes.	2.1 Legado, lugar y contexto histórico, desarrollo, aportes, factores de crecimiento.	Visión del Espacio operativo a través de perspectivas alternativas.	
	2.2 atracciones, distinciones, posición simbólica.		
3. Definición de Perspectiva de Sistemas del Espacio de Operaciones.	3.1 Identificación local y global – vínculos y relaciones críticas de entradas y salidas	Características básicas de las dependencias del área local y global. Centro – componente central con múltiples dependencias.	
	3.2 Identificación de impulsores críticos e influencia en el espacio operativo.		
	3.3 Identificación de sistemas culturales.		

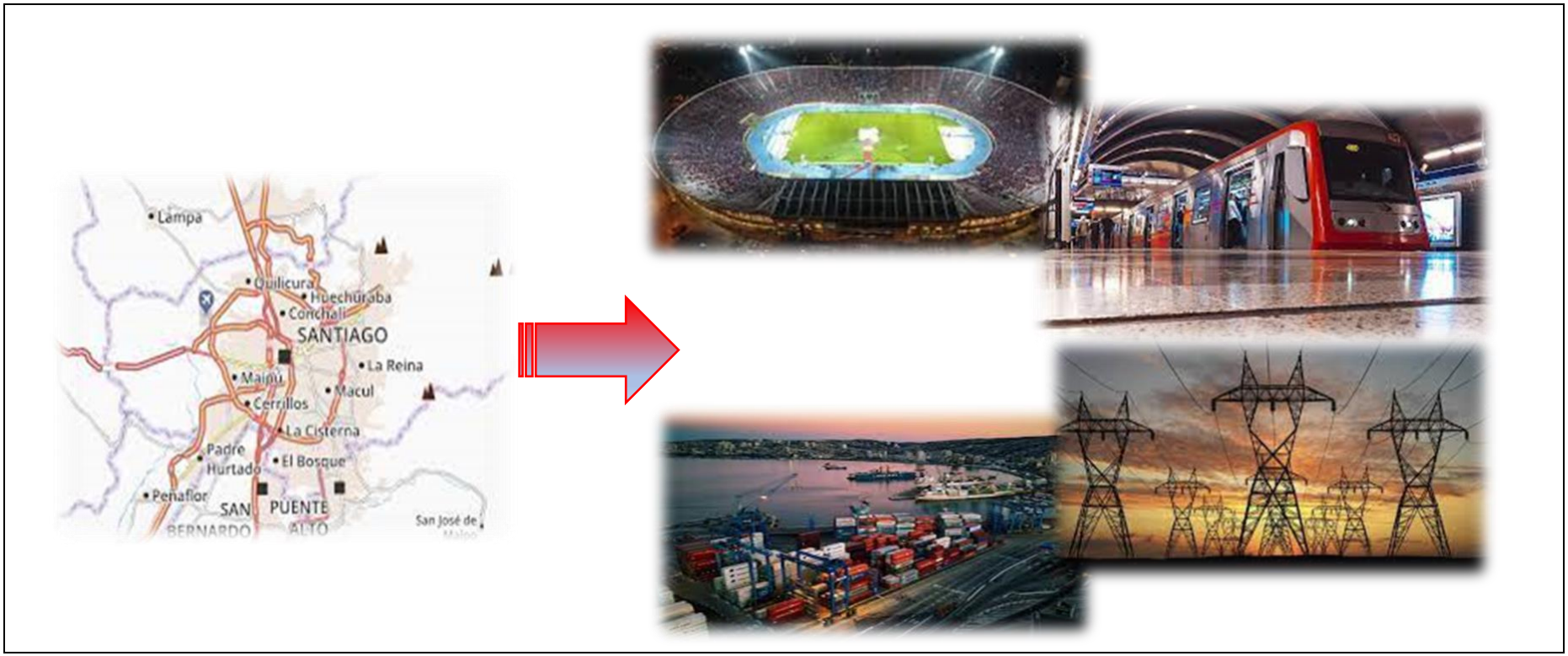
	3.4 Identificación de sistemas y estructuras de infraestructura crítica.		

Resumen	Entrada	Resultados Esperados
Identificar las características que definen el Espacio de Operaciones.	Base de datos, inteligencia básica y actual, últimos eventos, recursos cartográficos, datos demográficos, etc.	Orientación del área o espacio de operaciones.

(I – II): Identificar Infraestructura Crítica

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. Identificar Infraestructura Crítica.	1.1 Instalaciones y Servicios Críticos. 1.2 Vínculos entre Sistemas de Infraestructura nacional, regional, local. 1.3 Lista de IC y Valoración de Criticidad. 1.4 Determinar Prioridad Relativa y orden de clasificación.	**Infraestructura Crítica** Infraestructura que si es atacada, podría producir las consecuencias más graves. Incluye sitios, instalaciones, sistemas, componentes del sistema o eventos especiales, que sin son atacados podría producir: - Gran número de muertos o heridos (eventos y lugares de reunión masiva). - Extensos daños a organismos y servicios básicos y vitales (nodos críticos de blancos). Se identifican los servicios que podrían sufrir los más severos daños, definiendo sitios claves, instalaciones u otras características que componen este servicio. El proceso asigna un valor relativo a cada servicio, simplificando la priorización de la IC. **Áreas de Interés Designadas (NAIs).** Serán sitios geográficos o instalaciones que funcionan como nodos dentro de un sistema de IC, y se usa para definir su perfil físico. También puede ser un sitio o instalación que presta un servicio de IC.	Áreas de Interés Designadas (NAIs)

		Definen las características del sistema de IC y se evalúan con más detalle en el paso Nº2, pudiendo ser identificados como objetivos potenciales. **Bienes y servicios esenciales.** Sectores de IC como la agricultura, alimentación, agua, salud pública, servicios de emergencia, los cuales proveen de bienes a la población para subsistir. **Entrega de bienes y servicios esenciales.** Energía, transporte, servicios financieros, industria química, servicios postales, transporte marítimo, etc., hacen posible el flujo de bienes y servicios esenciales. **Interconexión y operabilidad.** La infraestructura de telecomunicaciones e información, permite la conexión y control del funcionamiento de los sistemas de IC.	



Resumen	Entrada	Resultados Esperados
Durante la evaluación del área de operaciones se definieron los términos de los sistemas críticos. Se identificaron dependencias, conjuntos de sistemas en donde en este sub-paso se deberá identificar la infraestructura crítica. Aquí se definirán las características, determinación de vínculos, definición de puntos críticos, en donde los nodos e instalaciones claves serán designados como NAIs y podrán ser identificados como potenciales objetivos en pasos subsiguientes. Así la infraestructura crítica una vez identificada , será evaluada y priorizada por su relativa criticidad.	Infraestructura crítica jurisdiccional – criterios de priorización y estandarización de puntuación – datos de evaluación del área.	Infraestructura crítica identificada y priorizada - NAIs identificados.

Anexo Nº4 – Paso Nº2 “Describir los efectos en el espacio de operaciones”

(II – I): Inventario de Objetivos.

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. **Identificar eventos de reuniones masivas.**	1.1 Identificar eventos, fechas y lugares como potenciales objetivos de alto valor (HVT).	**Inventario de objetivos.** La IC muchas veces no es en sí, un sitio o evento que puede ser catalogada como blanco u objetivo. Se basa en una serie de componentes de un sistema altamente dependientes, ubicados con dispersión y no solo en un sitio determinado. Los objetivos que busca el adversario, implican la negación, interrupción o destrucción de medios vitales, por lo tanto dirigirán las acciones sobre los nodos críticos del sistema de IC. El proceso de identificación de objetivos, por lo tanto, definirá el entorno del sistema de objetivos e identificará los nodos críticos que podrían ser dañados. Se identifican además, otro conjunto de objetivos potenciales, incluidos eventos de reunión masivas y de valoración simbólica para el adversario. **Infraestructura Crítica (IC) y bienes críticos.** Plantas físicas, sistemas o funciones y recursos humanos, podrán ser bienes esenciales o críticos para la disponibilidad y entrega de servicios vitales. Su destrucción puede tener consecuencias adversas y podrían poner en riesgo la seguridad económica y publica, y por lo tanto podría afectar la calidad de vida de la población. Así, los bienes, sistemas y los procesos asociados que componen la IC son altamente complejos, costosos y sofisticados. Estos bienes estarán formados por bienes y recursos humanos y físicos, sistemas cibernéticos que trabajan en forma interdependiente. También están comprendidos por nodos o bienes críticos, los cuales son esenciales para la operación y funcionamiento de la IC. La destrucción o interrupción de estos bienes críticos podría paralizar el funcionamiento de las estructuras que apoyan.	Contorno de objetivos – Identificación de Potenciales Objetivos
2. **Analizar el comportamiento del sistema de objetivos, a partir de NAIs.**	2.1 Identificar sistemas de IC y definir el sistema ambiental.		
	2.2 Identificar funciones y procesos del sistema.		
3. **Realizar análisis de la conducta de Nodos Críticos**	3.1 Evaluar componentes del sistema y determinar componentes críticos.		
	3.2 Identificación de nodos críticos a HVT.		
4. **Identificar objetivos de interés de OPFOR**	4.1 Identificar sitios o eventos con significancia simbólica como HPT.		

