FUERZA AÉREA DEL PERÚ

ESCUELA DE OFICIALES

TRABAJO DE SUFICIENCIA PROFESIONAL
TÍTULO:

“LAS REDES DE AMENAZAS EN LA FUERZA AÉREA DEL PERÚ”

Línea de Investigación:

TECNOLOGÍAS DE INFORMACIÓN

PRESENTADO POR:

MAY. FAP IRVING RAÚL PORTOCARRERO PELÁEZ

ASESOR TEMÁTICO: COR. FAP RAFIK HUARCAYA IPENZA

ASESOR METODOLÓGICO: DRA. MERCY NOELIA PALIZA CHAMPI

PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS DE LA ADMINISTRACIÓN AEROESPACIAL

LIMA – 2024

DEDICATORIA

A mi guía y ángel quien fue mi Padre Raúl, a mi madre Miriam, a mis hermanas Jessica y Ana Paula y a mi novia Valeria, que son mi gran soporte, apoyo incondicional y motivación para seguir en mi desarrollo profesional y personal, y a mi abuelita Yolanda que es mi ejemplo de Esencia y Humildad.

ESCUELA DE OFICIALES DE LA FAP

DEPARTAMENTO DE INVESTIGACIÓN

DECLARACIÓN JURADA DE ORIGINALIDAD Y DE NO PLAGIO

Yo, Mayor FAP **IRVING RAÚL PORTOCARRERO PELÁEZ**, Oficial egresado de la Carrera Profesional "Ciencias de la Administración Aeroespacial" de la Escuela de Oficiales de la FAP con número de serie O-9754706 –O+, identificado con DNI 45158467 autor(a) de la Tesis titulada/ Informe de suficiencia Profesional

"LAS REDES DE AMENAZAS EN LA FUERZA AÉREA DEL PERÚ"

DECLARO BAJO JURAMENTO QUE,

El tema y contenido de la tesis son originales, reflejando el resultado de mi dedicación, y esfuerzo personal. No he recurrido a prácticas de copia, ni he empleado ideas, formulaciones, citas textuales, ni ilustraciones de otras tesis, obras, artículos, memorias, etc., ya sea en versión digital o impreso, sin mencionar de forma exacta y clara su origen, fuente o autor, tanto al texto como a los elementos visuales, como gráficos, figuras, cuadros, tablas u otros contenidos protegidos por derechos de autor.

En este sentido, soy consciente de que infringir los derechos de autor y cometer plagio conllevan consecuencias que pueden dar lugar a sanciones tanto a nivel de la institución de la FAP como a nivel legal.

Ratifico plenamente lo expresado y, como manifestación de mi compromiso, suscribo el presente documento en la Ciudad de Lima, a los TRES (03) días de abril del 2024.

Firma Digital Fuerza Aérea del Perú
Firmado digitalmente por PORTOCARRERO PELAEZ Irving Raul FAU 20144364059 soft
Motivo: Soy el autor del documento
Fecha: 03.04.2024 17:55:21 -05:00

IRVING RAÚL PORTOCARRERO PELÁEZ
D.N.I. 45158467

DNI N° 10557937
DRA. MERCY NOELIA PALIZA CHAMPI

ÍNDICE

RESUMEN

El informe de Suficiencia Profesional, se ha realizado luego de un búsqueda minuciosa y análisis detallado sobre las redes de amenazas, lo que conllevó a conseguir documentos doctrinarios, legales y operativos a nivel FAP, que me acarreó a realizar un diagnóstico situacional, para luego describir un marco teórico, metodológico, supuesta solución y proponer finalmente la solución más acorde al problema para contrarrestar las redes de amenazas.

En lo que respecta a la metodología empleada, se ha seguido el paradigma positivista, tipo de investigación aplicado, enfoque cuantitativo, alcance descriptivo y diseño no experimental. Se aplicó la técnica encuesta con su instrumento cuestionario de catorce reactivos a una muestra de 37 efectivos entre oficiales y técnicos con conocimiento en sistemas, informática, seguridad de la información, redes y algoritmos.

El informe se diseñó contemplando la aplicación del instrumento cuestionario a la muestra, para obtener información sobre el estado actual de las redes de amenazas y de los tópicos a ser considerados en el manual a implementar (Anexo I). Posteriormente, se propone el documento "Manual para contrarrestar las redes de amenazas en la FAP" (Anexo II).

El análisis de los resultados, concluye que existe la necesidad de contrarrestar las redes de amenazas, lo que sustenta la elaboración de manual que de los lineamientos para su implementación y que en la actualidad no se ha implementado, por lo que la Institución no está dando cumplimiento al requerimiento legal, por lo que se sustenta el desarrollo de un documento a modo de propuesta. Además, se manifiesta la importancia de contar con dicho documento como parte de las funciones de la Dirección de Telemática - DITEL y el Servicio de Informática - SINFA en cumplimiento de la Misión y Visión encomendada.

Palabras clave: Redes, Amenazas, Informática, Telemática.

LISTA DE FIGURAS

CAPÍTULO I

INTRODUCCIÓN

INTRODUCCIÓN

Las redes Institucionales como las redes sociales ofrecen facilidades para que las personas puedan conectarse y compartir sus formatos, información de trabajo y personal. Pero compartir de manera inadecuada, da paso a que personas ataquen o violen la seguridad de las redes, comprometiendo de esa manera la seguridad personal e Institucional. Los atacantes suelen servirse de las cuentas de redes sociales durante la fase de reconocimiento de un ataque de ingeniería social, catfishing o de phishing. Las redes pueden dar a los atacantes una plataforma para suplantar la identidad de personas y marcas, o la información que necesitan para ejecutar ataques adicionales, incluyendo los de ingeniería social y phishing. En ese sentido, el presente informe en la modalidad de Suficiencia Profesional, desarrolla el tema "LAS REDES DE AMENAZAS EN LA FUERZA AÉREA DEL PERÚ"

Las diferentes unidades FAP, siguen protocolos para la seguridad de la información, pero no todo está descrito en lo que respecta a la seguridad, por lo que, en lo que respecta a las amenazas de redes, se ha podido constatar que se tiene deficiencias.

El informe servirá como elemento de titulación; y que desarrolla como tema principal la elaboración de un manual que estará detallado en un documento. Este tema se origina primero en la necesidad de mejorar la seguridad de las redes en la FAP y por lo tanto cumplir con una de las funciones de la Dirección de Telemática que es encomendada por normatividad, que exige un desempeño eficaz y eficiente de la DITEL en el cumplimiento de su misión y por tanto la misión Institucional.

Para la mejor comprensión del trabajo y atendiendo a la necesidad de aplicación de la metodología de trabajo, se plantea y desarrolla en diez capítulos. En el capítulo I, se detalla la introducción. En el Capítulo II, se detalla el análisis situacional que contempla la situación actual en el tema de las redes de amenazas en la Fuerza Aérea del Perú, la documentación doctrinaria, legal y operativa a nivel FAP. En el Capítulo III, se desarrolla el marco teórico necesario para la mejor comprensión de los temas tratados en el cual se otorgan conceptos de ciberseguridad, control ciberespacial y capacidades operacionales del ciberespacio a nivel FAP. En el Capítulo IV, se desarrolla los supuestos de solución respecto a la metodología en investigación que sirve de base. En el Capítulo V, se propone la metodología para dar solución al problema que es contrarrestar las redes de amenazas en la FAP. En el Capítulo VI, se detallan los resultados de la ejecución de la encuesta con su cuestionario aplicado. En el Capítulo VII, se manifiestan las conclusiones más resaltantes. En el Capítulo VIII, se detallan las recomendaciones. En el Capítulo IX, se detalla la bibliografía utilizada y en el

Capítulo X, se detallan los anexos correspondientes a la encuesta con su cuestionario y a la propuesta “Manual para contrarrestar las redes de amenazas en la FAP”.

CAPÍTULO II

DIAGNÓSTICO SITUACIONAL

DIAGNÓSTICO SITUACIONAL

2.1. Ámbito del problema

El mundo del internet, ofrece a los usuarios una amplia gama de aplicaciones, como aperturas comerciales y divulgación de información con diferentes fines, pero también expone a que los usuarios puedan ser atacados por personas que buscan otros beneficios o intenciones.

Los atacantes utilizan métodos en las plataformas de las redes sociales. Los atacantes suelen solicitar acceso como petición de amistad, para validar datos o mediante solicitudes diversas que hacen posible acceder a sus publicaciones privadas, incluso se puede acceder mediante los amigos con el objetivo de llegar a un usuario en particular. Por lo que, además de acceder a las publicaciones de los usuarios, también podría accederse a sus contraseñas y como se ha visto en muchos casos, se podría hasta suplantar identidades. Incluso un atacante accediendo a la información de los usuarios y la suficiente, podría adivinar o crear algoritmos para dar respuesta de claves de seguridad privada.

En la actualidad, no sólo se acceden a la información de usuarios, sino también a marcas e instituciones, por lo que un atacante podría suplantar una marca comercial o empresarial, accediendo a envío de información, dinero y otros medios de conveniencia para el atacante de red.

A nivel internacional, se manifiesta que las 4 amenazas más comunes en las redes sociales que pueden dañar la seguridad de tus datos son: Ataques de phishing, Perfiles falsos, Lugares con redes públicas de Wi-Fi y Uso indebido de datos personales (Nicola, 2024). Asimismo, los piratas informáticos constantemente actualizan sus ataques con el objetivo de lograr un mayor éxito, algunas de las estafas que están en boga son: Vishing, Smishing, Pedir dinero por Whatsapp e Ingeniería social (Ciberseguridad: nuevas amenazas online, 2023).

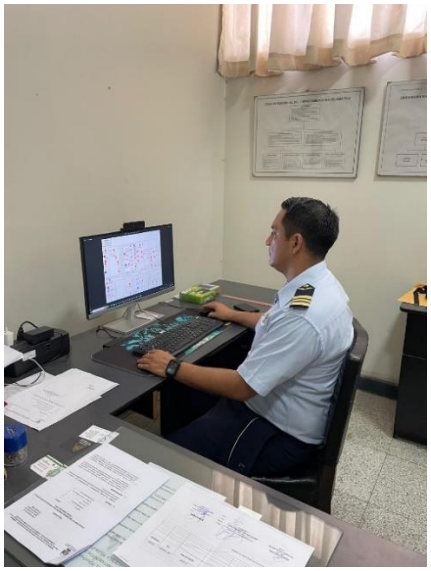
A nivel nacional, el Perú no es ajeno a las amenazas de redes, por lo que los delitos informáticos más frecuentes son los delitos contra el patrimonio. Asimismo, en el 2019, los fraudes informáticos y sus subtipos alcanzaron 2,097 denuncias (1,641 denuncias fueron transacciones no autorizadas vía internet), 268 denuncias fueron ataques con herramientas digitales como redes sociales, software y otras plataformas en línea; mientras que 247 casos fueron suplantación de identidad (Pichihua, 2020). Además, el secuestro de datos o más conocido como ransomware, es una de las principales amenazas cibernéticas, y una de la

más crecientes en el Perú; además las pequeñas empresas están expuesta a ataques cibernéticos por lo que deben incorporar dentro de su planificación del riesgo el componente digital (Ríos, 2023). Finalmente, el ciberataque se incrementó en más de 130% en pagos directos mediante las aplicaciones móviles; por malware móvil, se registran 6,334 ataques al día; por troyanos se incrementó un 50%, por lo que el Perú se ubica en el cuarto lugar en Latinoamérica con 58,000 ataques (Flores, 2023)

La Fuerza Aérea del Perú, es una institución que podría ser atacada con diferentes fines, ya sea militar o privado. En ese sentido, acceder a la información FAP, pondría en peligro, las operaciones, al personal y por tanto la Defensa de la Nación. Por lo que la FAP, debe y en la actualidad cuenta con una división encargada de velar por la seguridad del ciberespacio, por lo que se prevén operaciones de información para salvaguardar la integridad de la información y mantener la supremacía del Ciberespacio, ya que todas las organizaciones e infraestructuras críticas están bajo el control y supervisión de sistemas de adquisición de datos y redes o sistemas de control. En ese sentido, la institución podría presentar tres vulnerabilidades que son: Propiedad extranjera, control e influencia de los vendedores, Cadena de suministro y Tecnología comercial.

Figura 1

Gestión del sistema de redes de la EOFAP



La FAP cuenta entre sus Órganos de Administración Interna con la Dirección de Telemática de la Fuerza Aérea del Perú (DITEL), es el órgano dependiente de la Comandancia General, responsable de planificar y dirigir las actividades para el desarrollo

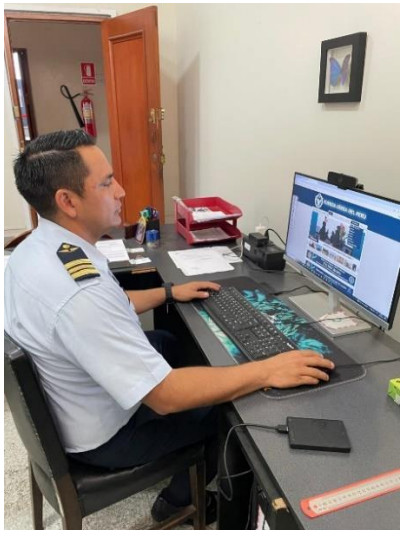
de las tecnologías de la información y comunicaciones, así como el soporte tecnológico para la defensa del ciberespacio. Está compuesta por el Servicio de Informática (SINFA) y el Servicio de Comunicaciones (SECOM). Asimismo, el Servicio de Informática (SINFA) es responsable de desarrollar, integrar, mantener, proteger y operar las capacidades de la infraestructura de tecnologías de información necesarias para el soporte de las actividades ante las amenazas contra las tecnologías de la información y comunicaciones a las redes de la Fuerza Aérea del Perú, a fi n de contribuir al logro de la superioridad de la información (D. S. Nº 008-2023-DE, 2023).

Figura 2

Mantenimiento del sistema de redes de la EOFAP

Figura 3

Programación en el Departamento de Telemática de la EOFAP



A nivel de las Unidades y Dependencias FAP, se cuenta con Departamentos de Informática, como es el caso particular de la EOFAP, que cuenta con el Departamento de Telemática que, entre sus tareas, administra el sistema de informática y medios de comunicación, previendo sus requerimientos y operatividad; además en su estructura orgánica, cuenta con la Sección Informática y la Sección Comunicaciones (MOF FAP, p, 211).

Debido a las vulnerabilidades a las que puede estar sometida la institución, la presente investigación tiene por objetivo describir las redes de amenazas a nivel institucional para poder proponer una respuesta inmediata para reducir, contener y eliminar las amenazas de redes.

2.2. Aspecto doctrinario

2.2.1. Doctrina Básica de la Fuerza Aérea del Perú – DBFA1

Según la DBFA1 (2021), en lo referente al ciberespacio, se detalla lo siguiente:

El Poder Militar Aeroespacial, es la capacidad que posee un Estado, de emplear los medios que tienen las Fuerzas Armadas en el aire, espacio y ciberespacio, para contribuir con la Seguridad y Defensa Nacional. La Fuerza Aérea del Perú lidera el Poder Militar Aeroespacial. Los dominios que configuran el Poder Militar Aeroespacial son los siguientes: dominio aéreo, domino espacial y dominio ciberespacial (p. 8).

El Potencial Militar Aeroespacial, es la capacidad futura que posee un Estado, de emplear los medios que tienen las Fuerzas Armadas en el aire, espacio y ciberespacio, para contribuir con la Seguridad y Defensa Nacional. Considera como parte de sus elementos a la reserva aérea; así como la infraestructura y la industria militar aeronáutica, espacial y ciberespacial (p. 9).

Dominios del Poder Militar Aeroespacial, los dominios son construcciones útiles para visualizar y caracterizar el entorno físico (terrestre, marítimo, aéreo, espacial) y no físico (ciberespacial) en el que se realizan las operaciones y acciones militares; tienen características propias diferenciadas, que condicionan las aptitudes y procedimientos de los medios, fuerzas y capacidades que deben operar en ellos. Los dominios en los cuales la Fuerza Aérea del Perú, como líder del Poder Militar Aeroespacial, realiza sus operaciones y acciones militares, son el dominio aéreo, el dominio espacial y el dominio ciberespacial. Además, el domino ciberespacial es "un dominio global artificial dentro del entorno de

información que consiste en la red interdependiente de infraestructuras de tecnología de la información, que incluye internet, redes de telecomunicaciones, sistemas informáticos, así como procesadores y controladores integrados". Este dominio actúa de manera transversal a los demás dominios (p. 10).

El Poder Ciberespacial, se refiere a la capacidad de un Estado de utilizar los medios tecnológicos a través de señales digitales en forma ofensiva o defensiva en el dominio ciberespacial, para crear ventajas operacionales e influenciar en los otros dominios operacionales (p. 46).

El Control Ciberespacial, es la capacidad para controlar toda acción en el ciberespacio propio, o asignado, que contribuya a la libertad de acción de las fuerzas propias y amigas, independientemente del domino en el que estas operen, siendo a) Operaciones Defensivas, b) Operaciones de Explotación y c) Operaciones de Respuesta (p. 79).

El Apoyo y sostenimiento a las operaciones ciberespaciales, es la capacidad de procesar la información obtenida en y mediante el ciberespacio propio o asignado (p. 90).

2.3. Aspecto legal

2.3.1. Constitución Política del Perú

Según la Constitución Política del Perú de 1993 (2022), en lo referente a la persona, se indica lo siguiente:

En el Título I: De la Persona y de la Sociedad, Capítulo I: Derechos fundamentales de la persona, en su Artículo 2. Toda persona tiene derecho entre otros a, las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley (p. 10).

En el Título IV: De La Estructura del Estado, en el Capítulo XII: De la seguridad y defensa nacional, en su Artículo 165, indica que las Fuerzas Armadas están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea. Tienen como finalidad primordial garantizar la independencia, la soberanía y la integridad territorial de la República (p. 102). Asimismo, el Artículo 171. Las Fuerzas Armadas y la Policía Nacional participan en el desarrollo económico y social del país, y en la defensa civil de acuerdo a ley (p. 103).

2.3.2. Decreto legislativo Nº 1139, Ley de la Fuerza Aérea del Perú

Según el D. L. N° 1139 (2012), dispone lo siguiente:

En el Titulo II: Competencias y funciones. Capítulo I: Competencias, en su Artículo 3°. - Ámbito de competencia, la FAP, controla, vigila y defiende el espacio aéreo del país, qua cubre su territorio y el mar adyacente hasta el límite de las doscientas millas, de conformidad con la ley y con los tratados ratificados par el Estado, con el propósito de contribuir a garantizar la independencia, soberanía e integridad territorial de la Republica. Interviene en los estados de excepción y participa en el control del orden interno, de acuerdo con lo establecido en la Constitución Política del Perú y leyes vigentes. Participa en el Desarrollo Económico Social del País, en la ejecuci6n de acciones cívicas y de apoyo social en coordinaci6n con las entidades públicas cuando corresponda, así como en las acciones relacionadas con la Defensa Civil, de acuerdo a la ley. La FAP dirige las actividades correspondientes al Poder Aéreo y participa en las acciones relacionadas con los intereses aeroespaciales (p. 480442).

En el Capítulo II Funciones, el Artículo 4°. - Funciones, se indica que la FAP, en el marco de sus competencias, cumple las siguientes funciones entre otras: Garantizar la independencia, la soberanía y la integridad territorial de la República, en el ámbito de su competencia; Desarrollar actividades de inteligencia orientadas a la Seguridad y Defensa Nacional en el ámbito de su competencia; Conducir las acciones de preparación, formación, capacitación, especialización, perfeccionamiento, entrenamiento, mantenimiento y equipamiento del Componente Aéreo de las Fuerzas Armadas, en funci6n de los objetivos y de las Políticas de Seguridad y Defensa Nacional (p. 480443).