		Sistema de objetivos. El análisis del sistema de objetivos, identifica los sistemas fundamentales de la IC. Este análisis describe las funciones, procesos, y dependencias de cada componentes, nodos e instalaciones de los respectivos sistemas, y prepara el escenario para el análisis de nodos críticos. **Nodos Críticos.** El análisis de los nodos críticos asigna puntajes numéricos a los componentes de un sistema en función de la importancia de cada parte y su dependencia con otros componentes. El esfuerzo estará en identificar los componentes de la columna vertebral, es decir nodos críticos, con los cuales el sistema no podría funcionar. Los nodos críticos de cada sistema cuando se asocian con un sitio físico se identificarán como HVT. **Eventos de Reuniones Masivas.** Eventos especiales programados o no, de alta visibilidad y alta participación, requieren un análisis para su identificación. Los pasos involucran: - Identificar lugares - Revisar el calendario de eventos programados de cada lugar - Determinar qué objetivos específicos dentro del lugar identificado, causarían mayores pérdidas de vidas. Los sitios asociados a potenciales objetivos dentro de esos lugares, se identifican como HVT. **Objetivos de Interés de OPFOR** El adversario puede asignar valores simbólicos a ciertos tipos de instalación por razones particulares. Sitios, eventos, fechas significativas, personalidades que tienen un valor simbólico serán identificados y designados como HPT.	

Resumen	Entrada	Resultados Esperados
Se identifican los objetivos potenciales mediante la identificación de nodos críticos, eventos y lugares de reunión masivas y sitios con valor simbólico. Esta último lista de objetivos potenciales son sitios que no necesariamente tienen alto valor en términos de servicios o sistemas críticos y de letalidad, no obstante igual tienen cierto valor relativo a la vista de un adversario.	Infraestructura crítica – NAIs identificados en Paso Nº1 IPO.	Potenciales objetivos identificados.

(II – II): Modelo de Respuesta de Objetivo.

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. Identificar requisitos de información.	**-.-**	**Carpetas de Información de Respuestas (RIFs)** Una RIF es una referencia completa y especifica de un sitio, que sirve de apoyo en la toma de decisiones para guiar e integrar una respuesta a un NAI específico (HVT o HPT). El TEW utiliza plantillas estandarizadas para el desarrollo de una RIF. Esta plantilla define campos de información requeridos para completarla, incluyendo: - Planos de sitio - Análisis del terreno - Tendencias meteorológicas - Análisis de estallido o explosión - Modelos de elevaciones interiores y exteriores - Mapas indicativos de puntos vulnerables - Sitios potenciales de actividades de incidentes Un componente crítico del RIF es el análisis de consecuencias. Los modelos de consecuencias son desarrollados para apoyar al personal que trabaja en respuesta de emergencias en los recursos de planificación y ejecución. Estos modelos proporcionan una evaluación predictiva de	Carpetas de Información de Respuestas (RIFs)
2. Reunir materiales e información requerida.	**-.-**		
3. Realizar los análisis, y desarrollar los productos de información.	**-.-**		
4. Desarrollar las Carpetas de Información de Respuestas (RIFs)	**-.-**		

		posibles incidentes catastróficos asociados con objetivos vulnerables y son herramientas importantes para desarrollar los planes de mitigación. Durante el proceso de desarrollo de RIF, cualquier vacío o requisitos de información debe ser considerado y entregado al organismo encargado de las tareas de recolección de información. RIFs también conocidos como carpetas de objetivos, son herramientas de conocimiento específicos del sitio del terreno. Son una herramienta específica y completa de referencia para la toma de decisiones en la orientación de respuestas integradas de emergencia a un objetivo específico de alta importancia en una zona determinada. Una carpeta de objetivos podría incluir planos de sitio, análisis del terreno, análisis de daño. Se podrán incluir mapas o gráficos que indiquen puntos vulnerables y sitios potenciales para incidentes. Son componentes de GEOINT para analizar IC, espacios de reunión pública, por lo tanto usarán formatos estandarizados para describir las características de un lugar.	

Resumen	Entrada	Resultados Esperados
Para los potenciales HVT y HPT, se desarrollarán (RIFs) con una serie de información estandarizada.	Terreno, estructuras y otros datos identificados como objetivos potenciales/ NAI y sitios designados como HVT y HPT. Recursos de información de respuesta, acerca de hospitales, la comunidad local, residencias, escuelas y negocios.	Carpetas de Información de Respuestas (RIF) desarrolladas para cada NAI.

(II – III): Identificación de Factores Ambientales

<table>
<tr><th>Sub-pasos</th><th>Actividades asociadas</th><th>Antecedentes</th><th>Producto</th></tr>
<tr><td rowspan="4">1. Realizar análisis del terreno</td><td>1.1 Líneas de comunicación.</td><td rowspan="11">Factores ambientales del espacio operativo
Terreno
El proceso comienza con el análisis del terreno. El estudio se mejora con imágenes aéreas para resaltar los hallazgos analíticos. Los aspectos del terreno incluirán mapas actualizados y una evaluación de las ventajas y limitaciones tanto para la OPFOR como para las fuerzas propias. El enfoque incluye un análisis que proporciona información que podría complementar la RIF en el caso de que hubiera una crisis en uno de los NAI.
Dentro de los factores que se consideran están los siguientes:
• Líneas de comunicación: carreteras – autopistas – avenidas de aproximación – avenidas de infiltración (callejones, túneles, pasajes subterráneos), radio y dimensión del espacio de muerte.
• Terrenos claves o críticos: áreas que proporcionan una ventaja decisiva, puntos de control de acceso, cuellos de botella, puntos de observación, campos de tiro.
• Obstáculos de protección y ocultamiento: estructuras, edificios, zonas industriales.
• Infraestructura de respuesta y emergencia: estaciones de bomberos, policías, zonas de aterrizaje de helicópteros.

Tiempo atmosférico
Se identifican los efectos de los factores meteorológicos, considerando principalmente los patrones estacionales y su influencia en la zonas en estudio.
Dentro de los factores que se consideran están los siguientes:
• Patrones climáticos
• Vientos
• Zonas de peligro, incendios, inundaciones y deslizamientos.

Los aspectos militares del terreno y el tiempo atmosférico resultantes,</td><td rowspan="11">Estudio de Factores Ambientales</td></tr>
<tr><td>1.2 Terrenos claves o críticos.</td></tr>
<tr><td>1.3 Obstáculos, cubierta y protección.</td></tr>
<tr><td>1.4 Infraestructura de respuesta y emergencia.</td></tr>
<tr><td rowspan="3">2. Realizar análisis meteorológico y tiempo atmosférico.</td><td>2.1 Patrones climáticos.</td></tr>
<tr><td>2.2 Vientos.</td></tr>
<tr><td>2.3 Zonas de peligro (incendios, inundaciones, deslizamientos).</td></tr>
<tr><td rowspan="5">3. Evaluación de factores geosociales.</td><td>3.1 Población</td></tr>
<tr><td>3.2 Catastro de Demografía y cultura</td></tr>
<tr><td>3.3 Distribución etérea</td></tr>
<tr><td>3.4 Factores políticos</td></tr>
<tr><td>3.5 Factores sociales</td></tr>
<tr><td></td><td>3.5 Características generales de la comunidad.</td></tr>
</table>

	3.6 Educación, ingresos y economía.	incluirán mapas y una evaluación de las oportunidades y limitaciones, tanto para las fuerzas amigas como para las actividades del adversario y posibles amenazas. **Factores Geosociales** Consiste en identificar las características demográficas y culturales que abarcan o influyen estratégicamente en cualquier NAI. El análisis demográfico y cultural incluye la recopilación de datos e información actualizada, por medio de censos, programas de policía comunitaria u otras agencias gubernamentales apropiadas para identificar y comprender los aspectos más críticos del ambiente, el cual son las personas. Se buscará alcanzar predisposiciones culturales desde varias perspectivas en el área de operaciones. Esta fotografía incluirá entre otros estudios: - Número de población - Distribución de edades - Grupos por ingresos - Factores socioeconómicos - Datos culturales - Estadísticas delictuales. Otra información relevante de la situación Geosocial, será la calendarización de eventos significativos, identificando fechas importantes, celebraciones, conmemoraciones, aniversarios, aspectos importantes de cada comunidad. Eventos especiales se calendarizan y se darán por la concurrencia de visitas de funcionarios gubernamentales, representantes y dignatarios extranjeros y otras personalidades de alta importancia. Esta calendarización también contiene fechas significativas que podrían tener adjuntos ciertos simbolismos considerados provocativos para determinados sectores de la población. Finalmente, también incluyen fechas simbólicas y todos los aspectos del medio ambiente que sigue un cronograma regular, ejemplo (ciertas enfermedades). Las características culturales incluirán el desarrollo de la CULTINT, considerando además los factores teológicos en los análisis. Será	
4. Influencias locales y globales	4.1 Asuntos de interés nacionales y extranjeros.		
	4.2 Sector económico		
	4.3 Sector industrial		
	4.4 Entretenimiento		
5. Evaluar presencias o influencias cibernéticas.	-.-		
6. Examinar aspecto teológico, sistemas de creencias y fundamentos de los sistemas de fe.	-.-		
7. Identificar otros factores de influencia.	-.-		

		complementado por su parte por Cyberinteligencia, explotando sistemas avanzados de información y redes sociales. Finalmente, el objetivo será una comprensión de todas las dinámicas geoespaciales y sociales, incluidos aspectos sicológicos que influyen en las operaciones, siendo la combinación de lo anterior (Inteligencia Geosocial). **Conexiones locales y globales** Las condiciones ambientales que aparentemente solo impactarían en zonas remotas del mundo pueden convertirse instantáneamente en un elemento impulsor e influyente de las condiciones locales a medida que los problemas que enfrentan las comunidades extranjeras se manifiestan en las actitudes y disposiciones de ellas en una zona local. El estudio demográfico de una zona, se utiliza para identificar sectores de extranjeros. Se evalúan sectores y el origen de extranjeros y sus países de origen, identificando posibles problemas. La evaluación proporciona una herramienta para identificar comunidades donde las simpatías, los agravios o las alianzas con raíces en el país de origen, todavía están en juego o controversia. La evaluación de la influencia global y local continúa en tantos sectores y subsectores como sea posible, incluidos los sectores económicos, religiosos, políticos y sociales para obtener una lectura razonable de las influencias globales que afectan una zona en particular.	

Resumen	Entrada	Resultados Esperados
Describir las variables y aspectos ambientales dentro del espacio operativo y determinar la forma en cómo estas condiciones afectan a las operaciones de las propias fuerzas y del adversario.	Evaluación material del área, incluyendo datos de IC. Información de las RIFs y datos adicionales del ambiente, considerando terreno, tiempo atmosférico, datos demográficos, frecuencia de eventos y actividades locales y próximos a los NAI.	Evaluación del espacio operativo, identificando las características y los efectos ambientales claves. Evaluación de los efectos producidos de los factores combinados.

(II – IV): Identificar Efectos de Factores Combinados

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. **Recolección previa del desarrollo de los productos de los factores ambientales.**	**-.-**	**Factores y efectos** Las influencias ambientales tienen un efecto significativo en cómo los eventos se desarrollan en el espacio de operaciones. Los factores de los objetivos y la amenaza e incluso los factores que afectan a las respuestas de las propias fuerzas están sujetos a las influencias y efectos de la circunstancias del medio ambiente. Los estudios de factores ambientales realizados en actividades anteriores, se combinan para evaluar la dinámica de las influencias y determinar qué oportunidades o limitaciones, pueden resultar al combinar esos factores. Cuando es posible, se identifican patrones o ciclos regulares para facilitar los pronósticos. La evaluación busca analizar como las condiciones cambiantes se combinan para influir en el carácter del espacio de operaciones, ejemplo de lo anterior, como ciertas vulnerabilidades en un sitio son afectados por un objetivo potencial, producto de un ataque terrorista, considerando el tiempo, la selección de armas, blancos, etc. y como se ven afectadas las capacidades de las propias fuerzas. Las influencias típicas incluyen eventos políticos, actitudes sociales, fechas especiales, clima, estaciones, eventos globales y problemas geosociales y sus influencias. La evaluación produce un panorama de factores combinados, que equivale a una muestra actualizada de cómo los factores y efectos del ambiente, en forma integrada y relacionados con la amenaza pueden alterar ciertos NAI. Esta muestra instantánea del panorama es revisada y actualizada en forma regular, permitiendo con lo anterior tomar mayores medidas de vigilancia y atención a un NAI afectado. **Factores combinados y efectos en el riesgo.** Los factores de riesgo estarán influenciados por las condiciones ambientales que regularmente actuarán sobre ellos. Así por ejemplo, las densidades de población podrán cambiar drásticamente en el trascurso	Evaluación de los efectos de factores combinados.
2. **Evaluar cada factor en forma independiente e identificar patrones, frecuencias y ciclos.**	**-.-**		
3. **Combinar todos los factores y patrones usando una matriz, superponiendo los patrones de efectos uno sobre otro, extendiéndolo por medio de un ciclo de 12 meses.**	3.1 Evaluar la matriz de factores combinados e identificar alineamientos de alto riesgo. 3.2 Registrar ventanas de oportunidad. 3.3 Refinar y validar la matriz con regularidad.		
4. **Desarrollar pronósticos de alineamientos de alto riesgo para los próximos tres meses, empleando la matriz.**	**-.-**		
5. **Monitorear pronósticos, validar o refinar la matriz.**	**-.-**		

		del día, semana o mes, en concordancia con ciertos eventos especiales. Entonces la letalidad de un ataque por lo tanto repercutirá de diferente manera si es que se produce bajo una aglomeración masiva de población en un determinado lugar. La relación entre el terreno y los factores climáticos también pueden condicionar la situación en forma dramática. De esta manera una amenaza al comprender los efectos de factores ambientales, podrá maximizar los daños al perpetrar un ataque sobre un blanco determinado, con el sólo hecho de seleccionar el momento y las condiciones adecuadas para una acción ofensiva. Así, cuando los factores ambientales ofrecen condiciones óptimas para lograr efectos maximizados o amplificados existirá una "ventana a de oportunidad" para un ataque. Existirán condiciones ventajosas que podrán amplificar los efectos de un ataque en un sitio, lugar, zona específica.	

Resumen	Entrada	Resultados Esperados
Identificar las influencias del ambiente sobre las actividades de fuerzas enemigas como en las propias, así como aquellas condiciones que afectan los NAI. Identificar aquellos problemas económicos, políticos o sociales existentes, condiciones de inestabilidad, debilidad, fricción o crisis, que el adversario podría explotar como parte de un ataque a un objetivo físico.	Antecedentes e información de evaluación del área incluyendo datos de IC. RIF y todos los estudios y análisis de factores del ambiente realizados en forma previa.	Patrones de efectos combinados y estudio de regularidad y frecuencia de factores significativos del ambiente.

Anexo Nº5 – Paso Nº3 “Evaluar fuerzas adversarias, amenazas y elementos de potenciales de amenaza”

(III – I): Lista de Amenazas

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. Identificar grupos o actores conocidos.	**-.-**	**Lista de amenazas** El propósito de la lista de amenazas, es reevaluar rutinariamente las amenazas y OPFOR dentro del área de operaciones. El TEW identifica grupos o actores dentro de una región que podrían llegar a constituirse como posibles amenazas. Se incluirán actores conocidos vinculados a asociaciones u organismos terroristas, agrupaciones locales, individuos con ideologías de interés especial u organismos criminales. La lista de amenazas responderá las siguientes preguntas: ¿Quiénes son las personas involucradas?, ¿Cuál es la afiliación grupal, si existiera, y en que creen?. También identificará los motivos, métodos y objetivos. Así por ejemplo en organismos delictivos o criminales las variables a analizar serán los métodos, objetivos, financiamiento y lugares de empleo y de interés. Se buscará entender como la entidad criminal opera, lo que busca, en definitiva, proporcionará una visión significativa de su capacidad de accionar. La lista de amenazas TEW, permitirá identificar (PTE) en el área local. El proceso se esforzará en identificar grupos o individuos cuyas asociaciones extremistas, radicales o de otro tipo, ensalzados por el odio y violencia, quedan bajo sospecha, o se conoce que podrían actuar en un futuro. Un programa activo de lista de amenazas, junto con un proceso de análisis de transacciones I&W, será necesario para reducir las probabilidades de que elementos desconocidos emerjan y lleven a cabo acciones ofensivas con cualquier capacidad o apoyo a otras entidades.	Identificación de elementos de potenciales amenazas (PTE).
2. Identificar densidades de población a través del continuo de interés relativo, para identificar probables variaciones en la densidad de la amenazas.	**-.-**		
3. Evaluar actividades globales de OPFOR en relación a las actividades locales de una amenaza como parte del Proceso de Análisis de Transacciones.	**-.-**		
4. Identificar posibles vectores complejos de la amenaza.	**-.-**		

		Así una sofisticada lista de amenazas, da como resultado un mapa de relaciones de redes de PTE, indicando zonas jurisdiccionales, conexiones, y transacciones de posibles amenazas en el área de operaciones y su vinculación con un contexto más amplio o global. Será crítico que el esfuerzo de inteligencia continúe buscando una mejor comprensión de las relaciones globales y locales de los actores que pueden constituirse como posibles amenazas, y como repercuten en forma recíproca. **Identificación de vectores complejos de la amenaza.** TEW reconoce que existen diferentes tipos de amenazas y ataques terroristas que involucran procesos con características altamente complejas, dinámicas y múltiples técnicas que pueden implicar un alto índice de consecuencias catastróficas. Así, la lista de amenazas por lo tanto, identificará posibilidades del adversario de una forma diversa, como el despliegue de armas químicas, biológicas, radiológicas, nucleares, de destrucción masiva (WDM) y otras de alta letalidad, denominándose vectores de amenazas complejas.	

Resumen	Entrada	Resultados Esperados
Evaluar el espacio de operaciones y determinar los elementos de la amenaza local.	Estudio de los factores ambientales , bases de datos criminales y delictuales e inteligencia actual.	Lista de amenazas y su constante mejoramiento y actualización.

(III – II): Modelo de Amenazas

<table>
<tr><th>Sub-pasos</th><th>Actividades asociadas</th><th>Antecedentes</th><th>Producto</th></tr>
<tr><td>1. Desarrollar archivos OOB de OPFOR.</td><td>-.-</td><td rowspan="7">Modelo de amenaza
Busca reducir la incertidumbre en la respuesta de las primeras tres respuestas específicas de la amenaza.
1. Fines: ¿Cuáles son las intenciones del adversario?
• Intenciones
2. Formas o modos: ¿Cómo el adversario ha conducido sus operaciones con anterioridad?
• TTP demostradas.
3. Medios: ¿Qué puede hacer el adversario?
• Recursos y capacidades
4. ¿Qué hará o podrá hacer el adversario?
• Hipótesis de COA de la amenaza.

Los componentes de análisis de fines, formas y medios del modelo de amenaza, son empleados para describir el proceso de planificación, movilización, y actividades ofensivas del adversario del proceso de cadena de destrucción. Esto facilitará a los equipos de planificación propio (Red Team), generar hipótesis de ECOAs, generando las condiciones de responder la cuarta y última respuesta.