En el Titulo III: Organización, Capítulo VI: Órganos de Administración Interna, en su Artículo 14.- Direcciones Generales y Direcciones, se manifiesta que la FAP cuenta con Direcciones Generales como órganos de apoyo de primer nivel; asimismo con Direcciones, como órganos encargados de proporcionar el apoyo administrativo, técnico y normativo, así como desarrollar acciones para el cumplimiento de las competencias, funciones y la defensa de los intereses Institucionales. Su organización interna, conformación, funciones y atribuciones se establecerán en el reglamento de la presente norma (p. 480445).

2.3.3. Ley Nº 30096, Ley de Delitos Informáticos

Según la Ley N° 30096 (2013), dispone lo siguiente:

En el Capítulo II: Delitos Contra Datos y Sistemas Informáticos, en su Artículo 3. Atentado contra la integridad de datos informáticos. El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa (p. 505484). Asimismo, en el Artículo 4. Atentado contra la integridad de sistemas informáticos. El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa (p. 505485).

2.3.4. Ley Nº 30999, Ley de Ciberdefensa

Según la Ley Nº 30999 (2019, p. 9-10), dispone lo siguiente:

En el TÍTULO II: De la Ciberdefensa, Capítulo I: Las Capacidades de Ciberdefensa y las Operaciones en y mediante el Ciberespacio, en el Artículo 6. De las capacidades de ciberdefensa. Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

El Artículo 7. De las operaciones militares en el ciberespacio. Es el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o los ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

El Artículo 8. De la planificación y ejecución de las operaciones en el ciberespacio. La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

En el Capítulo III: De la Seguridad de los Activos Críticos Nacionales y Recursos Claves, en su Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves. El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de

protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fi n de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

2.3.5. Decreto Supremo Nº 017-2024-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa

Según el Decreto Supremo Nº 017-2024-PCM (2024), dispone lo siguiente:

El Capítulo III: Capacidades de Ciberdefensa, en su Artículo 5.- De las medidas pasivas y activas de ciberdefensa. 5.1 Medidas pasivas en ciberdefensa: conjunto de actividades de prevención, protección y resiliencia del ciberespacio propio y/o asignado. Son de aplicación constante y generalizada, abarcando al personal, medios y sistemas propios o asignados. Involucra, pero no se limita al monitoreo de redes propias o asignadas, mantenimiento de sistemas informáticos, actualizaciones de seguridad y operativas, establecimiento de políticas, disposiciones, procedimientos y reglas de seguridad institucional, robustecimiento en la infraestructura cibernética propia y la concientización en materia de ciberdefensa, entre otras. 5.2 Medidas activas en ciberdefensa: conjunto de actividades de naturaleza proactiva, reactiva o de recuperación, en o mediante el ciberespacio propio, asignado y/o de interés. Estas medidas se aplican ante la necesidad militar para la defensa y la seguridad nacional. Involucra, pero no se limita al análisis de vulnerabilidades, una intensa labor de detección, evaluación, identificación y reconocimiento de actos hostiles o amenazas en el ciberespacio; o la aplicación de acciones cibernéticas sobre medios o sistemas que constituyen una amenaza, para degradar o neutralizar sus capacidades y formas de acción, a fin de impedir que estas puedan afectar la libertad de acción en el ciberespacio propio, asignado y/o de interés, entre otras.

En el Artículo 6.- Capacidades de ciberdefensa de los Órganos Ejecutores del Ministerio de Defensa. En el ámbito de sus competencias, el COCID y los Componentes de Ciberdefensa de las Instituciones Armadas cuentan con las capacidades siguientes: a. Capacidad de Defensa: consiste en la prevención, protección y resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas; b. Capacidad de explotación: consiste en la búsqueda, identificación, reconocimiento, vigilancia y seguimiento de ciber amenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas; c. Capacidad de respuesta: consiste en limitar o negar, temporal

o permanentemente, el uso del ciberespacio del objetivo militar mediante la degradación o neutralización de sus sistemas, impactando en sus capacidades; recurriendo a medidas activas.

En el Capítulo V: Del Uso de la Fuerza en y Mediante el Ciberespacio, en su Artículo 9.- Autorización para el uso de la fuerza La autorización para el uso de la fuerza en las operaciones militares en y mediante el ciberespacio que atente contra la seguridad nacional está sujeta a disposición expresa, por parte del Presidente de la República, Jefe Supremo de las Fuerzas Armadas, que se efectúa por medio de Resolución Suprema refrendada por el Ministro de Defensa, y se ejecuta a través de los procedimientos establecidos para las otras operaciones militares, conforme a la normativa establecida para tal fin.

En el Título II: De la Seguridad de los Activos Críticos Nacionales y Recursos Claves, Capítulo I: De la Protección de Control de los ACN/RC. Artículo 14.- Protección y control de los activos críticos nacionales y recursos claves en y mediante el ciberespacio. 14.1 Se considera que la seguridad digital de los ACN/RC es afectada cuando se genera un ataque directo o inminente a sus recursos, infraestructura y sistema en sus componentes digitales, por la materialización de riesgos derivados de amenazas y vulnerabilidades en y mediante el ciberespacio, y que generen como consecuencia daños a la persona, prosperidad económica, social y la seguridad nacional.

2.4. Aspecto Operativo

2.4.1. DOFA 1-4, Doctrina Operacional de Operaciones en el Ciberespacio

Según la DOFA 1-4 (2016), dispone lo siguiente:

En el Capítulo III: Comando y Organización, 3.- Organización de las Operaciones en el Ciberespacio. La Fuerza Aérea organiza, entrena y equipa a sus fuerzas cibernéticas para apoyar a los Comandos Operacionales. Las fuerzas conjuntas del ciberespacio son una parte integral de las operaciones militares y las relaciones de comando son cruciales para garantizar el empleo eficaz y oportuno. El personal del Estado Mayor Conjunto planea y ejecuta las operaciones militares y del ciberespacio, además tienen la responsabilidad de establecer prioridades, evitar conflictos, integrar y sincronizar las operaciones militares del ciberespacio con las operaciones conjuntas en curso y previstas. Las operaciones del ciberespacio se ejecutan como se indica: a.- Nivel Estratégico, b.- Nivel Operacional, c.- Comando de la Fuerza Aérea en el Ciberespacio, y d.- Organizaciones ISR de la Fuerza

Aérea (p. 21).

2.4.2. Ordenanza FAP 21–1, "Telemática", Estimación de Riesgos de Ciberseguridad en las Unidades FAP

Según la Ordenanza FAP 21–1 (2023), dispone lo siguiente:

En el punto 1.- Objeto. Establecer las normas y los procedimientos que orienten el desarrollo y la realización de la estimación de riesgos de ciberseguridad en las Unidades FAP 5.- Finalidad. Identificar, analizar y evaluar los riesgos de ciberseguridad en las UU FAP, con el propósito de determinar su adecuado tratamiento, así como posibilitar la implementación de una o varias opciones orientadas a lograr su modificación o neutralización

En el punto 8.- Procedimientos, se toma en cuenta, entre otros lo siguiente:

a.-. La DITEL solicitará al SECOM y al SINFA, la relación del personal que conformará el Equipo de Especialistas, para la ejecución El COPCE formulará y presentará el Programa Anual de Estimación de Riesgos de Ciberseguridad al COMCA, para su aprobación en el mes de octubre del año anterior a su ejecución. Dicho Programa podrá ser modificado de acuerdo a necesidades del servicio, debidamente autorizado por el COMCAde las estimaciones de riesgos programadas en el año.

b. - El COMCA solicitará a la DITEL la relación del personal de SECOM y al SINFA que conformará el Equipo de Especialistas, para la ejecución de las estimaciones de riesgos programadas en cada año

c.- El COMCA gestionará ante la DIGPE el pago de comisiones, viáticos y pasajes para el equipo multidisciplinario de especialistas de seguridad digital que realizará la estimación de riesgos de ciberseguridad en las UU FAP fuera de Lima y Callao, considerando que la presente estimación está compuesta de evaluaciones que requieren la verificación in situ.

d.- El COMCA, a propuesta del COPCE, pondrá en conocimiento del Comandante/Director de la Unidad a evaluar la siguiente información:

1) Fecha, hora de inicio y tiempo que demandará la realización de la estimación de

riesgos.

2) Plan de trabajo, indicando las áreas o asuntos a tratar.

3) Relación del personal que integrará el equipo de especialistas.

e.- La estimación de riesgos de ciberseguridad comprenderá las siguientes actividades:

1) Identificación de Riesgos.

2) Análisis de Riesgos.

3) Evaluación de Riesgos.

4) Recomendaciones de Tratamiento de Riesgos.

5) Exposición de Resultados del Análisis Situacional al Comandante / Director de Unidad.

6) Conferencia de concientización en ciberseguridad dirigida al Personal Militar y Civil de la Unidad.

7) Elaboración y entrega de los siguientes informes:

a) Informe Ejecutivo: Resumen que resalta de manera puntual, clara y entendible la información, utilizando como contenido una breve introducción, el análisis, conclusiones y las recomendaciones en una extensión máxima de 3 páginas.

b) Informe Técnico: Informe que detallará el análisis realizado, las conclusiones y las recomendaciones para el tratamiento de cada riesgo conforme a la siguiente estructura:

CAPÍTULO I

GENERALIDADES

1.- Resumen

2.- Objetivo

3.- Base Normativa

4.- Equipo de Trabajo

CAPÍTULO II

DESARROLLO DE LA ESTIMACIÓN DE RIESGOS DE CIBERSEGURIDAD

1.- Establecimiento del Contexto

2.- Estimación de Riesgos

a.- Identificación de Riesgos:

1) Área de Informática

Identificación y Tasación de Activos.

2) Área de Comunicaciones

3) Área de Análisis de Vulnerabilidades

Identificación de Amenazas.

Identificación de Vulnerabilidades (de ser aplicable, incluir imágenes de evidencias).

b.- Análisis de Riesgos.

c.- Evaluación de Riesgos.

3.- Recmendaciones para el Tratamiento de los Riesgos

CAPÍTULO III

CONCLUSIONES Y RECOMENDACIONES

1.- Conclusiones

2.- Recomendaciones

ANEXOS

f.- El personal más antiguo del equipo de especialistas, días previos a la visita de inspección, será el encargado de recopilar información necesaria de la Unidad a inspeccionar, la cual pueda enriquecer el informe final; así como orientar la correcta ejecución de la estimación de riesgos.

g.- El equipo de especialistas deberá presentarse al Comandante / Director de la Unidad objeto de la estimación, quien designará a un responsable del área de comunicaciones o informática, y al Oficial de Seguridad para acompañar al equipo y brindar

información relacionada a los riesgos identificados.

h.- El personal especialista del COPCE, realizará el análisis de vulnerabilidades a la infraestructura de red de la Unidad, así como el análisis de vulnerabilidades a los aplicativos y/o sitios web bajo su responsabilidad, si lo tuvieran y la búsqueda de ciberamenazas propias de la Unidad.

i.- El personal especialista del SINFA realizará la verificación física de los equipos de cómputo, de acuerdo al inventario de bienes de la Unidad; asimismo, por ejemplo, verificará la configuración del equipo, que sistema operativo utiliza, si tiene instalado el antivirus institucional y toda aquella información que permita evaluar las vulnerabilidades en los equipos y los posibles riesgos asociados, a fin de determinar los controles a implementar.

j.- El personal especialista del SECOM, evaluará los equipos de comunicaciones como, por ejemplo, la antigüedad que tienen, si el firmware de éstos se encuentra actualizado, operatividad y funcionalidad de los mismos; así como el cableado estructurado de la Unidad.

k.- El COPCE presentará al COMCA los Informes de la estimación de riesgos de ciberseguridad realizadas (ejecutivo y técnico) en las fechas indicadas en el Plan de Trabajo, en formato digital e impreso, para su remisión a la Unidad involucrada.

l.- El COPCE llevará un control de los riesgos identificados por cada Unidad y remitirá esta información conforme al siguiente detalle:

1) Cuadro de control de indicadores de riesgos al COMCA.

2) Informe Ejecutivo y Técnico al COMCA para que sea remitido a la Unidad evaluada.

3) Informe Ejecutivo a la INSPE, para la verificación de los levantamientos de observaciones en sus visitas programadas.

m.- Las UU FAP inspeccionadas, coordinarán si fuera necesario con el COPCE, SINFA y SECOM, para la implementación de las recomendaciones e informarán al COMCA e INSPE, las acciones realizadas para subsanar las deficiencias encontradas.

CAPÍTULO III
MARCO TEÓRICO REFERENCIAL

MARCO TEÓRICO REFERENCIAL

3.1. Marco teórico

El siguiente marco teórico ha sido considerado para mejor entendimiento del presente trabajo en la modalidad de informe de suficiencia profesional.

3.1.1. Ciberespacio

Según el DOFA 1-4 (2016, p. 3-5), manifiesta que el ciberespacio es un dominio. Las operaciones del ciberespacio no son un sinónimo de las Operaciones de Información (IO). Las IO son un conjunto de operaciones que se pueden realizar en el ciberespacio y otros dominios. Las operaciones en el ciberespacio pueden apoyar directamente a las IO, pero las IO no cibernéticas pueden afectar las operaciones del ciberespacio. El ciberespacio es un dominio establecido por el hombre y es por lo tanto, un dominio distinto de aquellos naturales como son el aire, tierra y mar.

Requiere una atención continua de parte de los seres humanos para adaptarse a las características de especificidad, alcance global y particularidades del espectro electromagnético. Los Nodos del ciberespacio residen físicamente en todos los ámbitos. Las actividades en el ciberespacio, pueden permitir la libertad de acción para realizar actividades en los otros dominios, y las actividades en los otros dominios pueden crear efectos en y a través del ciberespacio.

A pesar que las redes en el ciberespacio son interdependientes, parte de estas redes pueden quedar aisladas. El aislamiento del ciberespacio se puede lograr a través de protocolos, firewalls, encriptación y la separación física del resto de las redes. Por ejemplo, las redes clasificadas de las Fuerzas Armadas no están conectadas en todo momento a Internet, pero cada vez que lo hacen lo realizan a través de puertos seguros. La construcción de algunas redes cableadas de manera específica, minimiza la mayoría de las formas de interferencia por radiofrecuencia. Estos factores permiten que estas redes no queden aisladas del ciberespacio y con eso garantizan su conectividad con las redes globales.

Segmentos del ciberespacio están conectados y apoyados por infraestructuras físicas, sistemas electrónicos y porciones del espectro electromagnético (EMS). Los sistemas e infraestructuras evolucionan rápidamente debido a que los usuarios necesitan una mayor capacidad y velocidad de procesamiento de datos, por lo tanto, se exige el uso de porciones cada vez mayores del EMS y el uso de un mayor ancho de banda. Los sistemas suelen ser diseñados para cambiar las frecuencias en las que operan dentro del EMS, para evitar la manipulación de datos.

La maniobrabilidad lógica en el ciberespacio es a menudo una función de los protocolos de seguridad utilizados por los sistemas “Host”. Los sistemas que intentan conectarse a un Host seguro tendrán muchas más dificultades para acceder a la información de ésta, respecto de aquellos que están conectados a Hosts inseguros. Además, la defensa contra sistemas no deseados que intentan entrar se encuentra fundamentalmente en los códigos o la lógica de los sistemas Host. Una vez que la conexión es establecida, cualquier intruso puede explotar una falla en la lógica para ingresar permanentemente en el sistema y maniobrar en ella.

La escritura de los códigos de seguridad puede ser una forma de maniobra lógica en el ciberespacio. El potencial intruso puede crear un código para obtener maniobrabilidad frente a los sistemas de destino.

Esto puede resultar muy peligroso ya que mientras que el defensor se da cuenta de la presencia no deseada de un intruso dentro de su sistema, éste ya puede haber alterado el código de entrada del mismo, incluso para impedir el ingreso de los normales usuarios. El intruso que desee permanecer en el sistema instala su código y accede cuando lo desea.

Este proceso es el equivalente a las fuerzas que maniobran para ganar posiciones de ventaja en los ambientes tradicionales de aire, tierra, espacio y marítimos. Los espacios de maniobra lógica y física son necesarios ambos; uno es a menudo inútil sin el otro.

3.1.2. Amenazas a las Operaciones en el Ciberespacio

La DOFA 1-4 (2016, p. 13), manifiesta que, en otros ámbitos, las principales amenazas a la Seguridad Nacional provienen de Estados-Nación o actores transnacionales tales como organizaciones terroristas. Grandes recursos de capital y de personal son necesarios para construir, posicionar, mantener y operar naves, aviones de combate y satélites, pero tan sólo una pequeña organización y con herramientas sencillas pueden hacer volar en pedazos estructuras y organizaciones enteras.

Los adversarios buscan ventajas asimétricas y el ciberespacio ofrece oportunidades significativas para su obtención. Hay una gran variedad de amenazas a las operaciones del ciberespacio. Estas amenazas y otras deben ser consideradas cuando se realizan las operaciones del ciberespacio, que son: Nación-Estado, Amenaza Transnacional, Organización Criminal, Grupos pequeños o Individuales, Amenazas Tradicionales, Amenaza Irregular, Amenaza Catastrófica, Amenaza Interruptora, Amenaza Natural, Amenaza Accidental.

3.1.3. Poder Militar Aeroespacial

La DBFA 1 (2021, p. 8), indica que el Poder Militar Aeroespacial, es la capacidad que posee un Estado, de emplear los medios que tienen las Fuerzas Armadas en el aire, espacio y ciberespacio, para contribuir con la Seguridad y Defensa Nacional. La Fuerza Aérea del Perú lidera el Poder Militar Aeroespacial. Asimismo, los dominios que configuran el Poder Militar Aeroespacial son los siguientes: dominio aéreo, domino espacial y dominio ciberespacial.

3.1.4. Potencial Militar Aeroespacial

La DBFA 1 (2021, p. 9), manifiesta que el Potencial Militar Aeroespacial, es la capacidad futura que posee un Estado, de emplear los medios que tienen las Fuerzas Armadas en el aire, espacio y ciberespacio, para contribuir con la Seguridad y Defensa Nacional. Considera como parte de sus elementos a la reserva aérea; así como la infraestructura y la industria militar aeronáutica, espacial y ciberespacial.

3.1.5. Dominios del Poder Militar Aeroespacial

La DBFA 1 (2021, p. 10), indica que los Dominios del Poder Militar Aeroespacial, son construcciones útiles para visualizar y caracterizar el entorno físico (terrestre, marítimo, aéreo, espacial) y no físico (ciberespacial) en el que se realizan las operaciones y acciones militares; tienen características propias diferenciadas, que condicionan las aptitudes y procedimientos de los medios, fuerzas y capacidades que deben operar en ellos. Los dominios en los cuales la Fuerza Aérea del Perú, como líder del Poder Militar Aeroespacial, realiza sus operaciones y acciones militares, son el dominio aéreo, el dominio espacial y el dominio ciberespacial. Asimismo, el domino ciberespacial es "un dominio global artificial dentro del entorno de información que consiste en la red interdependiente de infraestructuras de tecnología de la información, que incluye internet, redes de telecomunicaciones, sistemas informáticos, así como procesadores y controladores integrados". Este dominio actúa de manera transversal a los demás dominios.

3.1.6. Poder Ciberespacial

La DBFA 1 (2021, p. 46), manifiesta que el Poder Ciberespacial se refiere a la capacidad de un Estado de utilizar los medios tecnológicos a través de señales digitales en forma ofensiva o defensiva en el dominio ciberespacial, para crear ventajas operacionales e influenciar en los otros dominios operacionales.

3.1.7. Control Ciberespacial

La DBFA 1 (2021, p. 79), indica que el Control Ciberespacial, es la capacidad para controlar toda acción en el ciberespacio propio, o asignado, que contribuya a la libertad de acción de las fuerzas propias y amigas, independientemente del domino en el que estas operen. Siendo las operaciones de este dominio: a) Operaciones Defensivas, b) Operaciones de Explotación y c) Operaciones de Respuesta.

3.1.8. Apoyo y sostenimiento a las operaciones ciberespaciales

La DBFA 1 (2021, p. 90), manifiesta que el Apoyo y sostenimiento a las operaciones ciberespaciales, es la capacidad de procesar la información obtenida en y mediante el ciberespacio propio o asignado.

3.1.9. Política Nacional del Ciberespacio

La DOFA 1-4 (2016, p. 7), manifiesta que, la Seguridad Cibernética Nacional consiste de un número de iniciativas que se refuerzan mutuamente con el objetivo principal de asegurar el ciberespacio del Estado para:

- Establecer una línea de defensa contra las amenazas inmediatas de hoy en día, mediante la creación o la mejora de la conciencia situacional de las vulnerabilidades de la red, las amenazas y los eventos del Gobierno y tener la capacidad de actuar con rapidez para reducir nuestra vulnerabilidad actual y prevenir intrusiones.
- Defenderse contra todo el espectro de amenazas a través de la mejora de capacidades nacionales de contrainteligencia y el incremento de la seguridad en la cadena de suministros de tecnologías de información clave.
- Fortalecer la seguridad del ambiente futuro cibernético, mediante la educación cibernética, la coordinación y la reorientación de los esfuerzos de investigación y desarrollen todo el Estado, para definir y desarrollar estrategias que disuadan la actividad hostil maliciosa en el ciberespacio.

Sea como fuere, la ciberseguridad es uno de los más grandes desafíos a la Seguridad Nacional que enfrentamos hoy en día como nación, pero nosotros, como gobierno o como país, aun no estamos adecuadamente preparados para contrarrestar las amenazas existentes, por lo que se debe ordenar una revisión exhaustiva de los esfuerzos nacionales, para determinar el grado en el cual podemos defender la información y la infraestructura de comunicaciones, a través del desarrollo de un enfoque integral para asegurar la infraestructura digital del Estado.

Se deben aceptar todas las recomendaciones en cuanto a la política nacional para empleo del ciberespacio y que considere una estrecha colaboración con todos los actores claves en la ciberseguridad nacional incluyendo a los gobiernos regionales y al sector privado para:

- Asegurar una respuesta organizada y unificada que nos permita enfrentarlos futuros incidentes ciberespaciales.
- Fortalecer las alianzas público/privadas.
- Encontrar soluciones tecnológicas que garanticen la seguridad del Estado y el desarrollo.
- Invertir en investigación y desarrollo para la innovación y poder afrontar los retos digitales de nuestro tiempo.
- Iniciar una campaña de sensibilización sobre la seguridad cibernética.

3.1.10. Organización de las Operaciones en el Ciberespacio

La DOFA 1-4 (2016, p. 21), manifiesta que, la Fuerza Aérea organiza, entrena y equipa a sus fuerzas cibernéticas para apoyar a los Comandos Operacionales. Las fuerzas conjuntas del ciberespacio son una parte integral de las operaciones militares y las relaciones de comando son cruciales para garantizar el empleo eficaz y oportuno. El personal del Estado Mayor Conjunto planea y ejecuta las operaciones militares y del ciberespacio, además tienen la responsabilidad de establecer prioridades, evitar conflictos, integrar y sincronizar las operaciones militares del ciberespacio con las operaciones conjuntas en curso y previstas.

Las operaciones del ciberespacio se ejecutan: a.- Nivel Estratégico, b.- Nivel Operacional, c.- Comando de la Fuerza Aérea en el Ciberespacio, d.- Organizaciones ISR de la Fuerza Aérea.

3.2. Términos básicos

Para el presente trabajo, ha considerado los términos básicos que contiene el anexo B de la Ordenanza FAP 185–5 (2018), que son los siguientes:

Amenaza. - Causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

Amenaza Cibernética. - Factor externo representado por la posibilidad que ocurra un fenómeno o un evento adverso en el ciberambiente de interés, en un momento, lugar específico, con una magnitud determinada y que podría ocasionar daños a las personas o a las instalaciones o medios TIC; la pérdida de personal o medios de vida o trastornos al empleo del Instrumento Militar u Objetivos de Valor Estratégico nacionales.

Ambiente de la Información. - Conjunto de individuos, organizaciones y sistemas que recogen, procesan, difunden o actúan sobre la información.

Análisis del Riesgos. - Implica desarrollar una comprensión de riesgo. El análisis del Riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados.

Ataque Cibernético. - Agresión cibernética voluntaria cuya finalidad es la de destruir, exponer, alterar, degradar, inhabilitar o dominar una infraestructura.

Ciberdefensa. - Conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler una amenaza o agresión cibernética, sea esta inmediata, latente o potencial, a fin de permitir el empleo del instrumento Militar de la Nación.

Ciberdelincuencia. - Actividades delictivas llevadas a cabo mediante el empleo del ciberespacio, ya sea para dirigirlas hacia los sistemas y servicios presentes en el mismo o alcanzables a través suyo.

Ciberespacio. - Dominio global dentro del ambiente de la información consistente de una red interdependiente de infraestructura tecnológica de la información que incluye a la internet, las redes de telecomunicaciones, sistemas informáticos junto con los procesadores y controladores asociados. El ciberespacio es un ámbito que requiere del hombre para entrar y explotar dicha tecnología. La única diferencia es que es más fácil de ver y sentir que en los otros dominios. Al igual que con el aire y el espacio, los efectos de las operaciones del ciberespacio pueden ocurrir simultáneamente en muchos lugares. Pueden ser más precisos, amplios, permanentes y transitorios.

Ciberseguridad. - Acciones comprendidas dentro de la seguridad de la información, en la cual se busca garantizar la confidencialidad, integridad y disponibilidad de los activos de la información digital y de la infraestructura que la soporta.

Delitos Informáticos. - Conducta ilícita que afecta los sistemas y los datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de la TI o de la Comunicación.

Evaluación de Riesgos. - En base a los resultados del análisis del riesgo la finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad para implementar el tratamiento.

Gestión de Riesgos en Ciberseguridad. - Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo. La gestión de riesgos usualmente incluye la evaluación

de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

Identificación de Riesgos. - Identificación de los orígenes de riesgo, las áreas de impactos, los sucesos (incluyendo los cambios de circunstancias), así como sus causas y sus consecuencias potenciales. El objetivo de esta etapa consiste en generar una lista de riesgos exhaustiva basada en aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos.

Malware. - Softwares tales como virus y troyanos diseñados para causar daño o interrupción a un sistema de cómputo.

Operaciones del Ciberespacio. - Es el empleo de las capacidades cibernéticas donde el objetivo principal es lograr objetivos en o a través del ciberespacio. Estas operaciones incluyen las operaciones de redes informáticas y actividades para operar y defender la Red de Información.

Política de Seguridad de la Información. - Es un documento de alto nivel que denota el compromiso de la alta gerencia con la seguridad de la información. Contiene la definición de la Seguridad de la Información bajo el punto de vista de cierta entidad. Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos. Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad.

Riesgo. - Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

Seguridad Digital. - Estado de confianza en el entorno digital que resulta de la gestión y aplicación de los conjuntos de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Seguridad de la Información. - Medidas para proteger y defender la información y sistemas de información asegurando su disponibilidad, integridad, autentificación, secreto y no rechazo. Esto incluye prever la restauración de los sistemas de información incorporando capacidades para la protección, la detección y de reacción.

Tecnología de la Información. - Conjunto de herramientas que se utilizan para la administración y tratamiento de la información. Estas herramientas pueden incluir cualquier dispositivo de comunicaciones o la computadora, sus equipos auxiliares, aplicaciones de software y los recursos de apoyo.

Tratamiento de Riesgos. - Implica la selección y la implementación de una o varias opciones para modificar los riesgos.

CAPÍTULO IV

SUPUESTOS DE SOLUCIÓN

SUPUESTOS DE SOLUCION

Realizado el diagnóstico situacional en base al análisis de la información, se manifiesta que en la actualidad se cuenta con una normativa que detalla y norma lineamientos de Ciberseguridad ante amenazas de redes en la FAP en cumplimiento de la misión y visión institucional; pero a la fecha no existe un documento que describa en detalle las redes de amenazas en la institución, ello como un elemento de mejora a nivel de las operaciones de Ciberseguridad y Ciberdefensa en la FAP, por lo que es necesario la implementación de un documento general que manifieste los lineamientos y características de las Redes de Amenazas en la FAP para el adecuado desarrollo de las actividades informáticas en la Fuerza Aérea del Perú.

En tal sentido, es necesario que, en la presente investigación, se considere los conocimientos metodológicos para el desarrollo adecuado de los supuestos de solución existentes y nos sirva de referencia para una adecuada propuesta. En tal sentido, se ha considerado al manual ESFAP 50-1 (2021), que da los lineamientos teóricos para abordar en una mejor medida una investigación científica.

Se considera a los paradigmas de investigación, como elementos que sirven de marco para la comprensión de los fenómenos de la realidad; brindan una guía para abordar cuestiones y problemáticas; otorgan, dentro de un esquema de criterios, las técnicas apropiadas y la epistemología coherente para abordar situaciones emergentes. Los paradigmas de investigación son: Paradigma positivista, Paradigma Interpretativo y Paradigma pragmático. Asimismo, el Paradigma positivista, se ubica dentro de la teoría positivista; plantea la posibilidad de llegar a verdades absolutas en la medida en que se abordan los problemas y se establece una distancia significativa entre el investigador y el objeto de estudio (p. 14)

Los tipos de Investigación son dos, que cumplen los siguientes propósitos fundamentales: a) Investigación básica: Produce conocimientos y teorías; b) Investigación aplicada: Busca Resolver problemas.

Respecto a los enfoques de la investigación, se consideran tres enfoques, siendo: a) El enfoque cuantitativo, b) El enfoque cualitativo y c) El enfoque Mixto. El enfoque cuantitativo, utiliza la recolección de datos para probar una hipótesis con base en la medición numérica y el análisis estadístico, a fin de establecer pautas de comportamiento y probar

teorías (p. 18).

Respecto a los alcances de la investigación, se consideran los siguientes alcances de investigación: a) Estudios exploratorios, b) Estudios descriptivos, c) Estudio correlacional y d) Estudios explicativos. Los estudios descriptivos, buscan especificar las propiedades importantes de personas, grupos comunidades o cualquier otro fenómeno que sea sometido análisis, es decir, buscan saber quién, dónde, cuándo, cómo y porqué del sujeto de estudio, y principalmente miden o evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. En un estudio descriptivo se selecciona una serie de cuestiones y se mide cada una de ellas independientemente, para así describir lo que se investiga (p. 21)

El diseño y corte de la investigación, constituye el Plan o estrategia que se desarrolla para obtener la información que se requiere en una investigación y responder al planteamiento. Para los estudios cuantitativos: 1) Experimentales y 2) No experimentales. Siendo los diseños No experimentales: Diseño transaccional o transversal y Diseño longitudinal (p. 22)

Para poder obtener datos, es necesario saber quiénes proveerán la información, por lo que es necesario definir la población y muestra. La Población, es un conjunto de todos los casos que concuerdan con determinadas especificaciones. La Muestra es un Subgrupo o subconjunto propio de la población del cual se recolectan los datos y que debe ser representativo de esta. La Muestra son de dos tipos: 1) Muestra probabilística y 2) Muestra no probabilística o dirigida Las Muestra probabilística, son un Subgrupo de la población en el que todos los elementos tienen la misma posibilidad de ser elegidos. Pueden ser: Aleatorio simple, Aleatoria sistemática y Aleatoria estratificada (p. 23)

Para determinar la muestra aleatoria simple se aplica comúnmente la ecuación:

$$n = \frac{z^2 * p * q * N}{(N-1) * E^2 + z^2 * p * q}$$

Dónde: n = tamaño de muestra, z = nivel de confianza (Z= 1,96), p = porcentaje de ocurrencia probable, q = porcentaje de no ocurrencia probable (1-p), N = tamaño de la población y e = error máximo permitido (5%)

Respecto a las técnicas e instrumentos de investigación, las técnicas son procedimientos sistematizados, operativos que sirven para la solución de problemas

prácticos. Las técnicas deben ser seleccionadas teniendo en cuenta lo que se investiga, porque, para qué y cómo se investiga. Las técnicas son: encuesta, cuestionario y el censo. (p. 23). Los instrumentos son medios auxiliares para recoger y registrar los datos obtenidos a través de las técnicas y pueden ser: Guía de Observación, Ficha de Observación; Guía de Entrevista, Cuestionario de Entrevista; Guía de Análisis de Documentos; Escalas Tipo Likert, Diferencial Semántico; Test; Cuestionario (p. 24).

En lo que respecta a las técnicas de procesamiento y análisis de datos. Se especifican como van a ser tratados, analizados e interpretados los datos. Siendo las más usuales: a) Tablas de frecuencia, b) Tablas cruzadas, c) Gráficos y d) Estadísticos (p. 25).

CAPÍTULO V

PROPUESTAS DE SOLUCIÓN

PLANTEAMIENTO DE LA PROPUESTA DE SOLUCIÓN

Para el presente informe de suficiencia profesional, se ha propuesto que la investigación fuera bajo el paradigma positivista con el objeto de dar respuesta a nuestro problema bajo el uso y aplicación de técnicas adecuadas para contrarrestar las redes de amenazas. Además, la investigación será bajo un enfoque cuantitativo, porque se utilizó herramientas estadísticas como frecuencia y porcentajes para medir nuestra variable de estudio. En lo que respecta al tipo de investigación, fue de tipo aplicado porque, se identificó los lineamientos para solución actual a nuestro problema centrado en un contexto específico de la vulnerabilidad y las amenazas de las redes institucionales. En lo respecta al diseño, se aplicó el diseño no experimental, dado que no se realiza experimentos. La recolección de datos es realizada en un único momento al aplicar la técnica encuesta con su instrumento cuestionario.

En lo que respecta a la población, fue conformada por el personal de Oficiales y técnicos con experiencia en Informática de la FAP que están destacados en la Región Lima, que son en aproximación 37 personas. Asimismo, la muestra es determinada por la ecuación:

$$n = \frac{z^2 * p * q * N}{(N-1) * E^2 + z^2 * p * q}$$

En donde, n es el tamaño de la muestra a ser determinado, z=1,96 (nivel de confianza para α=0.05), p=0,5 o 50% que corresponde a la proporción de la población, sabiendo que p+q=1, q que es 0,5 o 50%, N=37 y E = 0.05 (Siendo el 5%).

Se realiza el cálculo de la muestra utilizando la ecuación, se reemplaza los valores y se obtiene:

$$n = \frac{1{,}96^2 * 0{,}95 * 0{,}05 * 37}{(37-1) * 0{,}05^2 + 1{,}96^2 * 0{,}95 * 0{,}05} = 33{,}83$$

Dado que la ecuación nos arroja un valor muestral de 33,83, se cree conveniente para el trabajo, decidir un valor de muestra de 34 personas entre oficiales y técnicos con experiencia en Informática de la FAP, por lo que podríamos tomar a los 37 especialistas dado que el número es muy cercano.

La técnica aplicada para la recolección de datos, es la encuesta y el instrumento realizado es un cuestionario de escala que utilizaremos para recolectar la información sobre el estado actual de la doctrina, normas y documentos operativos en Ciberseguridad e informática.

En lo que respecta al tratamiento de datos se ha utilizado el software M.S. Excel para

establecer las frecuencias y porcentajes, que luego serán presentados en figuras.

La información obtenida, luego de aplicar el instrumento, contribuye a los lineamientos adecuados para la realización de las operaciones de ciberseguridad y defensa ante redes de amenazas en la FAP. Lo que implica contar con un documento actualizado que contenga los lineamientos generales que permitan al personal de la FAP, tener un instrumento o herramienta para llevar a cabo una correcta capacitación y adaptación de las actividades que describe, a fin de optimizar el uso de los recursos informáticos en ciberseguridad.

La propuesta se realiza en dos etapas: La primera etapa está referida en determinar el estado actual de la doctrina, base legal y las operaciones en ciberseguridad que se tiene a nivel institucional, ello mediante la aplicación de una encuesta al personal de Oficiales y técnicos con una vasta experiencia en informática y ciberseguridad que como muestra es de 37 personas, los que conocen directamente sobre el trabajo en redes, algoritmos y amenazas cibernéticas en la FAP. La segunda etapa está referida a la propuesta del "Manual para contrarrestar las Redes de Amenazas en la FAP". Dicho documento está descrito en el Anexo II.

CAPITULO VI

RESULTADOS

RESULTADOS

El presente capítulo, describe los resultados obtenidos de la encuesta realizada. Para ello se detallará primeramente en forma de tablas y figuras, que indican los resultados de las preguntas de la encuesta con su instrumento aplicado, por lo que se ha confeccionado una encuesta estructurada - Anexo "I", que ayudará a identificar la necesidad de contar con los lineamientos bases para el documento "Manual para contrarrestar las Redes de Amenazas en la FAP".

6.1 Trabajo de Campo: Encuestas.

Con relación a la encuesta estructurada realizada al personal oficial y técnicos, se manifiesta que dicha encuesta fue aplicada a la muestra designada que fueron 37 personas. El personal que conformó la muestra fue militar con experiencia en trabajo en redes, algoritmos y amenazas cibernéticas en la FAP. Por lo que se ha podido obtener los siguientes resultados:

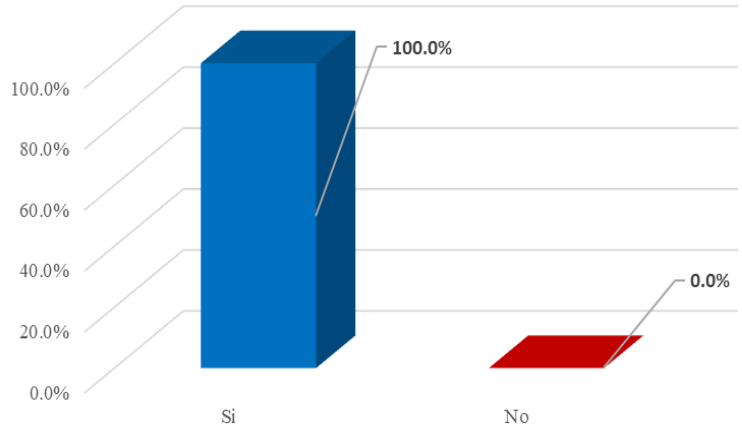
Respecto a la pregunta N 1: Se formula de la siguiente manera: ¿Usted, considera que, es importante la base legal de Ciberseguridad y Ciberdefensa?

El 100,0% del personal encuestado, manifestaron que, si consideran importante a la base legal de Ciberseguridad y Ciberdefensa. Lo que indica un alto compromiso por la legalidad en Ciberseguridad y Ciberdefensa.

En la figura 4, se presenta los datos a la pregunta N 1 en forma de barras en 3D.

Figura 4

Resultado de la encuesta respecto a la pregunta N 1.



Respecto a la pregunta N 2: Se formula de la siguiente manera: ¿Usted, considera que, la doctrina institucional vigente es adecuada para la Ciberseguridad y Ciberdefensa?