Las actividades del adversario y otras dinámicas reconocidas en la cadena de destrucción, serán reconocidas como precursores de ataques y luego serán identificadas como indicadores. Los indicadores son localizados dentro del ECOA, y son empleados como parte de la función de inteligencia para I&W en anticipar una situación en desarrollo de la amenaza.
La evaluación de OOB y fines, formas y medios, de los modelos de amenazas e hipótesis de ECOA, se actualizan regularmente en conjunto con el desarrollo de la situación del adversario.</td><td rowspan="7">Marco de amenazas</td></tr>
<tr><td>2. Realizar evaluación de fines.</td><td>-.-</td></tr>
<tr><td>3. Realizar evaluación de modos de empleo.</td><td>3.1 Estructura o marco de amenazas y cadena de destrucción.</td></tr>
<tr><td rowspan="3">4. Realizar evaluación de medios.</td><td>4.1 Capacidades</td></tr>
<tr><td>4.2 Vulnerabilidades Críticas</td></tr>
<tr><td>4.3 Centro de Gravedad</td></tr>
<tr><td>5. Desarrollar perfiles e integración de amenazas y objetivos.</td><td>-.-</td></tr>
<tr><td>6. Desarrollo de opciones.</td><td>-.-</td></tr>
</table>

		Análisis del Orden de Batalla (OOB) Será la herramienta principal para caracterizar una amenaza. Será un desglose de factores claves que describen la composición de cualquier fuerza de combate. Incluso interconectadas, transnacionales y no convencionales, como las organizaciones terroristas. Será una metodología para catalogar los principales atributos de combate de un adversario y establecer la comprensión el tipo de guerra que desea pelear. Determina en como estos atributos contribuyen o disminuyen la eficacia de combate de una fuerza. Ayuda a definir las capacidades, fortalezas y otras ventajas de un adversario, mientras que al mismo tiempo expone sus vulnerabilidades, debilidades y desventajas. **Factores OBB** - **Composición:** identificación – organización de unidades, grupos políticos, religiosos, étnicos. La identificación consistirá en la designación completa de una entidad específica (nombre o número, tipo, tamaño o fuerza relativa y subordinación). - **Disposición:** ubicación geográfica de los elementos de la OPFOR, despliegue, situación de empleo, movimientos o ubicaciones recientes, actuales y futuras. - **Fuerza:** personal, armas y equipamiento. Equipos de ataque, cuadros o células políticas, apoyo popular (simpatizantes, apoyo de sostenimiento, traslado, ocultación de información). - **Táctica:** estrategia, procedimientos y doctrina. Pueden implicar consideraciones políticas, militares, sicológicas y económicas. Las tácticas varían en sofisticación según la formación individual y organizacional. La OPFOR, planifica operaciones individuales y en pequeños grupos. - **Entrenamiento:** Ligada a las tácticas y procedimientos. - **Logística:** Condicionará la eficacia de la OPFOR. La dependencia será horizontal y vertical entre los grupos y niveles de operación. - **Eficiencia de Combate:** Condicionado por la motivación, adhesión	

		popular, miedo, intimidación, y cambios de poder político. - **Personalidades:** Concentración en las personas y líderes. Los diagramas organizacionales se pueden construir por medio del análisis de vínculos de las personalidades claves y sus grupos y asociaciones. Con lo anterior, se pueden generar las condiciones para determinar posibles actividades. - **Cultura:** ideologías, usos, costumbres, patrones de pensamiento, comportamiento. Problemas culturales, étnicos, religiosos, creencias políticas, económicas, tribus, clanes, actitudes militares, ley y justicia. - **Datos misceláneos:** información necesaria de respaldo, pero no cubierta por los factores anteriores. **Evaluación de fines, modos y medios** Los factores de OOB se utilizan para organizar la información sobre las amenazas y construir una base de conocimiento sobre ellas. Una vez obtenida la información, se analiza con mayor detalle para concluir que tan bien se alinean las capacidades con las intenciones. Lo anterior, se define como evaluación de fines, modos y medios y busca identificar las intenciones, los métodos, las capacidades y recursos de la OPFOR. **1) Evaluación de fines - ¿Qué quiere hacer el adversario?** Implica una evaluación de las metas estratégicas, operativas y tácticas del adversario, para luego determinar en cómo esas metas u objetivos se relacionan con la ejecución de acciones pasadas. **2) Evaluación de formas o métodos - ¿Cómo el adversario ha conducido sus operaciones con anterioridad?** Describe los métodos que utiliza o ha utilizado el adversario para lograr su estado final deseado (fases, tareas, y actividades si corresponde). Acciones anteriores realizadas por grupos conocidos, permiten la oportunidad de comprender de cómo esos grupos de factores de OOB, son empleados durante una operación para examinar la organización,	

		reclutamiento, equipamiento, entrenamiento, y despliegue para un ataque. Esta evaluación, por lo tanto, revisa acciones pasadas catalogando procesos, métodos, sincronización y secuencia, patrones, selección de objetivos, preferencias de armas, relaciones organizacionales, patrocinadores, entre otras concernientes a las actividades que componen la cadena de destrucción del adversario. Será de vital importancia el lugar o zonas de objetivos y la selección de armas, evaluando los atributos de los blancos, impacto, tiempo y efectos en él, determinando si se lograron las intenciones del adversario. • **Marco de amenazas** La información desarrollada por esta evaluación se utiliza para generar una mayor profundidad para la comprensión del marco operacional del adversario. El marco de las amenazas describen los elementos de la cadena de destrucción. En efecto, un producto primario que se desarrolla aquí, es una ilustración gráfica que representa la cadena de destrucción por medio de un diagrama de flujo a lo largo de una línea de tiempo. El marco de amenazas se utiliza para recopilar y compilar patrones de comportamiento y puntos de aprendizaje identificados y descubiertos de manera posterior a acciones previas. El marco es una herramienta destinada a describir como el OOB está organizado en tiempo y espacio, coordinado y apoyado para surgir en un momento adecuado. Se mejoran con el tiempo y son registros que permiten evaluar a la amenaza y se mantienen en evolución. Los siguientes factores representan un conjunto de tópicos que componen un marco de amenazas: **Organización** Selección de armamento – selección de objetivos – ataques. **Fines** Designación – objetivos – organización táctica – evaluación. **Modos** Condiciones – operaciones – desarrollo.	

		Medios Distribución – efectos – mando y control – BDA. El desarrollo del proceso implica investigar y analizar sobre acontecimientos pasados, identificando sobre cada uno de sus componentes, buscando continuidad, tendencias, patrones entre los ataques. **Modelo de Cadena de destrucción.** Describe los preparativos y la secuencia de actividades de la amenaza empleada para planificar, organizar, movilizar, entrenar, equipar y poner en ejecución los recursos en las operaciones. Estas evaluaciones comprenden el "Modus Operandis" del sistema de ataque de la amenaza. Además los modelos de cadena de destrucción se utilizan para identificar los recursos, capacidades, vulnerabilidades críticas y el centro de gravedad de cada adversario. **3) Evaluación de medios - ¿Qué puede hacer el adversario?** Se identificarán los recursos y las capacidades críticas que necesita la OPFOR para llevar a cabo las operaciones descritas en la cadena de destrucción. También se identificará el centro de gravedad y las vulnerabilidades críticas. Esta evaluación identificará lo que realmente es capaz de hacer el adversario, identificando la combinación de las capacidades esenciales y los recursos a disposición. Esto incluye identificar las capacidades claves esenciales para el éxito de la operación: 1. Que se ha demostrado en forma previa 2. Cuales han surgido en forma actual. La evaluación revisa el modelo de la cadena de destrucción y examina las capacidades demostradas en episodios pasados, señalando qué recursos se han incorporado para habilitar la capacidad esencial. Además identifica capacidades recientes o la intención de adquisición de capacidades.	

		Entonces, las capacidades y recursos claves, definen el rango de opciones para llevar a cabo el curso de acción del adversario, es decir ¿Qué hará?. Las actividades inherentes a la capacidades esenciales normalmente se seleccionan como indicadores y se utilizan como herramientas claves para anticipar las acciones de la amenaza y ataques terroristas. La evaluación de los medios también proporciona información clave sobre los fundamentos de la capacidad operativa que puede ser útil para las estrategia de interdicción. La disponibilidad de capacidades y recursos esenciales, se examinan durante el análisis de la vulnerabilidades críticas y el análisis del centro de gravedad. La evaluación de medios involucra una revisión de los materiales generados a través de las evaluaciones de fines y modos, incluyendo los modelos de amenazas y los modelos de cadena de destrucción, para aislar y caracterizar las capacidades esenciales y los recursos necesarios. La siguiente lista de capacidades estándares para una acción militar, proporciona una guía de inicio para comenzar la evaluación: 1) Administración de personal - reclutamiento, capacidad de inserción y extracción de personas u organismos transfronterizos, documentación, equipo, armamento, dirección e instrucción, sostenimiento, ocultamiento. 2) Focalización – evaluación de blancos, selección de blancos, desarrollo de objetivos, reconocimiento y vigilancia y despliegue. 3) Manejo de armas, calibre, adquisición de armas (comprar, robar, tomar prestadas) o material para diseñar, desarrollar y entregar un arma que funcione), movimiento y almacenamiento de armas e (innovaciones destacadas). 4) Mando y control, planificación, organización de tareas, comunicaciones operaciones coordinadas, operaciones de inteligencia y OPSEC, engaño e información. 5) Logística, financiamiento, movimiento de elementos, investigaciones, compra de elementos.	