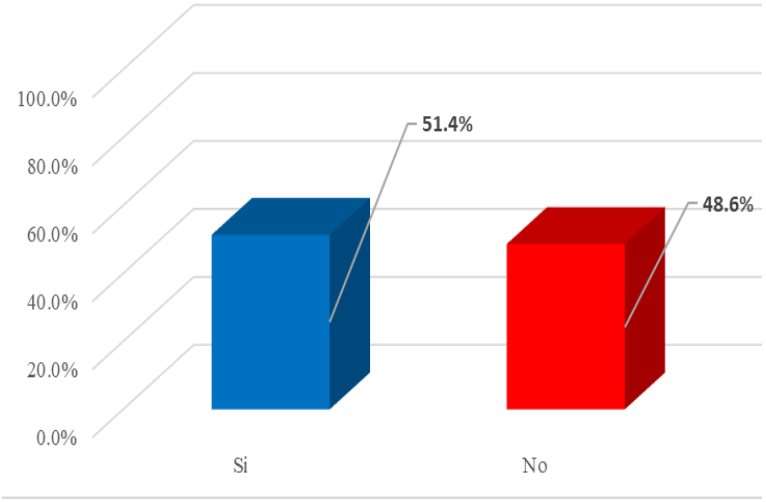
El 51,4% del personal encuestado, manifestaron que, si consideran que la doctrina institucional vigente es adecuada para la Ciberseguridad y Ciberdefensa. Asimismo, el

48,6% de los encuestados, no la considera adecuada.

En la Figura 5, se presenta los datos a la pregunta N 2 en forma de barras en 3D.

Figura 5

Resultado de la encuesta respecto a la pregunta N 2



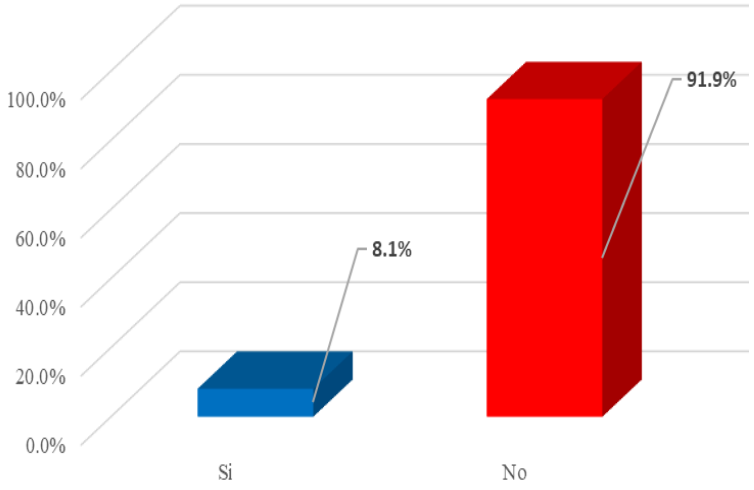
Respecto a la pregunta N 3: Se formula de la siguiente manera: ¿Usted, considera que la institución, ha implementado de manera adecuada el contrarrestar las redes de amenazas?

El 91,9% del personal encuestado, manifestaron que, no consideran que la institución, ha implementado de manera adecuada el contrarrestar las redes de amenazas. Asimismo, el 8,1% de los encuestados, considera que si se ha implementado de manera adecuada.

En la Figura 6, se presenta los datos a la pregunta N 3 en forma de barras en 3D.

Figura 6

Resultado de la encuesta respecto a la pregunta N 3



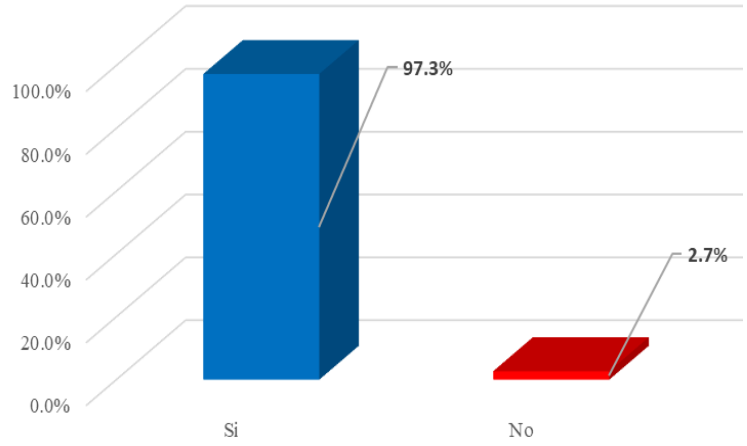
Respecto a la pregunta N 4: Se formula de la siguiente manera: ¿Usted, considera que, la institución está en la capacidad de implementar un documento para contrarrestar las redes de amenazas?

El 97,3% del personal encuestado, consideran que, la institución si está en la capacidad de implementar un documento para contrarrestar las redes de amenazas. Asimismo, el 2,7% de los encuestados, considera que no se está en la capacidad.

En la Figura 7, se presenta los datos a la pregunta N 4 en forma de barras en 3D.

Figura 7

Resultado de la encuesta respecto a la pregunta N 3

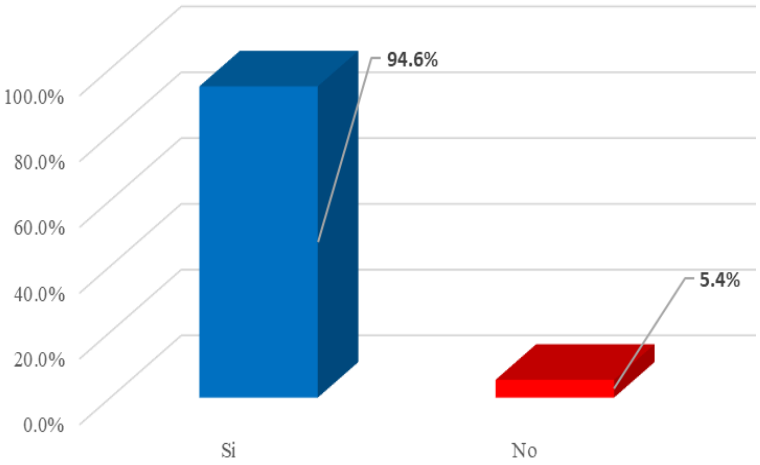


Respecto a la pregunta N 5: Se formula de la siguiente manera: ¿Usted, considera que, a nivel de Ciberdefensa y para fortalecer la misión institucional sea necesaria la implementación de un sistema para contrarrestar las redes de amenazas?

En la Figura 8, se presenta los datos a la pregunta N 5 en forma de barras en 3D.

Figura 8

Resultado de la encuesta respecto a la pregunta N 5



El 94,6% del personal encuestado, manifestaron que, si consideran que a nivel de Ciberdefensa y para fortalecer la misión institucional es necesaria la implementación de un sistema para contrarrestar las redes de amenazas. Asimismo, el 5,4% de los encuestados, considera que no es necesaria. El personal comprende que el tópico es de importancia para las operaciones de apoyo ante incendios forestales.

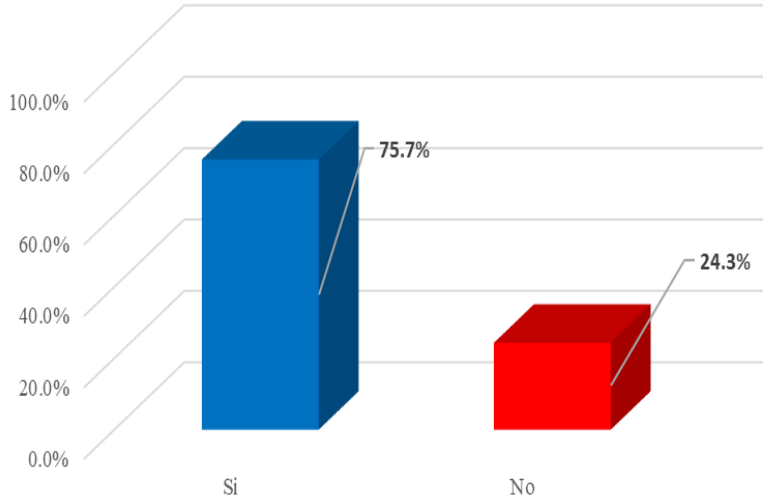
Respecto a la pregunta N 6: Se formula de la siguiente manera: ¿Usted, considera que, a nivel administrativo, la implementación para contrarrestar las redes de amenazas en las UU.DD FAP sería eficiente en vías de la modernización del Estado?

El 75,7% del personal encuestado, si consideran que, a nivel administrativo, la implementación para contrarrestar las redes de amenazas en las UU.DD FAP sería eficiente en vías de la modernización del Estado. Asimismo, el 24,3% de los encuestados, considera que no sería eficiente.

En la Figura 9, se presenta los datos a la pregunta N 6 en forma de barras en 3D.

Figura 9

Resultado de la encuesta respecto a la pregunta N 6



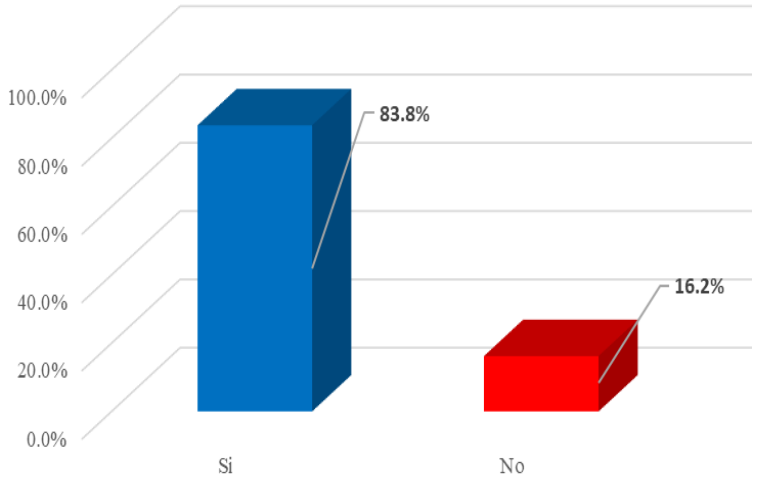
Respecto a la pregunta N 7: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando el entorno de seguridad?

El 83,8% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando el entorno de seguridad. Asimismo, el 16,2% de los encuestados, indica que no sea considerado.

En la Figura 10, se presenta los datos a la pregunta N 7 en forma de barras en 3D.

Figura 10

Resultado de la encuesta respecto a la pregunta N 7



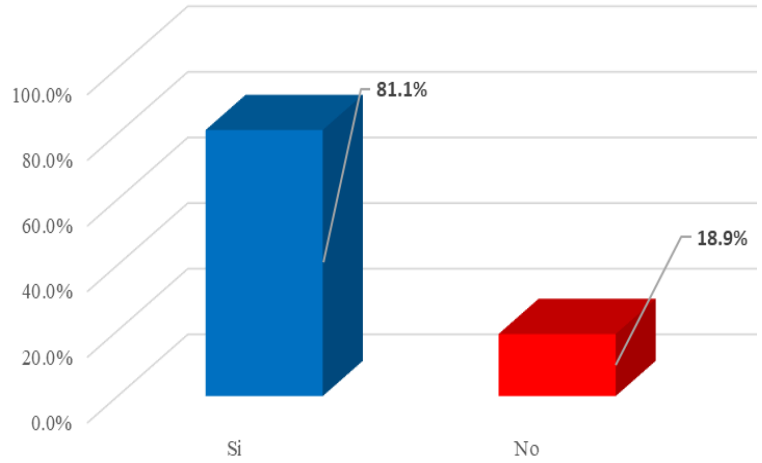
Respecto a la pregunta N 8: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando los fundamentos de las redes de amenazas?

El 81,1% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando los fundamentos de las redes de amenazas. Asimismo, el 18,9% de los encuestados, indica que no sea considerado.

En la Figura 11, se presenta los datos a la pregunta N 8 en forma de barras en 3D.

Figura 11

Resultado de la encuesta respecto a la pregunta N 8



Respecto a la pregunta N 9: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado

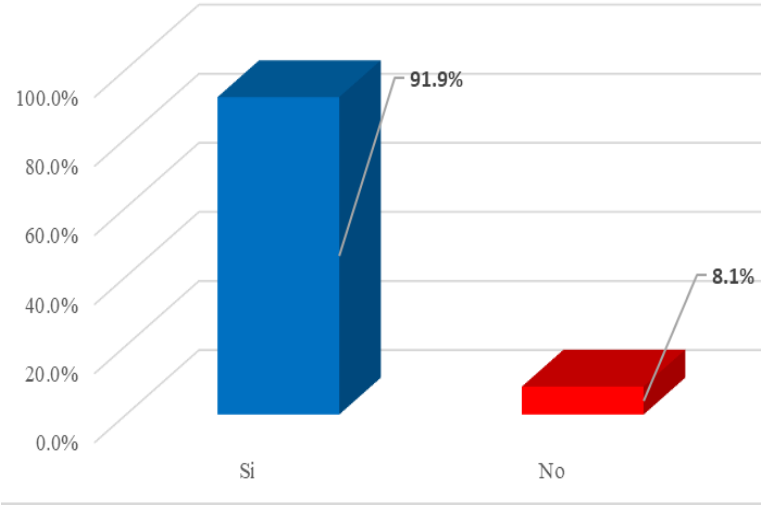
considerando las redes en el entorno operativo?

El 91,9% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las redes en el entorno operativo. Asimismo, el 8,1% de los encuestados, indica que no sea considerado.

En la Figura 12, se presenta los datos a la pregunta N 9 en forma de barras en 3D.

Figura 12

Resultado de la encuesta respecto a la pregunta N 9

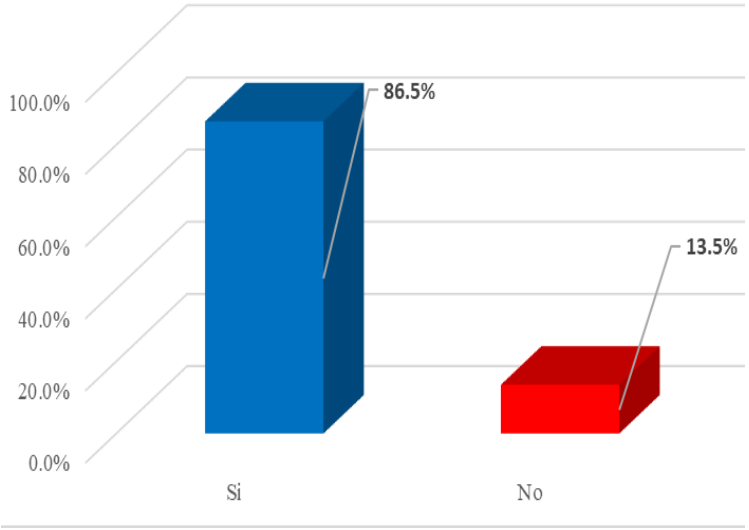


Respecto a la pregunta N 10: Se formula de la siguiente manera ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando planificación para contrarrestar las redes de amenazas?

En la Figura 13, se presenta los datos a la pregunta N 10 en forma de barras en 3D.

Figura 13

Resultado de la encuesta respecto a la pregunta N 10



El 86,5% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando planificación para contrarrestar las redes de amenazas. Asimismo, el 13,5% de los encuestados, indica que no sea considerado.

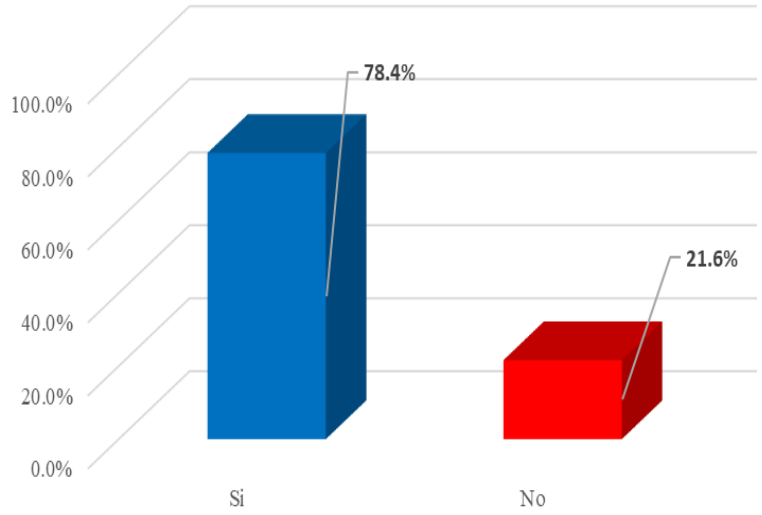
Respecto a la pregunta N 11: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando actividades para contrarrestar las redes de amenazas?

El 78,4% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando actividades para contrarrestar las redes de amenazas. Asimismo, el 21,6% de los encuestados, indica que no sea considerado.

En la Figura 14, se presenta los datos a la pregunta N 11 en forma de barras en 3D.

Figura 14

Resultado de la encuesta respecto a la pregunta N 11



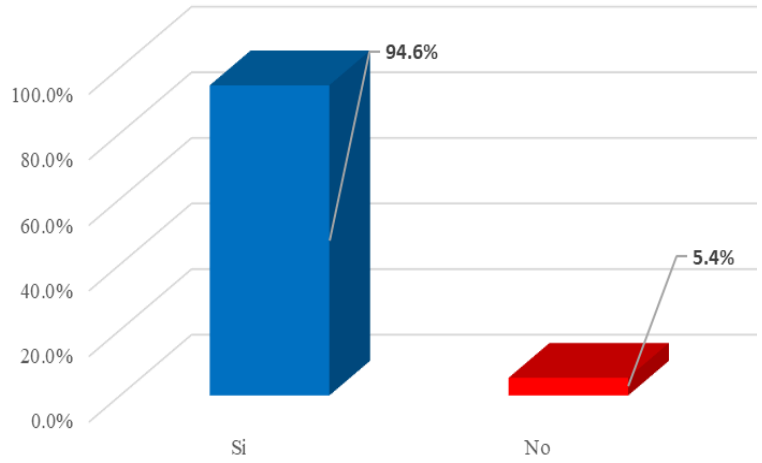
Respecto a la pregunta N 12: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las evaluaciones para contrarrestar las redes de amenazas?

El 94,6% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las evaluaciones para contrarrestar las redes de amenazas. Asimismo, el 5,4% de los encuestados, indica que no sea considerado.

En la Figura 15, se presenta los datos a la pregunta N 12 en forma de barras en 3D.

Figura 15

Resultado de la encuesta respecto a la pregunta N 12



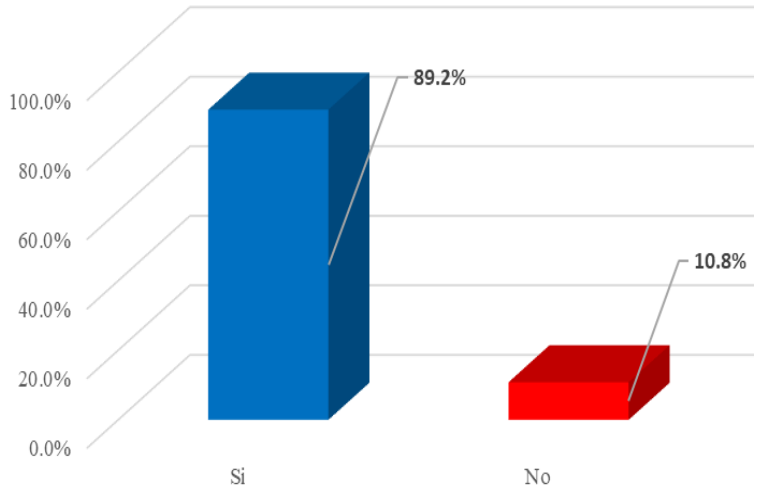
Respecto a la pregunta N 13: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las características clandestinas de las redes de amenazas?

El 89,2% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las características clandestinas de las redes de amenazas. Asimismo, el 10,8% de los encuestados, indica que no sea considerado.

En la Figura 16, se presenta los datos a la pregunta N 13 en forma de barras en 3D.

Figura 16

Resultado de la encuesta respecto a la pregunta N 13



Respecto a la pregunta N 14: Se formula de la siguiente manera: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado

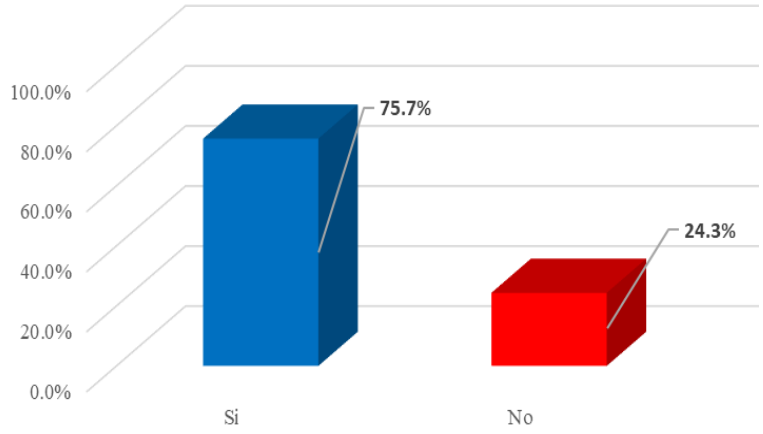
considerando el entorno operativo de las redes de amenazas?

El 75,7% del personal encuestado, si consideran que la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando el entorno operativo de las redes de amenazas. Asimismo, el 24,3% de los encuestados, indica que no sea considerado.

En la Figura 17, se presenta los datos a la pregunta N 14 en forma de barras en 3D.

Figura 17

Resultado de la encuesta respecto a la pregunta N 14



CAPÍTULO VII

CONCLUSIONES

CONCLUSIONES

En base al diagnóstico situacional y a la encuesta aplicada, se ha tenido pertinente plantear las siguientes conclusiones:

PRIMERA CONCLUSIÓN: Se concluye que, basado en el diagnóstico situacional a nivel doctrinarios, legales y operativo, se establecen que la FAP debe mantener la seguridad de la nación y entre las tareas se encuentra, la lucha contra las amenazas a las redes institucionales como parte de la ciberseguridad y ciberdefensa; además, se establecen los lineamientos para las operaciones del ciberespacio, la estimación de riesgos de ciberseguridad y los delitos informáticos con los que debe cumplir las instituciones como la FAP.

SEGUNDA CONCLUSIÓN: Se concluye que, el personal encuestado en un 100,0%, consideran importante a la base legal de Ciberseguridad y Ciberdefensa; el 51,4%, si consideran que la doctrina institucional vigente es adecuada para la Ciberseguridad y Ciberdefensa; el 91,9% no consideran que la institución, ha implementado de manera adecuada el contrarrestar las redes de amenazas; el 97,3% consideran que, la institución si está en la capacidad de implementar un documento para contrarrestar las redes de amenazas; el 94,6%, si consideran que a nivel de Ciberdefensa y para fortalecer la misión institucional es necesaria la implementación de un sistema para contrarrestar las redes de amenazas; y el 75,7%, si consideran que, a nivel administrativo, la implementación para contrarrestar las redes de amenazas en las UU.DD FAP sería eficiente en vías de la modernización del Estado.

TERCERA CONCLUSIÓN: Se concluye que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando el entorno de seguridad en un 83,8%; los fundamentos de las redes de amenazas en un 81,1%; las redes en el entorno operativo en un 91,9%; la planificación para contrarrestar las redes de amenazas en un 86,5%; las actividades para contrarrestar las redes de amenazas en un 78,4%; las evaluaciones para contrarrestar las redes de amenazas en un 94,6%; las características clandestinas de las redes de amenazas en un 89,2%; y el entorno operativo de las redes de amenazas en un 75,7%.

CUARTA CONCLUSIÓN: Se concluye que, existe un alto compromiso por parte del personal de Oficiales por la mejora de los sistemas en la institución, por lo que la propuesta de “MANUAL PARA CONTRARRESTAR LAS REDES DE AMENAZAS EN LA FAP”, nos indica sobre el adecuado nivel de preparación profesional de los oficiales de

la especialidad de ingeniería de sistemas.

QUINTA CONCLUSIÓN: Se concluye que, el personal de oficiales de la especialidad de ingeniería de sistemas cuenta con las capacidades de especialidad y militares para la implementación de sistemas que requieren exigencia actual, la tecnología y funcionalidad para contar con una institución moderna, eficaz y eficiente para hacer frente a las amenazas que se puedan presentar.

CAPÍTULO VIII

RECOMENDACIONES

RECOMENDACIONES

Luego de haber realizado las conclusiones, se recomienda lo siguiente:

PRIMERA RECOMENDACIÓN: En base a la necesidad de contar con un documento que manifieste los lineamientos para hacer frente a las amenazas en las redes de la institución, la Escuela de Oficiales, evalúe y apruebe el documento "MANUAL PARA CONTRARRESTAR LAS REDES DE AMENAZAS EN LA FAP", para ser considerado como una herramienta para la mejora de las actividades del Servicio de Informática de la FAP y en las diferentes UU. DD FAP, presentado en este informe de Suficiencia Profesional. Debido que trata un problema institucional y que es necesario solucionar para la mejora de las funciones y el desempeño de la Dirección de Telemática de la FAP - DITEL.

SEGUNDA RECOMENDACIÓN: Luego de la aprobación de la propuesta en la Escuela de Oficiales - EOFAP, se eleve a la Dirección de Telemática de la FAP - DITEL para que sus órganos correspondientes revisen de manera técnica y operativa para posteriormente validen y aprueben el documento manual "MANUAL PARA CONTRARRESTAR LAS REDES DE AMENAZAS EN LA FAP", para que sea elevada a la Comandancia General para su consideración como elemento de referencia para su aplicación.

TERCERA RECOMENDACIÓN: Luego de la aprobación en la Comandancia General para que en su personal especializado de documentación analicen y revisen el documento propuesto, para su consecuente aprobación institucional, para su vigencia e implementación, como una publicación complementaria en la Doctrina Institucional para que se difundida mediante medio físico y/o digital, el documento manual "MANUAL PARA CONTRARRESTAR LAS REDES DE AMENAZAS EN LA FAP", a todas las UU.DD. FAP.

CUARTA RECOMENDACIÓN: En base al compromiso del personal para la mejora permanente de los sistemas en la institución, es recomendable que exista una formación permanente del personal de oficiales que sea a nivel superior tanto en el país, como en el extranjero, encaminadas hacia los sistemas de redes con orientación hacia la optimización de los sistemas actuales en la institución.

QUINTA RECOMENDACIÓN: Basados en la alta capacidad demostrada por el personal de oficiales de ingeniería de sistemas, para proponer mejoras en la institución, es recomendable que se realice la promoción y difusión de los sistemas que se carece en la

actualidad para que se presenten proyectos de mejora de los mismos, de manera que se pueda luego realizar las evaluación tanto técnica, tecnológica, presupuestal y operativa para su aprobación y ejecución.

CAPÍTULO IX

REFERENCIAS

REFERENCIAS.

Ciberseguridad: nuevas amenazas online. (5 octubre de 2023). Www.ocu.org. Revisado el 21 de febrero de 2024, de https://www.ocu.org/tecnologia/antivirus/consejos/amenazas-online

Constitución política del Perú. (2022). *Constitución Política del Perú, promulgada el 29 de diciembre de 1993*. Promulgada por el Congreso Constituyente Democrático. Edición del Congreso de la República. Actualizada noviembre del 2022. https://www.congreso.gob.pe/Docs/files/constitucion/constitucion-noviembre2022.pdf.

DBFA 1. (2021). *Doctrina Básica de la Fuerza Aérea del Perú.* Doctrina aprobada el 28 de mayo del 2021. Estado Mayor General de la FAP.

Decreto Legislativo N° 1139 de 2012. *Ley de la Fuerza Aérea del Perú. 09 de diciembre de 2012*. D.O. No. 480442. https://busquedas.elperuano.pe/normaslegales/ley-de-la-fuerza-aerea-del-peru-decreto-legislativo-n-1139-876207-6/.

Decreto Supremo Nº 008-2023-DE (2023). *Decreto Supremo que aprueba el reglamento del Decreto Legislativo Nº 1139, Ley de la Fuerza Aérea del Perú*. 07 de octubre del 2023.

Decreto Supremo Nº 017-2024-PCM (2024). *Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa*. 13 de febrero del 2024. D. O. Año XLI - Nº 17742 (p. 2), en https://busquedas.elperuano.pe/cuadernillo/NL/20240213.

DOFA 1-4 (2016). *Doctrina Operacional de Operaciones en el Ciberespacio*. 19 de agosto de 2016. Comandancia General de la Fuerza Aérea del Perú.

Flores, M. (04 de setiembre de 2023). *¡Cuidado de los ciberataques! Aumentan las amenazas en aplicaciones bancarias*. Elperuano.pe. Revisado el 15 de febrero de 2024, de https://elperuano.pe/noticia/222128-aumentan-las-amenazas-en-app-bancarias

Ley Nº 30096 (2013), *Ley de Delitos Informáticos*. 27 de setiembre de 2013. D. O. 505484, en https://busquedas.elperuano.pe/dispositivo/NL/1003117-1

Ley Nº 30999 (2019), *Ley de Ciberdefensa*. 26 de agosto de 2019. D. O. Año XXXVI - Nº 15061 (p. 9), en https://busquedas.elperuano.pe/dispositivo/NL/1801519-5

MOF - Apéndice 2 - Anexo J. (2020). *Manual de Organización y Funciones de la Escuela de Oficiales*. Aprobado con Resolución de la Dirección General de Educación de la Fuerza Aérea Nº 097-DIGED del 03 de noviembre de 2020.

MOF - Apéndice 2 - Anexo K. (2020). *Manual de Organización y Funciones del Servicio de Informática*. Aprobado con Resolución de la Comandancia General de la Fuerza Aérea

Nº 0260-CGFA del 09 de mayo de 2019.

Nicola, M. D. (2024). *Las 4 amenazas más comunes en las redes sociales que pueden dañar la seguridad de tus datos* | Ciberseguridad LATAM. Www.ciberseguridadlatam.com. Revisado el 20 de febrero de 2024, from https://www.ciberseguridadlatam.com/2022/05/27/las-4-amenazas-mas-comunes-en-las-redes-sociales-que-pueden-danar-la-seguridad-de-tus-datos/.

Ordenanza FAP 21–1 (2023). *"Telemática", Estimación de Riesgos de Ciberseguridad en las Unidades FAP*. 31 de julio de 2023. Comandancia General de la Fuerza Aérea del Perú.

Pichihua, S. (17 de enero de 2020). *Estos son los delitos informáticos más frecuentes en el Perú*. Elperuano.pe. Revisado el 19 de febrero de 2024, de https://elperuano.pe/noticia/88720-estos-son-los-delitos-informaticos-mas-frecuentes-en-el-peru.

Ríos, M. (11 de setiembre de 2023). *Amenazas digitales: El porcentaje de peruanos que usa su equipo personal para trabajar*. Gestión.pe. Revisado el 19 de febrero de 2024, de https://gestion.pe/tecnologia/smartphones-tablets-pc-empresas-y-la-ciberseguridad-el-porcentaje-de-peruanos-que-usa-su-equipo-personal-para-trabajar-amenazas-digitales-noticia/.

CAPÍTULO X

ANEXOS

ANEXO “I”

Encuesta sobre el “Las Redes de Amenazas en la Fuerza Aérea del Perú”

Dirigido al personal Oficiales y técnicos de la especialidad sistemas e informática que realiza actividades de telemática en la FAP.

Me es grato saludarlo e invitarlo a responder el presente cuestionario. Sus respuestas son confidenciales y anónimas, tiene por objeto recoger su importante opinión sobre las actividades propias de redes, algoritmos y amenazas cibernéticas en la FAP y la normatividad que se encuentra vigente en la actualidad.

Marcar con un aspa (X), la respuesta que considere correcta.

Instrumento

Preguntas.

Pregunta N 1: ¿Usted, considera que, es importante la base legal de Ciberseguridad y Ciberdefensa?

Si ( ) No ( )

Pregunta N 2: ¿Usted, considera que, la doctrina institucional vigente es adecuada para la Ciberseguridad y Ciberdefensa?

Si ( ) No ( )

Pregunta N 3: ¿Usted, considera que la institución, ha implementado de manera adecuada el contrarrestar las redes de amenazas?

Si ( ) No ( )

Pregunta N 4: ¿Usted, considera que, la institución está en la capacidad de implementar un documento para contrarrestar las redes de amenazas?

Si ( ) No ( )

Pregunta N 5: ¿Usted, considera que, a nivel de Ciberdefensa y para fortalecer la misión institucional sea necesaria la implementación de un sistema para contrarrestar las redes de amenazas?

Si ( ) No ( )

Pregunta N 6: ¿Usted, considera que, a nivel administrativo, la implementación para contrarrestar las redes de amenazas en las UU.DD FAP sería eficiente en vías de la modernización del Estado?

Si ( ) No ( )

Pregunta N 7: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando el entorno de seguridad?

Si ( ) No ( )

Pregunta N 8: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando los fundamentos de las redes de amenazas?

Si ( ) No ( )

Pregunta N 9: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las redes en el entorno operativo?

Si ( ) No ( )

Pregunta N 10: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando planificación para contrarrestar las redes de amenazas?

Si ( ) No ( )

Pregunta N 11: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando actividades para contrarrestar las redes de amenazas?

Si ( ) No ( )

Pregunta N 12: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las evaluaciones para contrarrestar las redes de amenazas?

Si ( ) No ( )

Pregunta N 13: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando las características clandestinas de las redes de amenazas?

Si ( ) No ( )

Pregunta N 14: ¿Usted, considera que, la implementación para contrarrestar las redes de amenazas en la FAP, sea desarrollado considerando el entorno operativo de las redes de amenazas?

Si ( ) No ( )

ANEXO II

MINISTERIO DE DEFENSA
Fuerza Aérea del Perú
COMANDANCIA GENERAL

MANUAL FAP 21-01

Lima, 23 de febrero del 2024

"CIBERDEFENSA"

MANUAL PARA CONTRARRESTAR LAS REDES DE AMENAZAS EN LA FUERZA AÉREA DEL PERÚ

2024

INTRODUCCIÓN

El Presente Manual tiene como propósito poner al alcance de los usuarios un documento normativo que planifique, ejecute y evalúen lineamientos para identificar, neutralizar, interrumpir o destruir redes de amenazas.

El correcto empleo de este Manual, así como el estricto cumplimiento de su contenido, contribuirá a asegurar el eficiente funcionamiento de los Departamentos de Telemática en las UU.DD. FAP.

Durante su empleo, el usuario deberá poner en práctica los conocimientos necesarios para hacer frente a las redes de amenazas.

Por último, el presente Manual está destinado a facilitar la instrucción adecuada al respecto, sirviendo a la vez de guía y estableciendo los lineamientos en ciberseguridad más adecuados. Sin embargo; es pertinente hacer presente que el Manual debe considerarse como complemento.

"CIBERDEFENSA"

MANUAL PARA CONTRARRESTAR LAS REDES DE AMENAZAS EN LA FUERZA AÉREA DEL PERÚ

ÍNDICE

Página

CAPÍTULO I

GENERALIDADES

CAPÍTULO II

FUNDAMENTOS DE LAS REDES DE AMENAZAS

CAPÍTULO III

REDES EN EL ENTORNO OPERATIVO

CAPÍTULO IV

PLANIFICACIÓN PARA CONTRASTAR LAS REDES DE AMENAZA

CAPÍTULO V

ACTIVIDADES PARA CONTRASTAR LAS REDES DE AMENAZA

CAPÍTULO VI

EVALUACIONES

ANEXOS:

CAPÍTULO I

GENERALIDADES

1.- OBJETO

Establecer el manual para contrarrestar las redes de amenazas en las diferentes unidades y dependencias de la Fuerza Aérea del Perú.

2.- FINALIDAD

Proporcionar los principios fundamentales que orienten el hacer frente a las redes de amenazas en las diferentes unidades y dependencias de la Fuerza Aérea del Perú.

3.- ALCANCE

El presente manual puede ser empleado por el personal del SINFA y de las diferentes UU.DD. de la Fuerza Aérea. Asimismo, su contenido, sirve de referencia y guía a todo el personal militar de las diferentes unidades y dependencias FAP para identificar, neutralizar, interrumpir o destruir redes de amenazas.

CAPÍTULO II

FUNDAMENTOS DE LAS REDES DE AMENAZAS

1.- CONSTRUCCIÓN DE RED DE AMENAZAS

a. Componentes básicos de la red. Todas las redes, independientemente de su tamaño, comparten componentes y características básicas. Comprender los componentes y características comunes ayudará a desarrollar y establecer una terminología conjunta común y estandarizar los resultados para el análisis de redes, la planificación, las actividades y las evaluaciones de CTN en toda la fuerza conjunta y los CCMD

b. Terminología de redes. Una red de amenazas consta de nodos y enlaces interconectados y puede organizarse utilizando redes y células subordinadas y asociadas. Comprender las funciones y conexiones individuales de cada elemento es tan importante para realizar operaciones como lo es comprender la estructura general de la red, conocida como topología de la red.

La estructura general, tal como se ha formado con el tiempo y se ha adaptado a su entorno, afecta el comportamiento de las redes, los nodos y las células. La fortaleza y la cantidad de enlaces brindan una visión inicial de las capacidades, fortalezas, debilidades y COG de la red.

También deben determinarse los límites de las redes, especialmente cuando se trata de redes superpuestas y redes globales. Rara vez será posible realizar operaciones contra una amenaza completa o sus redes de apoyo. Comprender la topología de la red permite a los planificadores desarrollar un enfoque operativo y las tácticas asociadas necesarias para crear los efectos deseados en la red.

(1) Red. Una red es un grupo de elementos que consta de nodos y enlaces interconectados que representan relaciones o asociaciones. A veces los términos red y sistema son sinónimos. Esta publicación utiliza el término red para distinguir las redes de amenazas de la multitud de otros sistemas, como un sistema de defensa aérea, un sistema de comunicaciones, un sistema de transporte, etc.

(2) Celda. Una célula es una organización subordinada formada en torno a un proceso, capacidad o actividad específica dentro de una organización más grande designada.

(3) Nodo. Un nodo es un elemento de una red que representa una persona, lugar u objeto físico. Los nodos representan elementos tangibles dentro de una red u OE que pueden ser objeto de acción. Los nodos pueden pertenecer a una o más categorías PMESII.

(4) Enlace. Un vínculo es una relación de comportamiento, física o funcional entre nodos. Los vínculos ayudan al JFC y al personal a visualizar las funciones nodales internas y las interacciones con otros nodos, como los acuerdos de mando o supervisión que conectan a un superior con un subordinado, la relación de una fuente de armas con un traficante de armas y la ideología que conecta a un propagandista. a un grupo de terroristas. Los enlaces establecen la interconectividad entre nodos que les permite trabajar juntos como una red: comportarse de una manera específica (realizar una tarea o realizar una función). Los nodos y enlaces son útiles para identificar COG, redes y células en las que el JFC puede querer influir o cambiar durante una operación.