		Las capacidades esenciales pueden ser evaluadas de diferente maneras, pero como referencia la metodología incluirá la identificación y descripción de los siguientes elementos dentro de cada capacidad. • Personal, conocimiento y habilidades especiales. • Tácticas, técnicas, procedimientos definidos y adoptados. • Estructura y organización. • Equipamiento. • Instalaciones. • Tecnología. • Materiales. • Soporte. Nota: Cuando sea posible, identificar redes culturales y sistemas de apoyo dentro de los elementos de apoyo. **Centro de Gravedad y Vulnerabilidades Críticas.** Será la fuente de fuerza, poder o resistencia moral o física que es fundamental para la capacidad de la OPFOR para ejecutar sus operaciones. Las vulnerabilidades críticas son componentes del sistema operativo de la amenaza – cadena de destrucción, que son cruciales para el funcionamiento del sistema y vulnerables a la explotación. En forma posterior a la evaluación de las capacidades esenciales y la evaluación de medios, se realiza una fotografía total del adversario, el OOB, Fines, modos y medios, y se define el centro de gravedad y las vulnerabilidades críticas. **Emparejamiento de Amenaza - Objetivo:** Cada amenaza, PTE y grupo terrorista es evaluado para establecer un perfil de amenaza-objetivo, que se utiliza para emparejar objetivos con los intereses conocidos de la OPFOR. Cuando se identifican esta relación entre amenaza-objetivo, se dice que existe un “Carril de Ataque” entre ambos. La información desarrollada durante los procesos de evaluación de objetivos y gestión de amenazas proporciona las herramientas necesarias para	

		desarrollar perfiles de amenazas - objetivos, identificar las relaciones de amenazas - objetivos y realizar la evaluación de riesgos. **Carril de Ataque:** Describe la relación única entre un elemento de la amenaza y un objetivo en particular. Proporciona una imagen verbal para ver los objetivos en un extremo de un corredor de movilidad con una fuerza adversaria preparada en el otro extremo. Las clasificaciones de movilidad para carriles de ataque proporcionan criterios básicos para identificar las prioridades de relación entre amenazas y objetivos. Una amenaza con deficiencias de capacidades con respecto a un sitio específico de un objetivo, no es capaz de progresar a lo largo de un posible vía de aproximación. **Condiciones de Carril de Ataque:** Las características hipotéticas de movilidad dentro del carril de ataque, están determinadas por las condiciones de acuerdo de factor amenaza – objetivo. Por ejemplo: 1. **Condición de Avance:** Cuando los factores de la amenaza – objetivo, están sincronizados y las condiciones ambientales tienen un ciclo para crear una ventana de oportunidad, entonces existe una condición de “avance” dentro de ese carril de ataque. 2. **Condición de Avance Lento:** Cuando los factores de la amenaza – objetivo, están sincronizados, pero los factores ambientales no se presentan en forma óptima y por lo tanto, no existe una ventana de oportunidad. Entonces existe una condición de avance lento dentro del carril de ataque. 3. **Condición de No Seguir:** Cuando los factores de la amenaza – objetivo no están alineados, independiente de los factores ambientales o las ventanas de oportunidad. Existirá un “no seguir” dentro de la línea de ataque. **Vectores complejos de amenazas** El modelo de amenazas también examina los vectores complejos de	

		amenazas identificados de la lista de amenazas, catalogando el rango CBRNE de potenciales amenazas, revisando específicamente las características de cada sistema de arma, identificando materiales percusores, equipos especializados y requisitos de instalación, además de la experiencia necesaria para investigar, diseñar, desarrollar, almacenar y transportar los diversos componentes de las armas. Los componentes de los materiales y aparatos especiales que producen una única señal detectable también se identifican. Los vectores complejos de amenazas también incluyen amenazas emergentes, innovadoras, difíciles de detectar y escenarios de amenaza altamente peligrosas, que requieren análisis adicionales para un completo desarrollo de prevención y estrategias de respuesta. Prevenir, disuadir o responder a estas complejas amenazas, requiere del apoyo de detallados protocolos de referencia que guíen al TEW, por medio de fundamentos técnicos de reconocimiento de amenazas, prioridades de alerta de agencias claves, definir las estrategias y recursos de mitigación, apoyo a la célula OIC en la determinación de la asignación de tareas internas del personal. En definitiva, la toma de decisiones inherente a situaciones que involucran éstas clases especiales de amenazas, es más eficaz cuando se guían antes de una crisis por un desarrollo de referencias organizadas y en un entorno de planificación deliberada. **Archivos de Registro** El TEW, utiliza productos de referencia llamados archivos de registro para proporcionar una orientación general previa, en la evaluación de situaciones de amenazas complejas. Será una guía analítica interna. Están organizados en formatos estándar para realizar evaluaciones de la amenaza o ataques terroristas reales. Guían las actividades de evaluación del TEW antes, durante y después de un ataque. Identifican consideraciones comunes y requisitos típicos de inteligencia que probablemente necesiten los encargados de la toma de decisiones. El TEW ha desarrollado guías	

		para el terrorismo químico, biológico, garantía alimenticia y de suministro de agua, atentados suicidas, coches bomba, armas de radiofrecuencia y el terrorismo radiológico – nuclear, entre otros.	

Resumen	Entrada	Resultados Esperados
El proceso de modelo de amenazas involucra el desarrollo y análisis de los datos del Orden de batalla (OOB) de la amenaza, para realizar un análisis de los fines, modos y medios.	Lista de objetivos, lista de amenazas, recursos de obtención y análisis de inteligencia.	Base de datos de la amenaza, archivos OOB, estructura de amenazas, antecedentes de amenazas – objetivos, manuales.

(III – III): Integración de Amenazas

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. Identificar relación (amenaza – objetivo) de la amenaza.	**-.-**	**Integración de amenazas** Evalúa potenciales disposiciones de combinaciones de amenazas. El esfuerzo comienza identificando el rango de combinaciones de amenazas potenciales (ejes de amenazas), posiblemente vectores complejos de una o más amenazas, una preferencia de objetivos y las condiciones óptimas del ambiente que represente el mayor impacto catastrófico del área. Estas alineaciones de amenazas son consideradas en los escenarios de amenaza de mayor impacto	Eje combinado de amenazas complejas – Escenarios HIT.
2. Identificar los objetivos más adecuados para maximizar los efectos de amenazas complejas (letalidad, destrucción, disrupción e impacto).	**-.-**		

3. Identificar vectores complejos de amenazas - objetivos con respecto a relación de amenazas - objetivos.	**-.-**	(HIT). Los escenarios HIT, luego se llevan adelante en el proceso de pronóstico de amenazas. Cada eje de amenaza compleja combinada, representa un escenario de amenaza de alto impacto (HIT).	
4. Correlacionar vectores complejos de amenazas con la OPFOR, blancos y condiciones e identificar las posibles combinaciones.	4.1 Basado en condiciones y objetivos similares.		
	4.2 Basado en objetivos similares.		
	4.3 Basado en condiciones similares.		

Resumen	**Entrada**	**Resultados Esperados**
Disposición combinada de amenazas complejas – Eje único de amenazas identificado.	Modelo de amenazas - relación de amenaza/objetivo – evaluación de efectos combinados – archivos de registro.	Escenarios de Amenazas de Alto Impacto.

Anexo Nº6 – Paso Nº4 “Determinar Posibilidades”

(IV – I): Pronóstico de Amenazas

Sub-pasos	Actividades asociadas	Antecedentes	Producto
1. Evaluar las capacidades de la OPFOR. Identificando todas las opciones de COA dentro de los escenarios HIT.	**-.-**	**Pronóstico de amenazas** **Hipótesis de COA de la amenaza - ¿Qué hará la OPFOR?** De los escenarios HIT, el esfuerzo en el pronóstico de amenazas estará dado en el seguimiento de opciones reales. Un escenario se constituye como opción, cuando la OPFOR tiene la capacidad para ensamblar el eje de amenazas y ejecutar el ataque. Las combinaciones que se consideren más peligrosas serán identificadas como opciones del COA más peligroso del adversario. El resultado será la identificación del curso de acción más probable (ML) o más peligroso (MD). El resultado del pronóstico de la amenaza estará sustentada en las siguientes combinaciones de ejes de amenazas. 1. Escenarios de amenazas de mayor impacto (HIT) 2. Opciones de COA (MD) “Más peligroso” 3. Opciones de COA (ML) “Más probable” Estas combinaciones de ejes de amenazas se convierten en la base para las tareas posteriores, como la evaluación del riesgo, el desarrollo del marco I&W “Indicadores y advertencias”. Además, las opciones de COA MD y ML, se pueden refinar aún más, a través de la formación de Red Teams para comenzar a formular hipótesis que describan varios tipos de cadenas potenciales de destrucción. Nota: Evaluación del potencial impacto y letalidad de cada opción, ayuda a determinar las condiciones más peligrosas (MD), mientras que también ayuda a determinar una opción de COA más probable (ML).	Hipótesis del Curso de acción de la amenaza (ECOA)
2. Identificar basado en la inteligencia disponible, cuál de las opciones de COA es más probable y más peligroso.	**-.-**		

		La actividad central del pronóstico de amenazas implica formular hipótesis de opciones sobre el curso de acción del adversario. Estas hipótesis de COAs, se utilizan como base para desarrollar situaciones específicas de los modelos de cadenas de destrucción, representando gráficamente las acciones de la amenaza, como es el caso de la planificación, el objetivo, evaluación y selección, desarrollo de armas, reclutamiento y operaciones tácticas a lo largo de una línea de tiempo hipotética. Cuando está completo, el modelo de la cadena de destrucción es esencialmente una herramienta gráfica de pronóstico, una herramienta de mapeo de indicadores y un marco de referencia durante la fusión de información de todas las fuentes/todas las fases. Cuando se compilan los modelos de destrucción, el resultado es un conjunto integral de planes de ataques que incluyen ramas y secuelas. La evaluación produce diagramas gráficos de ataques para ilustrar como se vería la cadena de destrucción, si sus partes y componentes se estuvieran moviendo a través del carril de ataque. Esta técnica permite a los analistas visualizar posibles acciones de tiempo y secuencia. Los modelos gráficos no deben ser confundidos con una “verdad fundamental”, pero es una herramienta analítica que ayuda a los analistas a reconocer patrones y relaciones entre las actividades. Estos gráficos se denominan “plantillas de situación”. Una plantilla de situación normalmente representa una evaluación que involucra una OPFOR contra un objetivo en una sola cadena de destrucción a lo largo de un carril (vía) de ataque. Sin embargo, durante la evaluación, un Red Team, puede usarla para identificar puntos decisivos en la secuencia de la cadena, donde las opciones de ramificación y secuelas se desarrollarán y se identificarán aquellos puntos o eventos, en los el ataque de un adversario, puede pasar a otra línea de ataque contra un objetivo	