2.- ANÁLISIS DE RED

a. El análisis de redes es un medio para comprender un grupo, lugar, objeto físico o sistema. Identifica nodos relevantes, determina y analiza enlaces entre nodos e identifica nodos clave. La perspectiva de los sistemas PMESII es un punto de partida útil para el análisis de redes de amenazas. El análisis de redes facilita la identificación de

información importante sobre las redes que de otro modo podría pasar desapercibida. Por ejemplo, el análisis de redes puede descubrir posiciones de poder dentro de una red, mostrar las células que explican su estructura y organización, encontrar individuos o células cuya eliminación alteraría en gran medida la red y facilitar la medición del cambio a lo largo del tiempo.

b. Todas las redes están influenciadas por los OE en los que existen y, a su vez, influyen en ellos. Los analistas deben comprender las condiciones subyacentes; las fricciones entre individuos y grupos;

relaciones familiares, comerciales y gubernamentales; y factores de inestabilidad que están constantemente sujetos a cambios y presiones. Todos estos factores evolucionan a medida que las redes cambian de forma, aumentan o disminuyen su capacidad y se esfuerzan por influir y controlar cosas dentro de la OE, y contribuyen o dificultan el éxito de las redes. El encuadre ambiental consiste en seleccionar, organizar, interpretar y dar sentido a una realidad compleja; sirve como guía para analizar, comprender y actuar. El pensamiento crítico requiere que los analistas desarrollen una comprensión completa de la EO y resuelvan los problemas correctos y sigan siendo capaces y dispuestos a adaptarse a condiciones dinámicas e incluso impredecibles.

C. Las redes suelen formarse en la confluencia de tres condiciones: la presencia de un catalizador, una audiencia receptiva y un entorno complaciente. A medida que cambian las condiciones dentro de la OE, la red debe adaptarse para mantener una capacidad mínima para funcionar dentro de estas condiciones. Elementos de estas condiciones pueden estar directamente relacionados con los factores que componen el COG de la red.

(1) Catalizador. Un catalizador es una condición o variable dentro de la OE que podría motivar o unir a un grupo de individuos a tomar algún tipo de acción para satisfacer sus necesidades colectivas. Estos catalizadores pueden identificarse como variables críticas a medida

que las unidades realizan su evaluación del EO y pueden consistir en una persona, idea, necesidad, evento o alguna combinación de ellos. Existe la posibilidad de que el catalizador cambie según las condiciones del OE.

(2) Audiencia receptiva. Una audiencia receptiva es un grupo de individuos que sienten que tienen más que ganar participando en las actividades de la red que no participando.

Además, para que se forme una red, los miembros de la red deben tener la motivación y los medios para llevar a cabo acciones que aborden el catalizador que generó la red.

Dependiendo del tipo de red y de cómo esté organizada, el liderazgo puede ser necesario o no para que la red forme, sobreviva o sostenga la acción colectiva. El público receptivo proviene de la dimensión humana del OE.

(3) Ambiente acogedor. Un ambiente complaciente son las condiciones dentro de la OE que facilitan la organización y las acciones de una red. Deben existir condiciones adecuadas dentro de la OE para que se forme una red que satisfaga una necesidad real o percibida.

Las redes pueden existir durante un tiempo sin un entorno propicio, pero sin él la red acabará fallando.

d. Las redes utilizan la estructura del sistema PMESII dentro del OE para formarse, sobrevivir y funcionar. Al igual que la fuerza conjunta, las redes de amenazas también tendrán objetivos y estados finales deseados. A medida que se realiza el análisis de la OE, el personal conjunto debe identificar las variables críticas dentro de la OE para la red. Una variable crítica es un recurso o condición clave presente dentro de la OE que tiene un impacto directo en los objetivos del comandante y puede afectar la formación y el mantenimiento de redes. Una variable crítica es el enfoque para dar forma, dentro de la OE, a lograr el objetivo del comandante o alcanzar el estado final militar.

Identificar variables críticas es importante porque afectan los COG de componentes y actores clave dentro de los sistemas. Las variables críticas a menudo sirven para enfocar las medidas de efectividad (MOE) y el desarrollo de indicadores. Se convierten en el foco para dar forma y medir, dentro de la OE, para determinar el progreso hacia el estado final.

3.- DETERMINAR Y ANALIZAR LAS RELACIONES NODO-ENLACE

Los enlaces se derivan de datos o extrapolaciones basadas en datos. Una ventaja de representar gráficamente las relaciones entre nodos y enlaces es que el impacto potencial de las acciones contra ciertos nodos puede volverse más evidente. El análisis de redes sociales (SNA) proporciona un método que ayuda al JFC y al personal a comprender la relevancia de los nodos y enlaces. El mapeo de redes es esencial para realizar el SNA. Por ejemplo, el número de enlaces entre nodos puede indicar la importancia del nodo para el grupo funcional más amplio. La fuerza o intensidad de un único vínculo puede ser relevante para determinar la importancia de la relación funcional entre los nodos y la importancia general para el sistema más amplio. La fuerza o intensidad del enlace es una evaluación cualitativa que indica cuánta información, influencia y recursos fluyen entre los nodos. No existe una escala absoluta para la intensidad de los enlaces, ya que las redes varían ampliamente; es una asignación relativa en comparación con otros enlaces de la red. Por lo tanto, el número y la fuerza de los enlaces nodales dentro de un conjunto de nodos pueden ser indicadores de nodos clave y de un COG potencial. Debido a la posible complejidad de las relaciones de red, las técnicas de visualización gráfica pueden facilitar el análisis de la red.

a. Análisis de enlaces. El análisis de enlaces identifica y analiza las relaciones entre los nodos de una red. El mapeo de red proporciona una visualización de los enlaces entre nodos, pero no proporciona los datos cualitativos necesarios para definir completamente los enlaces.

El análisis de redes interrelacionadas requiere claridad del tipo y la fuerza de cada vínculo para proporcionar al comandante una mayor comprensión de la red. Una mejor comprensión de las relaciones entre los nodos de la red proporciona al comandante información que respaldará el proceso de selección de objetivos. Durante el análisis de vínculo, el analista examina las condiciones de la relación, fuerte o débil, informal o formal, formada por condiciones familiares, sociales, culturales, políticas, virtuales, profesionales o de cualquier otra índole. Los datos cualitativos producidos a partir del análisis de enlaces se utilizan luego con otros datos cuantitativos para distinguir nodos, líneas de comunicaciones y jerarquías para interrupciones dentro de la red.

b. Análisis nodal. Los individuos están asociados con numerosas redes debido a sus identidades individuales. La ubicación de un nodo dentro de una red y en relación con otros nodos conlleva identidad, poder o creencia e influye en el comportamiento. Ejemplos de estos tipos de

Las identidades incluyen lugares de nacimiento, familia, religión, grupos sociales, organizaciones o una serie de características diversas que definen a un individuo. Estos atributos individuales a menudo se recopilan durante actividades de identidad y se fusionan con atributos de actividades de recopilación no relacionadas para formar productos de inteligencia de identidad (I2). Algunos aspectos utilizados para ayudar a comprender y definir a un individuo están directamente relacionados con las condiciones que apoyaron el desarrollo de relaciones con otros nodos. Comprender este tipo de información sobre un nodo específico ayudará al comandante durante todo el proceso de selección de objetivos. El Capítulo V, “Actividades para contrarrestar las redes amenazantes”, explora cómo la información obtenida al comprender la red puede usarse para mejorar los esfuerzos del comandante para seleccionar objetivos. La Figura II-1 ilustra algunas características asociadas con las redes que el comandante puede considerar para ayudar a comprender la red que se va a atacar.

C. Análisis de red. A lo largo del proceso JIPOE, en cada escalón y categoría de producción, uno de los aspectos del análisis más importantes, pero menos comprendido, es el análisis sociocultural (SCA). SCA es el estudio, evaluación e interpretación de información sobre adversarios y actores relevantes a través de la lente de la toma de decisiones a nivel de grupo para discernir los catalizadores del comportamiento y el contexto que moldea el comportamiento. SCA considera las relaciones y actividades de la población, el SNA (observando las redes interpersonales, profesionales y sociales vinculadas a un individuo), así como la dinámica de grupos pequeños y grandes. El SNA no sólo examina individuos y grupos de individuos dentro de una estructura social como una organización terrorista, criminal o insurgente, pero también examina cómo interactúan. Las interacciones suelen ser repetitivas, duraderas y tienen un propósito mayor, y los patrones de interacción afectan el comportamiento. Si se puede recopilar suficiente información sobre nodos y enlaces, se pueden observar patrones de comportamiento y, hasta cierto punto, predecirlos. El SNA se diferencia del análisis de vínculos porque sólo analiza objetos similares (por ejemplo, personas u organizaciones), no las relaciones entre los objetos. SNA proporciona un análisis objetivo de la estructura de red actual y prevista y la interacción de redes que tienen un impacto en el OE. El software informático SNA puede ahorrar tiempo, permitir la manipulación de datos y producir representaciones gráficas (matrices, etc.) de redes para el comandante y el estado mayor.

4.- REDES Y CÉLULAS DE AMENAZA

Una red debe realizar una serie de funciones para sobrevivir y crecer. Estas funciones pueden verse como células que tienen su propia estructura organizativa interna y comunicaciones. Estas células trabajan en conjunto para lograr los objetivos generales de la organización. Para sobrevivir, la estructura interna de la red tiene un alto grado de flexibilidad, adaptándose a la presión amistosa y a los

requisitos de la OE. Las redes no existen en el vacío. Normalmente comparten nodos y enlaces con otras redes. Cada red puede requerir un enfoque operativo único a medida que se adaptan a su OE o para lograr nuevos objetivos. Pueden formar una mayor cantidad de células si son capaces de realizar operaciones independientes consistentes con los objetivos operativos generales de la red de amenazas. Es posible que pasen a un sistema más jerárquico debido a la falta de liderazgo, cuestiones relacionadas con la lealtad de los subordinados o personal de nivel inferior sin experiencia. Comprender estas dimensiones permite al comandante diseñar un enfoque operativo más eficaz. Estas celdas son sólo ejemplos. La lista no es excluyente ni inclusiva. Cada red y célula cambiará, se adaptará y se transformará con el tiempo.

a. Células operativas. Las células operativas llevan a cabo las operaciones diarias de la red y normalmente están basadas en personas (por ejemplo, terroristas, guerrilleros, traficantes de drogas). Es extremadamente difícil recopilar inteligencia y representar cada nodo y enlace dentro de una red operativa. Sin embargo, comprender los nodos, enlaces y células clave que son particularmente efectivos permite apuntar con precisión y lograr una mayor efectividad.

b. Células Logísticas. Las células logísticas proporcionan a las redes de amenazas los suministros, armas, municiones, combustible y equipo militar necesarios para operar. Las células logísticas son más fáciles de observar y apuntar que las operativas o de comunicaciones, ya que mueven grandes cantidades de material, lo que las hace más visibles. Estas células pueden incluir individuos que no están tan motivados ideológicamente o comprometidos como aquellos en las redes operativas. Las células logísticas de amenazas a menudo utilizan nodos y enlaces logísticos legítimos para ocultar sus actividades “entre el ruido” de suministros legítimos destinados a una economía local o regional. Es particularmente importante determinar qué vínculos se extienden a otros países o fuera del área operativa, ya que esto requerirá cooperación interinstitucional e internacional del Gobierno

de los Estados Unidos. Interdicción Las operaciones a lo largo de fronteras internacionales y regionales pueden apuntar eficazmente a enlaces y aislar redes de amenazas.

c. Células de formación. La mayoría de los líderes de redes desean hacer crecer la organización para obtener poder, prestigio y avance en sus objetivos. Las células logísticas pueden usarse para trasladar material, capacitadores y alumnos a un área de capacitación, o esa parte de la logística puede ser una parte distinta de las células de capacitación. Una vez que se completa la capacitación, las células logísticas trasladan a los nuevos miembros a las áreas operativas. Estas actividades pueden ser visibles y proporcionar información sobre las actividades de una red y su topología. La capacitación requiere la incorporación de personal nuevo y, a menudo, incluye estructuras físicas para respaldar las actividades que también pueden ser visibles y proporcionar información adicional para comprender mejor la red.

d. Células de Comunicaciones. La mayoría de las redes de amenazas tienen como mínimo células de comunicación rudimentarias para fines operativos, logísticos y financieros y otra para comunicar su narrativa estratégica a una población objetivo o neutral. Si bien es bastante difícil neutralizar completamente cualquier medio de comunicación, las organizaciones de inteligencia pueden recopilar y analizar mensajes, rastrear tendencias de contenido e identificar al autor del mensaje. El uso de plataformas de redes sociales basadas en Internet por parte de redes de amenazas aumenta la probabilidad de recopilar información, incluida información geoespacial.

e. Células financieras. Las redes de amenazas requieren financiación para todos los aspectos de sus actividades, para mantener y ampliar su membresía y para difundir su mensaje. Su célula financiera mueve dinero de operaciones comerciales legítimas e ilegítimas, donantes extranjeros e impuestos recaudados o coaccionados de la población hacia el área operativa. Este movimiento puede utilizar las redes

financieras formalmente reguladas que se extienden por todo el mundo o redes regionales informales como las hawalas (un sistema informal de transferencia regional que se basa en la confianza y que a menudo se presenta como una transferencia de dinero sin realmente moverlo). La financiación puede provenir de secuestro, piratería, otras actividades delictivas, patrocinadores estatales o negocios legítimos controlados por la red.

f. Células de proliferación de armas de destrucción masiva. Muchas de estas células no están organizadas específicamente para la proliferación de armas de destrucción masiva. De hecho, muchas células existentes pueden utilizarse por conveniencia. Ejemplos de células existentes incluyen la trata de personas, la falsificación y el tráfico de drogas.

Como consideración adicional, algunos nodos dentro de estas redes pueden ser socios involuntarios.

La amenaza se complica aún más por las operaciones de redes multinacionales, potencialmente con el apoyo de recursos estatales. Estas actividades de proliferación global emplean una combinación de secreto, dispersión y recursos fiscales que deben ser localizados, monitoreados y, en última instancia, atacados. El JFC debería utilizar una perspectiva de sistemas para comprender mejor la complejidad de la OE y las redes asociadas. Esta perspectiva analiza los sistemas PMESII para identificar los nodos, enlaces, COG y posibles vulnerabilidades dentro de la red.

El JFC entiende que a medida que estas subredes se expanden en alcance y área, las acciones necesarias para identificarlas y afectarlas adecuadamente pueden residir fuera de la influencia del DOD y pueden requerir esfuerzos de socios interinstitucionales, ONG, PN, HN u organizaciones internacionales. Dependiendo de la organización de la fuerza conjunta, el JFC puede carecer de una gama completa de capacidades que puedan

apoyar la unidad de esfuerzo para disuadir, disuadir, derrotar o negar de manera proactiva y completa a estas redes y células.

5.- ANALIZAR LA RED

Existen nodos clave en todas las redes importantes y son fundamentales para su función. Los nodos pueden ser personas, lugares o cosas. Por ejemplo, una ciudad que es el conducto principal para el movimiento de narcóticos ilegales sería el nodo clave en una red de tráfico de drogas. Algunos pueden convertirse en puntos decisivos para las operaciones militares ya que, cuando se actúa en consecuencia, podrían permitir al JFC obtener una marcada ventaja sobre el adversario o contribuir materialmente al logro del éxito. Debilitar o eliminar un nodo clave debería hacer que su grupo relacionado de nodos y enlaces funcione con menor eficacia o no funcione en absoluto, mientras que fortalecer el nodo clave podría mejorar el rendimiento de la red en su conjunto. Los nodos clave a menudo están vinculados a múltiples redes, residen en ellas o influyen en ellas. Por ejemplo, la religión predominante de un país podría ser central para el funcionamiento del sistema social del país, y el grupo central de líderes religiosos (o un solo líder) podría ser un nodo clave. Dependiendo de la estructura social y política del país, este mismo grupo de líderes religiosos también podría ser un nodo clave en el sistema político cuando se lo considera una red. Dado que cada sistema y subsistema PMESII está compuesto de nodos y enlaces, las capacidades de los instrumentos de poder nacional estadounidenses pueden emplearse contra nodos clave seleccionados para crear efectos operativos y estratégicos. Aunque está influenciado en gran medida por el juicio subjetivo, la identificación de un nodo clave potencial puede facilitarse mediante un análisis de la densidad de la red, el grado de centralidad y la centralidad del nodo (es decir, cómo encajan las entidades individuales en la red de sistemas). La centralidad de los nodos puede resaltar posibles posiciones de importancia, influencia o

prominencia y patrones de conexiones. La centralidad relativa de un nodo se determina analizando características medibles: grado, cercanía, intermediación y vector propio.

CAPÍTULO III

REDES EN EL ENTORNO OPERATIVO

1.- AMENAZAS EN RED Y SU IMPACTO EN EL ENTORNO OPERATIVO

a. En un mundo cada vez más caracterizado por la volatilidad, la incertidumbre, la complejidad y la ambigüedad, ha surgido una amplia gama de desafíos irregulares locales, nacionales y transnacionales a la estabilidad del sistema internacional. Las amenazas tradicionales como las insurgencias y las bandas criminales han estado explotando a los gobiernos débiles o corruptos durante años, pero el ascenso de los extremistas transnacionales y su cooperación activa con las amenazas tradicionales ha cambiado la dinámica global. La disuasión y eliminación exitosa de estas redes ilícitas es más complicada y menos predecible que en el pasado.

b. Todas las redes son vulnerables, y un JFC y su personal armados con una comprensión integral de la estructura, el propósito, las motivaciones, las funciones, las interrelaciones y las operaciones de una red de amenazas pueden determinar los medios, métodos y tiempos más efectivos para explotar esa vulnerabilidad. Para que el proceso JIPOE produzca comprensión de las amenazas y sus redes, el análisis debe ser realizado por analistas de inteligencia y planificadores operativos familiarizados con los principios del análisis de redes. El análisis y la explotación de redes no son tareas sencillas. Las amenazas en red son adversarios altamente adaptables con la capacidad de seleccionar una variedad de tácticas, técnicas y tecnologías y combinarlas de maneras no convencionales para alcanzar sus objetivos estratégicos. Además, muchas redes de amenazas suplantan o incluso reemplazan funciones gubernamentales legítimas, como servicios sociales y de salud, protección física o apoyo financiero en áreas no gobernadas o mínimamente gobernadas.

Esta gobernanza de facto de un área por parte de una red de amenazas hace que sea más difícil para la fuerza conjunta atacar simultáneamente una amenaza y satisfacer las necesidades de la población.

c. Una vez que el JFC identifica las redes en el OE y comprende sus interrelaciones, funciones, motivaciones y vulnerabilidades, el comandante adapta la fuerza para aplicar las herramientas más efectivas contra la amenaza. Se necesitan organizaciones de tareas personalizadas y equipos especializados para aplicar una presión efectiva en toda la estructura de la red. Por ejemplo, una JTF tradicional normalmente no cuenta con expertos financieros civiles en su personal para identificar y ayudar a atacar las actividades de las redes financieras amenazantes. Del mismo modo, una célula de fuego de la JTF puede requerir principalmente especialistas MISO y/o IO en lugar de artillería de campaña y controladores de ataque terminal conjuntos. Además, la JTF requiere el apoyo y la participación activos del Gobierno de los Estados Unidos, la HN, agencias no gubernamentales y socios, particularmente cuando se trata de abordar el santuario transfronterizo, los flujos de armas y las causas fundamentales de la inestabilidad. Este enfoque de "equipo de equipos" facilita la acción unificada, que es esencial para organizar las operaciones contra una amenaza adaptativa.

2.- CARACTERÍSTICAS DE LA RED DE AMENAZAS

Las redes amenazantes no difieren mucho de las redes no amenazantes en su organización funcional y requisitos. Las redes de amenazas se manifiestan e interactúan con redes neutrales para protegerse, perpetuar sus objetivos y ampliar su influencia.

Las redes que involucran a personas han sido descritas como insurgentes, criminales, terroristas, sociales, políticas, familiares, tribales, religiosas, académicas, étnicas o demográficas. Algunas redes

no humanas incluyen comunicaciones, financieras, comerciales, eléctricas/energéticas, agua, recursos naturales, transporte o informativas. Las redes toman muchas formas y sirven diferentes propósitos, pero todas están compuestas de personas, procesos, lugares, materiales o combinaciones.

Los componentes individuales de la red son identificables, seleccionables y explotables. Casi universalmente, los humanos son miembros de más de una red, y la mayoría de las redes dependen de otras redes para su sostenimiento o supervivencia. Debido a la gran cantidad de redes, el problema es encontrar las amenazas enterradas dentro de múltiples redes y operando a través de ellas.

Algunas amenazas, como los proliferadores de armas de destrucción masiva, son particularmente difíciles de detectar porque las redes legales pueden usarse con fines ilegales. Las amenazas organizadas aprovechan múltiples redes dentro de la OE en función de los requisitos de la misión o para lograr objetivos que no se pueden alcanzar unilateralmente. El siguiente ejemplo muestra algunas redes típicas que una amenaza utilizará y/o explotará. Esta “red de redes” siempre está presente y presenta desafíos para el JFC al planificar operaciones para contrarrestar las amenazas que anidan dentro de varias redes amigas, neutrales y hostiles.

3.- AMENAZAS ADAPTATIVAS EN RED

Para que una red de amenazas sobreviva a las presiones políticas, económicas, sociales y militares, debe adaptarse a esas presiones. La supervivencia y el éxito están directamente relacionados con la adaptabilidad y la capacidad de acceder a recursos financieros, logísticos y humanos. Las redes poseen muchas características importantes para su éxito y supervivencia, como una estructura C2 flexible; una identidad compartida; y los conocimientos, habilidades y capacidades de los líderes y miembros del grupo para adaptarse.

También deben tener un flujo constante de recursos y pueden necesitar un santuario (refugio seguro) desde el cual reagruparse y planificar.

a. Estructura C2. Hay muchos diseños potenciales para la organización interna de la red de amenazas. Algunas son jerárquicas, otras planas y otras pueden ser una combinación. La clave es que, para sobrevivir, las redes se adaptan continuamente a los cambios en la OE, especialmente en respuesta a acciones amistosas. Los comandantes deben ser capaces de reconocer los cambios en las estructuras C2 de la amenaza provocados por acciones amistosas y mantener la presión para evitar una reconstitución exitosa de la amenaza.

b. Identidad compartida. La identidad compartida entre los miembros normalmente se basa en el parentesco, la ideología, la religión y las relaciones personales que unen a la red y facilitan el reclutamiento. Estos atributos de identidad pueden ser una parte importante de los esfuerzos de actividades de identidad actuales y futuros, y el análisis puede iniciarse antes de que las hostilidades sean inminentes. El relativamente nuevo ISIL obtiene gran parte de su apoyo de grupos y poblaciones de larga data en Irak y Siria, al igual que lo hacen organizaciones palestinas dispares en el Levante. De manera similar, el Ejército Republicano Irlandés obtuvo gran parte de su apoyo y recaudación de fondos de grupos de larga data en los años 1960 y 1970 dentro de la población irlandesa-estadounidense.

c. Conocimientos, habilidades y capacidades de los líderes y miembros del grupo. Todas las redes de amenazas tienen distintos grados de competencia. En las etapas iniciales de desarrollo, una organización amenazante y sus miembros pueden tener capacidades limitadas. La supervivencia de una organización depende del conocimiento, las habilidades y las capacidades de sus líderes y miembros. Al buscar experiencia en la materia, respaldo financiero o apoyo de terceros, una organización puede aumentar sus conocimientos, habilidades y

destrezas, haciéndolas más adaptables y aumentando sus posibilidades de supervivencia.

d. Recursos. Las redes de amenazas utilizan recursos en forma de armas, dinero, tecnología, conectividad social y reconocimiento público. Identificación y sistemática.

El estrangulamiento de los recursos de amenaza es el principio fundamental de CTN. Por ejemplo, el dinero es uno de los recursos críticos de las redes adversarias. Negarle al adversario sus finanzas hace que sea más difícil, y quizás imposible, pagar, entrenar, armar, alimentar y vestir a las fuerzas o reunir información y producir propaganda. Consulte el Apéndice A, "Financiamiento contra amenazas del Departamento de Defensa", para obtener más información. Si bien ISIL ha podido utilizar el petróleo para ayudar a financiar sus operaciones, otras amenazas utilizarán diversas fuentes de financiación.

e. Adaptabilidad. Esto incluye la capacidad de aprender y ajustar comportamientos; modificar tácticas, técnicas y procedimientos (TTP); mejorar la seguridad de las comunicaciones y de las operaciones; emplear con éxito los IRC; y crear soluciones para salvaguardar nodos críticos y reconstituir experiencia, equipos, financiación y líneas logísticas que se pierden debido a esfuerzos amistosos de disrupción. Los analistas realizan análisis de tendencias y examinan indicadores clave dentro de la OE que podrían sugerir cómo y por qué las redes cambiarán y se adaptarán. Los esfuerzos de disrupción a menudo provocarán el cambio de métodos o prácticas de una red, pero a menudo las influencias externas, las relaciones locales y las fricciones internas, los desafíos geográficos y climáticos y los factores económicos globales también pueden ser algunos de los factores que motivan a una red de amenazas a cambiar o adaptarse. para sobrevivir.

f. Santuario (Refugios Seguros). Los refugios seguros permiten que las redes de amenazas lleven a cabo planificación, capacitación y reconstitución logística. Las redes de amenazas requieren ciertas capacidades críticas (CC) para mantener su existencia, entre ellas refugios seguros desde donde regenerar el poder de combate y/o áreas desde donde lanzar ataques. El JFC y su personal deben identificar y denegar el acceso a refugios seguros contra amenazas. Los refugios seguros fuera del área operativa inmediata albergados por terceros, Estados-nación u otros elementos criminales requieren un análisis integral de la amenaza y requerirán un enfoque ampliado de todo el gobierno.

4.- COMPROMISO CON LA RED

a. El compromiso de la red son las interacciones con redes amigas, neutrales y de amenazas, realizadas de forma continua y simultánea en los niveles táctico, operativo y estratégico, para ayudar a lograr los objetivos del comandante dentro de una OE. Para contrarrestar eficazmente las redes de amenazas, la fuerza conjunta debe buscar apoyar y vincularse con redes amigas e involucrar a redes neutrales mediante la construcción de confianza mutua y cooperación a través del compromiso de la red. La fuerza conjunta coordinará y trabajará en cooperación con socios interinstitucionales y PN. La acción unificada brinda al JFC la oportunidad de crear poderosas redes amigas con capacidades de largo alcance y comprometer redes neutrales para solicitar su asistencia o evitar que apoyen a nuestro adversario. Estas actividades integradas y sincronizadas tienen como objetivo establecer condiciones dentro de la OE que se alineen con el estado final deseado del JFC.

b. La participación de la red consta de tres componentes: asociarse con redes amigas, involucrar a redes neutrales y CTN para apoyar el estado final deseado por el comandante. La participación de la red no es un proceso independiente, sino que establece una serie de métodos que

apoyarán o amplificarán los procesos del JFC (JPP, JIPOE, focalización y evaluación) para prosperar y dominar en cualquier OE. La participación en la red utiliza acciones tanto letales como no letales contra redes, nodos y enlaces.

c. Los individuos pueden estar asociados con numerosas redes debido a sus identidades únicas. Ejemplos de estos tipos de identidades incluyen el lugar de nacimiento, la familia, la religión, los grupos sociales, las organizaciones o una serie de características diversas que definen a un individuo. Por lo tanto, no es raro que un individuo esté asociado con más de un tipo de red (amistosa, neutral o amenazante). Las identidades individuales proporcionan la base que permite que exista la interrelación entre redes amigas, neutrales y amenazantes. Es esta interrelación la que hace que categorizar las redes sea un desafío. Clasificar una red como amigable o neutral cuando en realidad es una amenaza puede proporcionarle demasiada libertad o acceso. Etiquetar erróneamente una red amiga o neutral como una amenaza puede provocar que se tomen acciones contra esa red que pueden tener consecuencias imprevistas.

d. Las redes están compuestas por personas que participan en una multitud de actividades, incluidas las sociales, políticas, monetarias, religiosas y personales. Estas redes humanas existen en todas las OE y, por lo tanto, las actividades de participación de la red se llevarán a cabo en todas las fases del conflicto y en toda la gama de operaciones.

e. La Figura III-2 muestra los resultados efectivos de utilizar acciones letales para contrarrestar las redes de amenazas y reducir su legitimidad en el OE. La Figura III-2 también muestra el efecto de las acciones no letales contra redes amigas y neutrales para aumentar su legitimidad en la OE.

Es importante recordar que las acciones no letales también pueden tener el efecto deseado cuando se utilizan contra redes amenazantes.

5.- REDES, VÍNCULOS Y GRUPOS DE IDENTIDAD

Todos los individuos son miembros de múltiples grupos de identidad superpuestos.

Estos grupos de identidad forman vínculos de afinidad y comprensión compartida, que pueden aprovecharse para formar redes con un propósito compartido. Estas redes pueden formarse en respuesta a amenazas percibidas al grupo de identidad, y las redes existentes pueden aprovechar las superposiciones entre el grupo de identidad central y otros grupos en el área operativa para ampliar su base de apoyo o atraer reclutas. Las redes con vínculos más fuertes y numerosos serán más resistentes a los esfuerzos externos que buscan dividir la red y tendrán una mayor motivación entre sus miembros. Muchas redes de amenazas dependen de vínculos familiares y tribales cuando reclutan para el núcleo interno de la red. Estos miembros han sido examinados durante años y es casi imposible recurrir a ellos. Para los analistas, identificar afiliaciones familiares y tribales ayuda a desarrollar un perfil objetivo del personal clave de la red. Incluso las redes criminales tenderán a estar densamente pobladas por un pequeño número de grupos identitarios interrelacionados.

a. Red Familiar. Algunos miembros o asociados tienen vínculos familiares. Estos vínculos pueden ser intergeneracionales.

b. Red Cultural. Los enlaces de red pueden compartir afinidades debido a la cultura, que incluyen idioma, religión, ideología, país de origen y/o sentido de identidad. Las redes pueden evolucionar con el tiempo desde una base cultural a una basada en la proximidad.

c. Red de Proximidad. La red comparte vínculos debido a vínculos geográficos de sus miembros (por ejemplo, vínculos anteriores en instituciones correccionales u otras instituciones o vivir dentro de regiones o vecindarios específicos). Los miembros también pueden

formar una red con proximidad a un área estratégico para sus intereses criminales (por ejemplo, un vecindario o un punto clave de entrada fronteriza). Puede haber una etnia dominante dentro del grupo, pero están juntos principalmente por razones distintas a la familia, la cultura o la etnia.

d. Red Virtual. Una red que puede no reunirse físicamente pero trabajar en conjunto a través de Internet u otros medios de comunicación, para fines legítimos o delictivos (por ejemplo, fraude en línea, robo o lavado de dinero).

e. Redes Especializadas. Las personas de esta red se reúnen para llevar a cabo actividades específicas basadas en las habilidades, experiencia o capacidades particulares que ofrecen. Esto puede incluir actividades delictivas.

6.- TIPOS DE REDES EN UN ENTORNO OPERACIONAL

Hay tres tipos generales de redes que se encuentran dentro de un área operativa: redes amigas, neutrales y hostiles/amenazantes. Una red también puede encontrarse en un estado de transición y, por tanto, difícil de clasificar. Para lograr con éxito los objetivos de la misión, el JFC debería considerar igualmente el impacto de las acciones en las fuerzas multinacionales y amigas, la población local, empresas criminales, así como el adversario. La inteligencia puede proporcionar al comandante la ubicación del adversario, pero si la planificación no considera el impacto de un ataque en la población local, el adversario podría ganar el doble de combatientes perdidos durante el ataque. Además, una comprensión y un modelo completos y precisos de las redes neutrales y cómo se interrelacionan con las redes de amenazas brinda a las fuerzas operativas mayores oportunidades para comprender, penetrar y atacar esas redes de amenazas. Proporcionar al comandante una variedad de capacidades letales y no letales (es decir, municiones de impacto contundente, dispositivos

acústicos/ópticos de granizo y advertencia, tapones para vehículos/embarcaciones) para dar forma al OE permite una respuesta variable al complejo entorno de seguridad.

a. Las redes amigas, se pueden dividir en dos grupos: organizaciones estadounidenses y aliadas (PN), y aquellas compuestas por la HN en la que se llevan a cabo las operaciones.

b. Las redes neutrales, , están compuestas por grupos generalmente benignos, que no están completamente asociados con unidades amigas ni alineados con la amenaza. Muchas veces, estas redes continuarán operando sin verse afectadas en gran medida por las actividades de amenazas u operaciones amigas. Por ejemplo, antes, durante y después de la caída de Francia en la Segunda Guerra Mundial, el metro de París, el servicio de taxi, los sistemas telefónicos, las discotecas, los bares y los restaurantes siguieron funcionando. El JFC debe tener en cuenta cómo las operaciones pueden afectar tanto positiva como negativamente a estas redes neutrales.

c. Las redes de amenazas, pueden estar compuestas por organizaciones criminales, insurgentes o terroristas, cada una de las cuales puede tener diferentes motivaciones para operar fuera de las normas sociales. También pueden ser entidades gubernamentales, organizaciones legales legítimas o cualquier persona que se oponga al logro de objetivos amistosos. Las redes de amenazas pueden entrelazarse formalmente o unirse cuando sean mutuamente beneficiosas.

Esta convergencia (o nexo) entre redes de amenazas ha fortalecido en gran medida la inestabilidad regional y ha permitido que las amenazas y alianzas aumenten su alcance operativo y poder hasta alcanzar proporciones globales.

7.- IDENTIFICAR UNA RED DE AMENAZAS

Las redes de amenazas a menudo intentan permanecer ocultas. ¿Cómo pueden los comandantes determinar no sólo qué redes se encuentran dentro de un área operativa, sino también cuáles representan la mayor amenaza? Al comprender las funciones de mantenimiento básicas, a menudo enmascaradas, de una red de amenazas determinada, los comandantes también pueden identificar redes individuales dentro de ella. Por ejemplo, todas las redes requieren comunicaciones, recursos y personas. Al comprender las funciones de una red, los comandantes pueden hacer suposiciones fundamentadas sobre su composición y determinar no sólo dónde están, sino también cuándo y cómo enfrentarse a ellas. Como se indicó anteriormente, existen muchas redes neutrales que son utilizadas tanto por fuerzas amigas como amenazantes; la parte difícil es determinar qué redes son una amenaza y cuáles no. El aspecto "buscar" de la metodología de focalización de buscar, reparar, finalizar, explotar, analizar y difundir (F3EAD) se utiliza inicialmente para descubrir e identificar redes dentro del OE. La metodología F3EAD no sólo se utiliza para identificar objetivos procesables específicos; también se utiliza para descubrir la naturaleza, funciones, estructuras y números de redes dentro del OE.

Un producto JIPOE exhaustivo, junto con una evaluación, observación y recopilación de inteligencia de todas las fuentes “sobre el terreno”, conducirá en última instancia a una comprensión de la OE y permitirá al comandante visualizar la red.

CAPÍTULO IV

PLANIFICACIÓN PARA CONTRASTAR LAS REDES DE AMENAZA

1.- PREPARACIÓN DE INTELIGENCIA CONJUNTA DEL ENTORNO OPERACIONAL Y REDES DE AMENAZAS

a. Una evaluación integral y multidimensional de la OE ayudará a los comandantes y al estado mayor a descubrir las características y actividades de la red de amenazas, desarrollar operaciones enfocadas para atacar las vulnerabilidades, anticipar mejor las consecuencias previstas y no deseadas de las actividades de la red de amenazas y las contramedidas amistosas, y determinar los medios apropiados para evaluar progreso hacia los objetivos establecidos. JIPOE es el primer paso para identificar los elementos esenciales que constituyen la OE y se utiliza para planificar y realizar operaciones contra redes de amenazas. El objetivo del análisis JIPOE de redes de amenazas es ayudar a caracterizar aspectos de las redes.

b. Los comandos y estados mayores de fuerzas, componentes y apoyo conjuntos utilizan productos JIPOE para preparar estimaciones utilizadas durante el análisis de la misión y la selección de cursos de acción amistosos (COA). Los comandantes adaptan el análisis JIPOE según la misión. Como se analizó anteriormente, el mejor COA puede no ser destruir toda la red o las células de una amenaza; poblaciones amigas o neutrales pueden utilizar la misma red o células, y destruirlas tendría un efecto negativo. Un análisis exhaustivo de la JIPOE y de la red ayudará a los comandantes a elegir el enfoque más eficaz..

2.- COMPRENDER LA RED DE AMENAZAS

a. La amenaza tiene su propia versión de la OE que busca moldear para mantener el apoyo y alcanzar sus objetivos. En muchos casos, el desafío que enfrentan las fuerzas amigas se complica por el simple hecho de que porciones significativas de la población podrían

considerar la amenaza como el “equipo local”. Para neutralizar o derrotar una red de amenazas, las fuerzas amigas deben hacer más que comprender cómo opera la red de amenazas, los objetivos de su organización y su lugar en el orden social; también deben comprender cómo la amenaza está moldeando su entorno para mantener el apoyo popular, reclutar y recaudar fondos. El primer paso para comprender una red es desarrollar un perfil de red mediante el análisis de sus factores críticos.

b. COG y Análisis de Factores Críticos (CFA). Una de las tareas más importantes que enfrentan el JFC y su personal durante la planificación es identificar y analizar la red de la amenaza y, en la mayoría de los casos, los factores críticos de la red y los COG. Un objetivo es siempre vinculado a un COG. Al analizar la red y los COG de la red, se debe recordar que no sólo habrá diferentes COG en diferentes niveles, sino que es probable que estén anidados. La determinación del COG de una red o célula, como finanzas o logística, puede También será necesario para una comprensión general de la red de amenazas. Lo que complica las cosas para el JFC es la posible convergencia de redes criminales, terroristas e insurgentes, todas con diferentes COG.

c. Plantilla de función de red. La creación de una plantilla de función de red es un método para organizar información conocida sobre la red asociada con la estructura y funciones de la red. Al desarrollar una plantilla de función de red, la información puede entenderse inicialmente y luego utilizarse para facilitar la CFA. La creación de una plantilla de función de red no es un requisito para realizar CFA, pero ayuda al personal a visualizar las interacciones entre las funciones y la estructura de soporte dentro de una red. Sería necesario desarrollar plantillas de funciones de red para redes individuales que tengan propósitos específicos, pero que aún involucren a las mismas personas, ya que las funciones, serían diferentes si las mismas

personas estuvieran involucradas con dispositivos explosivos improvisados (IED) o algo más.

3.- ANÁLISIS DE FACTORES CRÍTICOS

a. CFA es un marco analítico para ayudar a los planificadores a analizar e identificar un COG y ayudar a la planificación operativa. Los factores críticos son los CC, los requisitos críticos (CR) y los CV. El marco CFA se desarrolló para respaldar el análisis de los adversarios, pero se ha adaptado para respaldar al personal en su análisis de cualquier red dentro de la OE. Dado que se entiende que las redes comprenden la dimensión humana de los OE complejos, para comprender mejor el impacto de estos factores en la operación, debemos correlacionar los factores con el análisis del OE para determinar las variables críticas de la red a analizar. (ver Figura IV-1). La terminología clave para CFA incluye:

(1) El COG para el análisis de redes es un conglomerado de elementos tangibles y/o factores intangibles que no sólo motiva a los individuos a unirse a una red, sino que también promueve su voluntad de actuar para lograr los objetivos de la red y alcanzar el estado final deseado. A menudo será difícil dirigirse directamente a un COG para redes debido a su complejidad y accesibilidad.

(2) Los CC son las habilidades primarias esenciales para lograr el objetivo de la red dentro de un contexto determinado. El análisis para identificar CC para una red solo es posible si se comprende la estructura y las funciones de una red, lo cual está respaldado por otros métodos de análisis de red.