		diferente. El Red Team también puede identificar puntos decisivos en la secuencia de cadena de destrucción, en donde la OPFOR emplearía opciones de engaño o donde ha pasado al punto de no retorno. El desarrollo de la cadena de destrucción no sugiere que una OPFOR no se capaz de atacar a lo largo de varios carriles a la vez, contra varios objetivos con una sola cadena de muerte (ataque). La técnica utiliza un enfoque simple de uno a uno para aislar e identificar cualquier indicador potencial único. El enfoque uno a uno, también permite que el equipo rojo determine las condiciones ambientales que serían óptimas para mejorar los efectos del ataque y amplificar el impacto. Cuando se presentan estas condiciones en forma suficiente, existirá una ventana de oportunidad abierta para un ataque. Debido a esto, el esfuerzo de I&W, se orientará en rastrear indicios de que podría estar surgiendo una ventana de oportunidad. El objetivo es tener un conjunto de modelos de cadenas de destrucción para cada opción de COA, ya sea (MD) o (ML), así como para cada uno de los escenarios HIT restantes, iluminando la gama de factores que tendrían que unirse para que cualquiera de estos ejes combinados de amenazas emerjan dentro de un carril de ataque. Teniendo esto en cuenta, el Red Team incorpora técnicas de juego en el proceso de desarrollo de COA que involucren viñetas de escenarios que exploran las posibilidades de interacción entre el cuadro OPFOR y el PTE local. Estas técnicas ayudan a proporcionar un marco de referencia para evaluar las actividades locales. **Red Team** El trabajo implica examinar desde la perspectiva del adversario. Las actividades se utilizan para evaluar las medidas de seguridad física y de información. En estas situaciones, el Red Team lleva a cabo operaciones reales contra una instalación con el fin de	

		descubrir brechas de seguridad u otras vulnerabilidades. Estos equipos también son útiles durante los ejercicios para proporcionar las condiciones de un adversario pensante e intrigante que pueda interactuar dinámicamente con los participantes del ejercicio Este equipo analítico en apoyo a las tareas de inteligencia, involucra a un equipo de analistas que desarrollan planes de ataque y elaboración de pronósticos desde la perspectiva de la OPFOR. Este enfoque utiliza técnicas de juego de roles para comprender los matices, comprender las complejidades y tener una idea de dónde puede estar una OPFOR y ser vulnerable a ser expuesto mientras realiza acciones hostiles	

Resumen	Entrada	Resultados Esperados
El pronóstico de amenazas utiliza información desarrollada durante la lista de amenazas, modelo de amenazas y evaluaciones de integración de amenazas para desarrollar hipótesis con respecto de los cursos de acción de la OPFOR.	Lista de amenazas – modelo de amenazas – integración de amenazas - escenarios HIT.	Identificación de la posibilidad más probable y más peligrosa.

ANEXO Nº7

ENTREVISTA A ESPECIALISTAS EN INTELIGENCIA

I. FINALIDAD

El instrumento fue estructurado para obtener información específica de especialistas en inteligencia que permanentemente recurren a los procesos de preparación de inteligencia existentes y vigentes en nuestra doctrina, con el propósito de alcanzar los objetivos específicos planteados en el presente trabajo.

II. ESPECIALISTAS CONSIDERADOS PARA LA ENTREVISTA

- Especialistas en inteligencia (en servicio activo) que tengan conocimientos especializados sobre los procesos de preparación de inteligencia, y se desempeñen como asesores de la función en UACs.

- Especialistas en inteligencia (en servicio activo) que tengan conocimientos especializados sobre los procesos de preparación de inteligencia, y se desempeñen como comandantes de Agrupaciones de inteligencia.

- Especialistas en inteligencia (en servicio activo) que tengan conocimientos especializados sobre los procesos de preparación de inteligencia, y hayan impartido clases de la doctrina de las metodologías vigentes en nuestra reglamentación en la Escuela de Inteligencia.

III. DESARROLLO DE LA ENTREVISTA.

Presentación

Dar a conocer a los especialistas los motivos por los cuales se está desarrollando la presente investigación en el marco que establece el programa de estudios del Curso Regular de Estado Mayor (CREM) y cómo su aporte contribuye al proceso.

Introducción

Describir, en términos generales la investigación que se está realizando y enmarcar el contexto en que se desarrollará la entrevista, la cual será semiabierta, de opinión y conocimiento, lo que permite al experto referirse al sentido al tema. Se declara que la información vertida será para uso de este autor en el ámbito académico y específicamente en el desarrollo de esta investigación.

Preguntas asociadas a los Procesos de Inteligencia:

- *¿Considera que actualmente nuestra institución a través del trabajo directivo y operativo de sus organismos de inteligencia analiza amenazas de naturaleza híbrida?.*

- *¿Durante los EE-C, o en las tareas operativas propias de la función, cuáles han sido las herramientas de inteligencia que ha utilizado con mayor preponderancia en apoyo a los procesos de planificación, IPB, JIPOE u otras?.*

- *¿Cuál fue el motivo de esa elección y los recursos fueron eficientes para el análisis del campo de batalla o ambiente operacional y de las amenazas identificadas?.*

- *Considera que el IPB, y específicamente el paso Nº3 "Evaluación de la Amenaza", ¿es parte de un proceso metodológico y herramienta útil para el análisis de amenazas de naturaleza híbridas?.*

- *¿Considera que JIPOE ofrece factores y variables de análisis suficientes y precisas para analizar un ambiente operacional complejo y amenazas de naturaleza híbridas?. ¿Si no es así, cuál serían los vacíos doctrinales y analíticos que usted evidencia de este proceso?.*

- *A su juicio, ¿Cuál es el proceso o herramienta de inteligencia que actualmente ostenta de mayores recursos para analizar amenazas de naturaleza híbridas?.*

- *¿Qué otras variables de análisis deberían abordar los procesos de inteligencia presentes en nuestra doctrina institucional y conjunta, para analizar amenazas de naturaleza híbridas?*

- *¿Tiene usted algún conocimiento del concepto y metodología de preparación de inteligencia "Intelligence Preparations for Operations" (IPO) utilizado en EEUU en la primera década de los años dos mil?.*

- *¿Considera que una herramienta no vigente como IPO, podría contribuir a completar ciertos vacíos analíticos, debido a su especificidad en el análisis de amenazas ligadas a la criminalidad, terrorismo y crimen organizado?*

ANEXO Nº8

PROCESAMIENTO DE ENCUESTAS

Para poder dar complementar y entregar un mayor grado de rigor científico a la investigación, en la determinación de las experiencias obtenidas en el empleo de las herramientas de inteligencia, se consideró realizar encuestas a oficiales especialistas conforme a los perfiles declarados en el primer capítulo, basándose principalmente en comandantes de AGRINT, Asesores en UACs, integrantes de la Escuela de Inteligencia, y otros encuestados que entregaron fundamentos importantes para contribuir con este trabajo académico, siendo los siguientes:

- Especialista Nº1 SR. Nicolás Alfaro Muñoz.[13]
- Especialista Nº2 TCL. Gonzalo Gómez Abutridy.[14]
- Especialista Nº3 TCL. Andrés Rodríguez Menares[15]
- Especialista Nª4 TCL. Nicolás Kaiser Onetto.[16]
- Especialista Nº5 TCL. Branco Versalovic Serrano.[17]
- Especialista N°6 TCL. Juan Mansilla Garrido.[18]
- Especialista Nº7 MAY. Francisco Zúñiga Navarrete.[19]
- Especialista Nº8 MAY. Mauricio Solís Aliaga[20]
- Especialista Nº9 MAY. Carlos Espinoza Amas.[21]

---

[13] SR. Nicolás Alfaro Muñoz, Periodista. Se desempeña como analista en la Agencia Nacional de Inteligencia.

[14] TCL. Gonzalo Gómez Abutridy, Oficial de Ejército, posee la especialidad primaria de Ingeniero Politécnico Militar, especialista en Inteligencia. Se desempeña actualmente como Sub Jefe de Informática de la División de Telecomunicaciones.

[15] TCL. Andrés Rodríguez Menares, Oficial de Ejército, posee la especialidad primaria de Oficial de Estado Mayor, especialista en Inteligencia. Se desempeña como Comandante del Batallón de Guerra Electrónica perteneciente al RINTE Nº2 “Llaitún”.

[16] TCL. Nicolás Kaiser Onetto, Oficial de Ejército, posee la especialidad primaria de Oficial de Estado Mayor, especialista en Inteligencia. Se desempeñó como Comandante del Batallón de Ciberdefensa, perteneciente al RINTE Nº2 “Llaitún”.

[17] TCL. Branco Versalovic Serrano, Oficial de Ejército, posee la especialidad primaria de Oficial de Estado Mayor, especialista en Inteligencia. Se desempeñó como Comandante de la AGRINT “Antofagasta”.

[18] TCL. Juan Mansilla Garrido, Oficial de Ejército, posee la especialidad primaria de Oficial de Estado Mayor, no es especialista en Inteligencia, sin embargo, se desempeña actualmente como asesor de inteligencia en la III DE.

[19] MAY. Francisco Zúñiga Navarrete, Oficial de Ejército, posee la especialidad primaria de Oficial de Estado Mayor, especialista en Inteligencia. Se desempeña como comandante de la AGRINT Valdivia.

[20] MAY. Mauricio Solís Aliaga, Oficial de Ejército, alumno del II CREM de la Academia de Guerra del Ejército de Chile , especialista en Inteligencia. Se desempeñó como asesor de inteligencia para el EE-C del 2019 e impartió docencia de IPB y JIPOE en cursos institucionales y conjuntos en la ESCINT, desde el 2016 hasta el 2021.

Tabla "Contenidos encuestas a especialistas en inteligencia"

Pregunta formulada	Encuestado	Información obtenida
¿Considera que actualmente nuestra institución a través del trabajo directivo y operativo de sus organismos de inteligencia, analiza amenazas de naturaleza híbrida?	SR. N. ALFARO M.	*Desconozco si se está haciendo dicho trabajo*.
	TCL. G. GOMEZ A.	*"no las considera en su aplicación práctica, aun efectúa un proceso de compartimentaje de las amenazas y no en su concepción como una afectación a un todo, no solamente por niveles".*
	TCL A. RODRÍGUEZ M.	*"Si, en algunos aspectos de cómo se ha ido modificando o cambiando la amenaza, en el contexto de las nuevas amenazas a las cuales el estado se ve enfrentado, es así como también en el contexto de los estados de excepción que se encuentran actualmente en vigencia el análisis de la posibilidad se da de esta forma".*
	TCL. N. KAISER O.	*"Los organismos siempre están analizando amenazas, independiente de su naturaleza. La naturaleza hibrida obedece a que no hay claridad en ella. Por otra parte, no hay de perder de vista la producción de inteligencia es para la toma de decisiones para una tarea y misión específica por lo que sí es de naturaleza regular, irregular o hibrida dependerá de las orientaciones del escalón superior".*
	TCL. B. VERSALOVIC S.	*"En seguridad exterior, existiendo una planificación de crisis y EPB, para enfrentar un conflicto, pareciera lógico que estos organismos de inteligencia de los distintos niveles, debieran estar capacitados para analizar este tipo de amenaza. En tareas a asociadas a seguridad interior, es más difícil, pero no imposible. Lo anterior, dado los alcances de la ley de inteligencia, por tanto se circunscriben a lo que pueden hacer los organismos y unidades de inteligencia de las policías, con los recursos y capacidades disponibles, además de lo que debería aportar la ANI. En síntesis, y de acuerdo a mi experiencia, existe una brecha con respecto a este tema que podrían priorizarse;*

[21] MAY. Carlos Espinoza Amas, Oficial de Ejército, alumno del II CREM de la Academia de Guerra del Ejército de Chile , especialista en Inteligencia. Se desempeñó como como asesor de inteligencia para el EE-C del 2019 e impartió docencia de IPB y JIPOE en cursos institucionales y conjuntos en la ESCINT, desde el 2012 AL 2016.

		Doctrina, estructura, recurso humano, entrenamiento y capacitación, material y tecnología, a lo menos".
	TCL. J. MANSILLA G.	*No, debido a que la realidad institucional no se encuentra familiarizada con este tipo de amenazas y se enfoca a la amenaza tradicional*
	MAY. F. ZUÑIGA N.	*"Sí, si bien la doctrina institucional aún no aborda en plenitud las amenazas híbridas el trabajo directivo y operativo considera las amenazas del espectro híbrido".*
	MAY. M. SOLIS A.	*"A la fecha los organismos de inteligencia probablemente no enfocan sus análisis a las amenazas hibridas dado a que no se han estructurado posibilidades integrando fuerzas regulares y amenazas no convencionales, como es el caso de la amenaza hibrida. sin embargo en el último tiempo la Fuerza Terrestre ha tenido que enfrentarse a diferente tipos de amenazas, tales como el Narcotráfico, crimen organizado, migración ilegal descontrolada, violencia política, entre otros.* *Todas estas amenazas emergentes deben ser monitoreadas por los organismos de inteligencia, debido a que nuestros potenciales adversarios podrían aprovecharlos y complementarlos con una fuerza regular en caso de conflicto, pudiendo obtener una ventaja significativa".*
	MAY. C. ESPINOZA A.	*"Creo que efectivamente se está realizando un trabajo de análisis de estas amenazas, debido a que cada vez fueron afectando de manera evidente al país, por lo tanto, la institución se vio involucrada en el proceso de detección, identificación y determinación cualitativa y cuantitativa de las amenazas de naturaleza híbrida que cada vez tomaban más fuerza en su accionar".*

Pregunta formulada	**Encuestado**	**Información obtenida**
¿Durante los EEC, o en las tareas operativas propias de la función, cuáles han sido las herramientas de inteligencia que ha utilizado con mayor preponderancia en	SR. N. ALFARO M.	*Otras: En el ámbito civil no se usan dichas herramientas en su totalidad, sin embargo, algunos factores si son importantes, como los factores políticos, culturales, para analizar por ejemplo a una sociedad o a sus agrupaciones más influyentes.*
	TCL. G. GOMEZ A.	*Otras: "Nuevas herramientas de planificación tecnológicas TAK GOV, que son más acordes a*

apoyo a los procesos de planificación, IPB, JIPOE u otras? ¿Cuál fue el motivo de esa elección y los recursos fueron eficientes para el análisis del campo de batalla o ambiente operacional y de las amenazas identificadas?		*actividades MOOTW".*
	TCL. A. RODRÍGUEZ M.	*IPB, JIPOE y otras: "Se han ocupado las herramientas descritas, así como otras para realizar un análisis más completo en cuanto a la MZS ya que solo una herramienta no alcanza para definir el problema y no se ajusta a todas las variables que se presentan".*
	TCL. N. KAISER O.	*IPB y JIPOE: "El motivo es porque son las herramientas institucionales que se tiene para analizar en campo de batalla. Respecto a los recursos, es complejos porque los HQ en EEC no son Institucionales y los medios de obtención si (por causa de Ley de Inteligencia). Otra cosa es que las personas que componen un HQ de esas características no siempre tiene su dotación completa".*
	TCL. B. VERSALOVIC S.	*JIPOE: "ambiente multidimensional, se optó por recurrir a todos los organismos de inteligencia de la región".*
	TCL. J. MANSILLA G.	*IPB: Se considera esta herramienta por lo práctico y breve que es para su utilización sin embargo al no tener acceso a la información de posibles amenazas que podrían comportarse hibrida mente no se puede obtener antecedentes de este tipo de amenazas*
	MAY. F. ZÚÑIGA N.	*JIPOE: "El JIPOE entrega variables de análisis adecuadas para efectuar una comprensión del ambiente operacional".*
	MAY. M. SOLIS A.	*IPB, JIPOE y otras: Todas las herramientas han sido ocupadas y se seleccionan en base a la tarea por cumplir y la naturaleza de la amenaza, es importante recalcar que estas herramientas no son rígidas y no deben ocuparse completas, sino que se debe seleccionar lo que sea útil para el análisis. No existen herramientas perfectas, lo que existe es la preparación y habilidad del analista para seleccionar qué elementos del IPB o JIPOE ocupar y si es necesario modificar alguno, se debe hacer, basado en el principio de la flexibilidad.*
	MAY. C. ESPINOZA A.	*IPB, JIPOE y otras: "Se utilizaron todas las herramientas, sin embargo, en procesos reales es difícil determinar si se está ocupando una u otra herramienta, creo que uno intencionalmente utiliza todas las herramientas a disposición, tanto doctrinarias como otras que no lo son, pero que ayudan a simplificar los procesos".*

Pregunta formulada	Encuestado	Información obtenida
¿Considera que el IPB, y específicamente el paso Nº3 "Evaluación de la Amenaza", es parte de un proceso metodológico y herramienta útil para el análisis de amenazas de naturaleza híbridas?.	SR. N. ALFARO M.	*Sin duda, ya que el proceso de evaluación de la amenaza permite estimar las eventuales respuesta de nuestra parte, estableciendo cuales son efectivamente los mayores riesgos a los que se puede enfrentar un especialista de inteligencia. Esto es más necesario cuando se analizan amenazas de naturaleza híbrida, las que no siguen un modelo "común" y puede utilizar diversos mecanismos, por lo que es fundamental realizar un proceso metódico y acabado de evaluación de dicha amenaza.*
	TCL. G. GOMEZ A.	*"no es la mejor para amenazas hibridas, por su origen y concepción a un nivel especifico de la amenaza"*
	TCL. A. RODRÍGUEZ M.	*"No, ya que no se cuenta con todos las herramientas este paso para definir una amenaza que no se cuenta con información doctrinaria y que modifica su actuar de forma permanente".*
	TCL. N. KAISER O.	*"Si nos quedamos con lo que señala la doctrina nacional vigente, no lo es. Sin embargo se pueden complementar con doctrinas similares (EEUU) que están actualizada y consideran variables o amenazas de naturaleza híbrida".*
	TCL. B. VERSALOVIC S.	*"Si, pero es posible complementarla con otras herramientas metodológicas, empleadas por otros organismos de inteligencia asociados a seguridad interior".*
	TCL. J. MANSILLA G.	*No, debido a lo expuesto anteriormente que hace mención a su uso a la amenaza tradicional*
	MAY. F. ZÚÑIGA N.	*"No, la evaluación de la amenaza del IPB está diseñado para unidades regulares. Por lo anterior, es necesario ampliarlo para evaluar las amenazas de carácter híbrido".*
	MAY. M. SOLIS A.	*Si, totalmente la amenaza hibrida puede ser ¡clasificada dentro de los formatos ORBAT, ya que tienen una composición, dispositivo, fuerza, eficiencia de combate, tácticas y procedimientos de empleo, logística y características especiales, también se pueden elaborar plantillas doctrinales, como modelos de empleo de estas amenazas y por otra parte, también se puede clasificar la información en la matriz de sistemas claves.* *Un antecedente muy importante es el paso 3 del IPB para operaciones distintas a la guerra, en*

		donde sus elementos de análisis son totalmente compatibles con este tipo de amenazas.
	MAY. C. ESPINOZA A.	*"Creo que no se ajusta mucho a la realidad de este tipo de amenazas, debido a que puede ser en ocasiones poco flexible. Al mismo tiempo, si uno posee dominio del IPB logrará adaptar esta herramienta a la amenaza que esté enfrentando sin seguir el paso a paso y quizás utilizaría los aspectos más claves como la determinación de los HVT, que no necesariamente requieren todo el proceso establecido en el paso 3 del IPB".*

Pregunta formulada	**Encuestado**	**Información obtenida**
¿Considera que JIPOE ofrece factores y variables de análisis suficientes y precisas para analizar un ambiente operacional complejo y amenazas de naturaleza híbridas?. ¿Si no es así, cuál serían los vacíos doctrinales y analíticos que usted evidencia de este proceso?.	SR. N. ALFARO M.	*A mi parecer, dicho proceso se enfoca en las amenazas regulares, de un ejército contra otro y en menor medida en operaciones especiales. Sin embargo, se me hace necesario actualizar dichos mecanismos a las nuevas amenazas híbridas, las que pueden tener injerencia de medios de comunicación, actores estatales, incluso herramientas de inteligencia artificial, por lo que es necesario una actualización.*
	TCL. G. GOMEZ A.	*"Si, este considera lo requerido para el análisis. sin embargo, no se ve como la mejor para el ámbito de los productos requerimientos como información de la amenaza para una del tipo hibrida".*
	TCL. A. RODRÍGUEZ M.	*"El JIPOE es una herramienta de nivel operacional, por ende queda con vacíos a nivel táctico entendiendo que hay parámetros que doctrinariamente no cubre esta herramienta y menos con una amenaza de carácter hibrida, lo anterior se puede subsanar agregando más factores de análisis".*
	TCL. N. KAISER ON.	*El JIPOE es una metodología. El reglamento entrega herramientas. Si no están todas las variables, ahí está el arte del asesor para poder identificarlas e incorporarlas*
	TCL. B. VERSALOVIC S.	*"Si, solamente habría que incorporar en el análisis tanto la amenaza regular como la irregular, lo que debería decantar de los pasos 1 y 2. Estimo revisar el modelo que emplean las policías de chile, DIRECTEMAR, DGAC, además lo que especifica la doctrina de inteligencia de países referentes. ¿Cómo lo hace Colombia, Perú....?"*
	TCL. J. MANSILLA G.	*Sí.*

	MAY. F. ZÚÑIGA N.	*"El JIPOE es una herramienta de nivel operacional, por ende queda con vacíos a nivel táctico entendiendo que hay parámetros que doctrinariamente no cubre esta herramienta y menos con una amenaza de carácter hibrida, lo anterior se puede subsanar agregando más factores de análisis".*
	MAY. M. SOLIS A.	*Si, uno entre otros elementos del JIPOE que sirve al análisis de este tipo de amenazas, es la clasificación de información a través de los factores PEMSI -PT y el desarrollo de un diagrama de sistemas, para comprender el ambiente operacional.*
	MAY. C. ESPINOZA A.	*"Creo que ofrece incluso más variables que las que realmente se necesitarán aplicar, debido a que luego del análisis de los factores PEMSIIPT siempre hay elementos que finalmente son descartados del análisis".*

Pregunta formulada	**Encuestado**	**Información obtenida**
A su juicio, ¿Cuál es el proceso o herramienta de inteligencia que actualmente ostenta de mayores recursos para analizar amenazas de naturaleza híbridas?	SR. N. ALFARO M.	*JIPOE: El IPB nuevamente radica principalmente en la planificación en un nivel táctico, por lo que es insuficiente para analizar, prever o mitigar las amenazas híbridas. En este caso el JIPOE me parece una herramienta mucho más completa y que incluye más factores para poder hacer un análisis certero.*
	TCL. G. GOMEZ A.	*JIPOE: "es lo que actualmente entrega más productos".*
	TCL. A. RODRÍGUEZ	*IPB: En el ambiente donde se desarrollan las operaciones en el caso de la MZS se presenta como una mejor herramienta para poder describir este tipo de amenaza, no obstante, a lo anterior esta herramienta debe ser complementada*
	TCL. N. KAISER O.	*JIPOE: Las variables y metodología empleadas permite analizar de forma sistémica el problema, otorgando más herramientas para identificar diversas amenazas, independiente de su naturaleza.*
	TCL. B. VERSALOVIC S.	*JIPOE: Puntualmente del nivel estratégico, al abarcar más variables en función de herramientas disponibles para apoyar el proceso de toma de decisiones.*
	TCL. J. MANSILLA G.	*JIPOE: Por la amplitud de ambientes que se puede analizar*

	MAY. F. ZÚÑIGA N.	*JIPOE: Como se mencionó anteriormente, el JIPOE ofrece herramientas analíticas más adecuadas para comprender el ambiente operacional considerando actores de naturaleza híbrida y en todas las dimensiones.*
	MAY. M. SOLIS A.	*IPB y JIPOE: Ambas tienen buenos recursos, en el momento de seleccionar una o la otra, se deberá considerar el nivel de la conducción, la naturaleza de la amenaza y la tarea que se debe cumplir*
	MAY. C. ESPINOZA A.	*JIPOE: Contempla más factores, lo que es fundamental para analizar este tipo de amenazas.*

Pregunta formulada	**Encuestado**	**Información obtenida**
¿Qué otras variables de análisis deberían abordar los procesos de inteligencia presentes en nuestra doctrina institucional y conjunta, para analizar amenazas de naturaleza híbridas?	SR. N. ALFARO M.	*Si bien desconozco el detalle de la doctrina institucional, encuentro necesario abordar los procesos de inteligencia desde el enfoque de la prospectiva y en análisis del futuro. El objetivo de la inteligencia siempre debería ser prever los eventuales ataques y amenazas y en ese contexto, a mi parecer falta un enfoque prospectivo al enseñar la inteligencia.*
	TCL. G. GOMEZ A.	*"Del espectro electromagnético (CEMA)"*
	TCL. A. RODRÍGUEZ	*"Naturaleza e historia de la amenaza, razones de orden ideológico e historia, análisis de personalidades más características de la amenaza, estructura organizacional de cambio permanente".*
	TCL. N. KAISER O.	*Las variables son las que puedan estar afectando la misión y tarea específica. Obviamente se tienen que incorporar elementos como las amenazas cibernéticas, empleo de PMC (Wagner Group), etc. pero insisto todo lo que puede afectar el cumplimiento de la misión debe ser considerado, ya sea para una tarea de la Fuerza Militar o bien de una fuerza policial según corresponda.*
	TCL. B. VERSALOVIC S.	*"Revisar TICA El conflicto Hibrido y sus efectos en la conducción operacional y táctica".*
	TCL. J. MANSILLA G.	*Ninguna.*
	MAY. F. ZÚÑIGA N.	*"PEMSII-PTL y ASCOPE"*
	MAY. M. SOLIS A.	*Cualquier tipo de variable que sea necesario incorporar y que sea útil para el análisis, no existen herramientas perfectas, en cada una de*

		ellas existen diferentes elementos que pueden ser complementados con otras variables de análisis, es más importante la conclusión extraída del proceso, que el mismo proceso en sí.
	MAY. C. ESPINOZA A.	*"Creo que se debería hacer una análisis más profundo de los personalidades y liderazgos de sujetos claves, debido a que por mi experiencia con este tipo de amenazas, en ellos está el centro de gravedad".*

Pregunta formulada	**Encuestado**	**Información obtenida**
¿Tiene usted algún conocimiento del concepto y metodología de preparación de inteligencia "Intelligence Preparations for Operations" (IPO) utilizado en EEUU en la primera década de los años dos mil?. ¿Considera que una herramienta no vigente como IPO, podría contribuir a completar ciertos vacíos analíticos, debido a su especificidad en el análisis de amenazas ligadas a la criminalidad, terrorismo y crimen organizado?	SR. N. ALFARO M.	No. De todas formas, como mencioné en algunas respuestas, se debe pasar en el ámbito militar de ser un actor pasivo a un actor activo frente a amenazas híbridas tales como la criminalidad, el terrorismo interno y el crimen organizado. A mi parecer la idea de separar a las policías para interior y a las fuerzas armadas para exterior carece de fundamento en una sociedad donde las amenazas están entremezcladas. Entendiendo eso, se podrían conseguir mayores logros y prevenir eventuales amenazas a la seguridad.
	TCL. G. GOMEZ A.	*No.* *"No se encuentra pertinente".*
	TCL. A. RODRÍGUEZ	*No.* *"Si considero que puede ser una muy buena herramienta con el conocimiento adecuado y explicaciones necesarias para su implementación se puede convertir en una buena herramienta".*
	TCL. N. KAISER O.	*No.* *Podría, pero no hay que olvidar o perder de vista la naturaleza de la función defensa.*
	TCL. B. VERSALOVIC S.	*Si.* *"No lo considero necesario, si reforzar la doctrina nacional y capacidades para realizar el ciclo OODA de manera eficiente.*
	TCL. J. MANSILLA G.	*No.* *Sí.*
	MAY. F. ZÚÑIGA N.	*No".* *"Sí, el analista debe incorporar todas las herramientas y/o variables que sean necesarias*

		para obtener conclusiones sobre factores en todos los dominios. Esto permitirá una mejor comprensión del ambiente operacional y acercarse a lo que la amenaza podría realizar en función de sus capacidades".
	MAY. M. SOLIS A.	*Si.* *Es muy poco el conocimiento que tengo de ese proceso, de existir elementos que podrían ser útiles para la planificación sin duda deben ser considerados, lo importante de todo este análisis está en por qué no se ocupó este proceso finamente en el Ejército? a mi juicio es porque el IPO tiene una connotación policial y e IPB y el JIPOE a través de sus actualizaciones han ido mejorando sus elementos y herramientas útiles para cualquier tipo de amenaza*
	MAY. C. ESPINOZA A.	*No.* *"Creo que sí, debido a que se aprecia como una herramienta más pragmática".*