(3) Las CR son las condiciones, recursos y medios esenciales que la red requiere para realizar la CC. Estas cosas se usan o consumen para llevar a cabo acciones, lo que permite que un CC funcione por completo. Las redes requieren recursos para actuar y funcionar. Estos

recursos incluyen personal, equipos, dinero y cualquier otro bien que respalde los CC de la red.

(4) Los CV son CR o componentes de los mismos que son deficientes o vulnerables a la neutralización, interdicción o ataque de una manera que logre resultados decisivos. Los CV de una red cambiarán a medida que las redes se adapten a las condiciones dentro de la OE. La identificación de CV para una red debe considerarse durante el proceso de selección, pero no necesariamente puede ser un punto focal de operaciones sin un análisis adicional.

b. La creación de una plantilla de función de red implica varios pasos:

(1) Paso 1: Identificar el estado final deseado de la red. El estado final deseado de la red está asociado con el catalizador que apoyó la formación de la red. La pregunta principal que el personal debe responder es ¿cuáles son los objetivos de la red? Los siguientes son ejemplos de estados finales deseados para varias organizaciones:

(a) Reemplazar el gobierno del país X por un califato islámico.

(b) País liberador X.

(c) Controlar los campos petroleros en la región Y.

(d) Establecer una hegemonía regional.

(e) Imponer la Sharia a la aldea Z.

(f) Expulsar a las fuerzas multinacionales de la región.

(2) Paso 2: Identificar posibles formas o acciones (COA) que pueden alcanzar el estado final deseado. Este paso se refiere a las formas en que una red puede tomar medidas para alcanzar el estado final deseado a través de sus COA. De manera similar a cómo el personal analiza una fuerza convencional para determinar el COA probable que esa fuerza tomará, esto también debe hacerse para las redes que se

seleccionan para participar. Es importante señalar que cada red tendrá una variedad de opciones disponibles y su probable COA estará asociado con la intención de los miembros de la red. Ejemplos de formas para algunas redes pueden incluir:

(a) Llevar a cabo una operación o campaña de insurgencia.

(b) Fortalecer la capacidad de la PN.

(c) Atacar con fuerzas militares convencionales.

(d) Realizar actos de terrorismo.

(e) Aprovechar los campos petroleros en Y.

(f) Destruir las fuerzas enemigas.

(g) Pueblo defensor Z.

(h) Intimidar a los dirigentes locales.

(i) Controlar las rutas de contrabando.

(j) Sobornar a funcionarios

(3) Paso 3: Identificar las funciones que posee la red para tomar acciones.

Utilizando la plantilla de funciones de red del análisis anterior, el personal debe refinar este análisis para identificar las funciones dentro de la red que podrían usarse para respaldar las posibles formas o COA de la red. Las funciones identificadas dan como resultado una lista de CC.

Ejemplos de elementos asociados con las funciones de una red que respaldarían la lista de ejemplos de formas identificadas en el paso anterior son:

(a) Llevar a cabo una operación o campaña de insurgencia: los insurgentes están armados y puede realizar ataques.

(b) Fortalecimiento de la capacidad de la PN: fuerzas y capacidad de entrenamiento disponibles.

(c) Atacar con fuerzas militares convencionales: las fuerzas militares están en una nivel operativo con C2 implementado.

(d) Realizar actos de terrorismo: los miembros de la red poseen el conocimiento y activos para tomar medidas.

(e) Tomar los campos petroleros en Y: la red posee la capacidad de realizar ataques coordinados.

(f) Destruir fuerzas enemigas: la red tiene los recursos para identificar, localizar y destruir al personal enemigo.

(g) Pueblo defensor Z: la red posee las capacidades y la presencia para llevar a cabo la defensa.

(h) Intimidar a los líderes locales: la red tiene libertad de maniobra y acceso a los líderes locales.

(i) Controlar las rutas de contrabando: la esfera de influencia y las capacidades de la red permiten el control.

(j) Sobornar a funcionarios: la red tiene acceso a funcionarios y recursos para facilitar sobornos.

(4) Paso 4: Enumerar los medios o recursos disponibles o necesarios para que la red ejecute CC. El propósito de este paso es determinar los CR de la red. Nuevamente, esto es respaldo del análisis inicial realizado para la red, mapeo de red, análisis de enlaces, SNA y plantilla de función de red. Con base en los CC identificados para la red, el personal debe responder a la pregunta ¿qué recursos debe poseer la red para emplear los CC identificados? La lista de CR puede ser

extensa, dependiendo de la capacidad que se analice. Los siguientes son ejemplos de CR que pueden identificarse para una red:

(a) Un grupo de combatientes extranjeros.

(b) Un gran ejército convencional.

(c) Una gran formación militar convencional (por ejemplo, un cuerpo blindado).

(d) artefactos explosivos improvisados.

(e) Combatientes locales.

(f) Armas y municiones.

(g) Fondos.

(h) Liderazgo.

(i) Una red de apoyo local.

(5) Paso 5: Correlacionar los CC y CR con la evaluación de la OE para identificar aspectos críticos variables.

(a) La comprensión de los CC y CR de varias redes se puede utilizar por sí sola en la planificación y la focalización, pero existe la posibilidad de perder oportunidades o aceptar riesgos adicionales, no se entiende hasta que el personal relaciona estos elementos con el análisis de la OE. El análisis de la OE realizado como parte de la planificación se utiliza para apoyar la identificación de variables críticas. Durante el análisis de OE, el estado mayor identifica las variables críticas de la OE que están relacionadas con la misión y los objetivos del comandante. Estas variables se utilizan para describir el estado final deseado por el comandante y se utilizan para respaldar la evaluación de las operaciones.

Conocer las variables críticas para las redes ayuda al personal a centrar sus esfuerzos en la recopilación y la focalización de la red, lo cual es necesario para gestionar activos limitados. El árbol lógico proporciona un método para realizar este análisis.

(b) Una variable crítica puede ser un CC, CR o CV para múltiples redes.

Comprender esto se producirá en el siguiente paso de CFA. Los siguientes son ejemplos de variables críticas que pueden identificarse para las redes:

1. Un grupo de combatientes extranjeros está expuesto a un posible enfrentamiento.

2. Se localiza una gran formación militar convencional (por ejemplo, un cuerpo blindado) y se identifica el COA probable.

3. El fabricante y los recursos del IED están identificados y pueden ser neutralizados.

4. Las rutas de viaje y reclutamiento de los combatientes locales son identificables.

5. Las fuentes de suministro de armas y municiones son identificables.

6. Los fondos están ubicados y existe posibilidad de incautación.

7. El liderazgo está identificado y accesible para el compromiso.

8. Se identifica y comprende una red de apoyo local a través del análisis.

(6) Paso 6: Comparar y contrastar los CR de cada red analizada. Este paso de CFA solo se puede realizar después de que se haya completado el análisis completo de la red para todas las redes seleccionadas dentro de la OE. Para comparar y contrastar es necesario disponer de la

información del análisis de cada red. La intención de correlacionar las variables críticas para cada red permite comprender:

(a) Posibles efectos deseados del compromiso de primer y segundo orden.

(b) Posibles efectos no deseados de primer y segundo orden del compromiso.

(c) Oportunidades de participación directa.

(d) Oportunidades de participación indirecta.

(7) Paso 7: Identificar los CV para la red. La identificación de los CV de una red se completa analizando cada CR de la red con respecto a su criticidad, accesibilidad, recuperabilidad y adaptabilidad. Este análisis se realiza desde la perspectiva de la red teniendo en cuenta las amenazas dentro del OE que pueden afectar la red que se está analizado. Realizar el análisis desde esta perspectiva permite al personal identificar CV para cualquier tipo de red (amigable, neutral o amenazante).

(a) Criticidad. Un CR que, cuando se ve afectado por una amenaza, produce una degradación de la estructura, función o impacto de la red en su capacidad para sostenerse. La criticidad considera la importancia del CR para la red y se deben considerar las siguientes preguntas al realizar este análisis

1. ¿Qué impacto tendrá la eliminación del CR en la estructura de la red?

2. ¿Qué impacto tendrá la eliminación del CR en las funciones de la red?

3. ¿Qué función se ve afectada al activar el CR?

4. ¿Qué efecto tiene la RC en otras redes?

5. ¿El CR es un CR para otras redes? ¿De ser así, cuáles?

6. ¿Cómo se relaciona el CR con las condiciones de sostenimiento?

(b) Accesibilidad. Un CR es accesible cuando las capacidades de una amenaza a la red pueden emplearse directa o indirectamente para atacar al CR. La accesibilidad de la RC en algunos casos es un factor limitante para la verdadera vulnerabilidad de una RC. Hay muchos casos en los que no se puede acceder directamente a un CR debido a límites del espacio de batalla, fronteras internacionales o algún nivel de protección reforzada. Obtener este conocimiento como parte del CFA ayudará al personal a decidir qué objetivos recomendar al comandante. El personal debe considerar las siguientes preguntas al analizar la accesibilidad de un CR:

1. ¿Dónde está la CR?

2. ¿Está protegida la RC?

3. ¿El CR es estático o móvil?

4. ¿Quién interactúa con el CR? ¿Con qué frecuencia?

5. ¿Se encuentra el CR en el área operativa de la amenaza a la red?

6. ¿Puede el CR participar con capacidades de amenaza?

7. Si el CR es inaccesible, ¿existen CR alternativos que, si se ven afectados por una amenaza, produzcan un efecto similar en la red?

(c) Recuperabilidad. La cantidad de tiempo que la red necesita para reparar o reemplazar un CR afectado por una capacidad de amenaza. El análisis de la RC en cuanto a recuperabilidad está asociado a la capacidad de la red para regenerarse cuando se han eliminado o dañado componentes de su estructura. Esto juega un papel en la naturaleza adaptativa de una red, pero no debe confundirse con el

último aspecto del análisis de los CV. El personal debe considerar las siguientes preguntas al analizar la recuperabilidad de un CR:

1. Si se elimina CR:

a. ¿Se puede reemplazar el CR?

b. ¿Cuánto tiempo llevará reemplazarlo?

c. ¿El reemplazo cumple con los requisitos estructurales y funcionales de los niveles de la red?

d. ¿Necesitará la red hacer ajustes para implementar el reemplazo del CR?

2. Si CR está dañado:

a. ¿Se puede reparar el CR?

b. ¿Cuánto tiempo se tarda en reparar?

c. ¿El CR reparado devolverá la red a sus niveles estructurales y funcionales anteriores?

(d) Adaptabilidad. La capacidad de una red (con la que está asociada la CR) para cambiar en respuesta a las condiciones en la OE provocadas por las acciones de una amenaza adoptada contra ella, manteniendo al mismo tiempo su estructura y función. El análisis del CR para la adaptabilidad está asociado con condiciones dentro del OE como resultado de una amenaza a la red. Dado que los CR pueden ser cualquier tipo de recurso o condición necesaria para que la red sobreviva y funcione, este aspecto permite al personal analizar un CR de esa naturaleza con respecto a su vulnerabilidad potencial. La adaptabilidad considera la capacidad de la red para cambiar o modificar sus funciones, modificar su catalizador, cambiar el enfoque en audiencias potencialmente receptivas o realizar cualquier otro cambio para adaptarse a las condiciones del OE. El personal debe

considerar las siguientes preguntas al analizar la recuperabilidad de un CR:

1. ¿Puede el CR cambiar su estructura manteniendo su función?

2. ¿Está el CR vinculado a un CC que podría provocar que se adapte como respuesta normal a un cambio en un CC (ya sea debido a un compromiso hostil o a un cambio natural provocado por el ajuste de una red amiga a ese CC)?

3. ¿Se puede cambiar el CR para cumplir con una CC emergente o función para la red?

4.- VISUALIZACIÓN DE REDES DE AMENAZAS

a. Mapeo de la red. El mapeo de las redes de amenazas comienza detallando las amenazas principales (por ejemplo, grupo terrorista, cártel de la droga, grupo de lavado de dinero). El mapeo rutinariamente comienza con personas y lugares y luego agrega funciones, recursos y actividades. El mapeo comienza como un simple vínculo entre dos nodos y avanza para representar la estructura organizacional (ver Figura IV-4). Es posible que los propios miembros individuales de la red no sean conscientes de la estructura organizativa. Será raro que se recopile suficiente inteligencia e información para representar una red de amenazas completa y todas sus células. Comprender los COG y los factores críticos permite optimizar la recopilación de inteligencia y los esfuerzos analíticos para respaldar las necesidades de planificación del JFC. Las operaciones posteriores generarán inteligencia adicional y esfuerzos de explotación que arrojarán pistas valiosas para respaldar el mapeo adicional de redes.

Este será un proceso continuo a medida que las propias redes se transformen y se adapten a su entorno y a las operaciones de las fuerzas conjuntas. Para desarrollar y emplear opciones estratégicas en el teatro de operaciones, el comandante debe comprender la serie de

relaciones complejas e interconectadas que operan dentro de la OE. Una forma de desarrollar soluciones es ver estos desafíos interrelacionados desde una perspectiva de sistemas. En este análisis de sistemas, se debe considerar la relación entre todos los aspectos del sistema.

Para obtener más información, consulte el Apéndice E, "Explotación para respaldar la lucha contra las redes de amenazas" y el Apéndice G, "Análisis de redes sociales".

(1) Red de Cadenas. La cadena o red de líneas se caracteriza por personas, bienes o información que se mueven a lo largo de una línea de contactos separados con comunicación de extremo a extremo que viaja a través de nodos intermedios.

(2) Red Estrella o Hub. La red central, estrella o rueda, como en una franquicia o un cartel, se caracteriza por un conjunto de actores vinculados a un nodo o actor central (pero no jerárquico) que debe comunicarse y coordinarse con los miembros de la red a través del nodo central.

(3) Red multicanal. La red de todos los canales, o de matriz completa, se caracteriza por una red colaborativa de grupos donde todos se conectan con los demás.

b. Mapeo de múltiples redes. Cada red puede ser diferente en estructura y propósito. Normalmente, la estructura de la red está completamente mapeada y las celdas se muestran en relación con la red más grande. Mapear cada red requiere mucho tiempo y trabajo, por lo que el personal debe considerar cuidadosamente la utilidad de cuánto tiempo y esfuerzo deben asignar para lograr mapear las redes de apoyo y dónde enfocar sus esfuerzos para que brinden una respuesta oportuna e identifiquen con precisión las relaciones y los nodos críticos importantes para los esfuerzos de disrupción.

c. Identificar los factores que influyen en la red. Los factores que influyen en la red (o varias redes) dentro de una OE pueden identificarse en gran medida por las condiciones creadas por las actividades de la red. Estas condiciones son las que influyen en los comportamientos, actitudes y vulnerabilidades de poblaciones específicas. Factores como las actividades de información sobre amenazas (propaganda) pueden ser uno de los principales factores de influencia, pero también lo son actividades como el secuestro, la exigencia de pagos por protección, la construcción de lugares de culto, la destrucción de sitios históricos, la construcción de escuelas, la prestación de servicios básicos, la denegación de la libertad de movimiento, acoso, actividades de drogas ilegales, prostitución, etc. Para identificar los factores que influyen, un método probado es observar primero las condiciones de una población o grupo específico, determinar cómo esas condiciones crean/forzan el comportamiento y luego determinar las causas de las condiciones.

Una vez que se identifican los factores de influencia, el siguiente paso es determinar si las condiciones se pueden cambiar y/o si no es posible, determinar si existe un comportamiento alternativo y viable disponible para la población o grupo.

d. Para producir una visión holística de las redes amenazantes, neutrales y amigables en su conjunto dentro de una OE más grande se requiere un análisis para describir cómo se interrelacionan estas redes. Lo más importante para este análisis es describir las relaciones dentro y entre las diversas redes que afectan directa o indirectamente la misión. Aunque la dirección de inteligencia de un estado mayor conjunto (J-2) gestiona el proceso JIPOE, otras direcciones y agencias pueden aportar experiencia valiosa para desarrollar y evaluar las complejidades de la OE.

e. Colaboración. En la mayoría de los esfuerzos por producir una visión integral de las redes, es posible que ciertos tipos de datos o información

no estén disponibles para explicar o articular correctamente con gran detalle la naturaleza de las relaciones, capacidades, motivos, vulnerabilidades o comunicaciones y movimientos. Corresponde a las organizaciones de inteligencia colaborar y compartir información, datos y análisis, y trabajar en estrecha colaboración con socios interinstitucionales para responder a estas brechas de inteligencia. Antes de desarrollar o promover COA, los tomadores de decisiones siempre deben estar informados sobre el nivel de certeza y precisión de los datos y fuentes de inteligencia; Los socios interinstitucionales deben identificar claramente y discutir con frecuencia las lagunas de inteligencia y las ambigüedades en aspectos de las redes de amenazas.

5.- CRITERIOS DE EVALUACIÓN DE FOCALIZACIÓN

Una vez que se mapea la red, el JFC y el personal identifican los nodos de la red y determinan su idoneidad para ser atacados. Una herramienta útil para determinar la idoneidad de un objetivo para un ataque es el análisis de criticidad, accesibilidad, recuperabilidad, vulnerabilidad, efecto y reconocibilidad (CARVER). CARVER es un sistema subjetivo y comparativo que pesa seis factores característicos del objetivo y los clasifica para tomar decisiones de orientación y planificación. El análisis CARVER se puede utilizar en los tres niveles de guerra: táctico, operativo y estratégico. Una vez que se establecen los criterios de evaluación de objetivos, los analistas de objetivos utilizan un sistema de calificación numérica (1 a 5) para clasificar los factores CARVER para cada objetivo potencial. En un sistema de numeración del uno al cinco, una puntuación de cinco indicaría una puntuación muy deseable, mientras que una puntuación de uno reflejaría una puntuación indeseable. El analista debe adaptar los criterios y el esquema de adaptarse a la situación estratégica, operativa o táctica particular. En el párrafo 6, “Evaluación de la red nocional”, se proporciona un análisis CARVER relacionado con la red nocional. El método CARVER, tal como se aplica a las redes, proporciona un

modelo numérico basado en gráficos para determinar la importancia de involucrar a un objetivo identificado, utilizando un análisis cualitativo, basado en siete factores:

a. Afiliaciones de red. Las afiliaciones de red identifican cada red de interés asociada con el CR que se está evaluando. La importancia de comprender las afiliaciones a la red de un objetivo potencial surge de las interrelaciones entre las redes.

La evaluación de un objetivo potencial desde la perspectiva de cada red afiliada proporcionará al personal conjunto posibles efectos de segundo y tercer orden tanto en las redes de amenazas objetivo como en otras redes interrelacionadas dentro de la OE. Por ejemplo, la eliminación de una pieza clave de infraestructura afectará en última instancia a algo más que la red de amenazas.

b. Criticidad. La criticidad es una CR que, cuando se ve afectada por una amenaza, produce una degradación de la estructura, función o impacto de la red en su capacidad para sostenerse. La evaluación de la criticidad de un objetivo potencial debe realizarse desde la perspectiva de la asociación directa del objetivo o de la necesidad de una red específica. Dependiendo de las funciones y la estructura de la red, la criticidad de un objetivo potencial puede diferir entre redes. Por lo tanto, se debe evaluar la criticidad y asignar una puntuación a cada afiliación a la red. Si el analista ha completado el CFA para las redes de interés, se debería haber analizado la criticidad durante la identificación de los CV. El resultado del CFA simplemente tendría que aplicarse a la matriz CARVER (red) para cada objetivo potencial.

c. Accesibilidad. Un CR es accesible cuando las capacidades de una amenaza a la red pueden emplearse directa o indirectamente para atacar al CR. Los CR inaccesibles pueden requerir objetivos alternativos para producir los efectos deseados. La accesibilidad de un objetivo potencial seguirá siendo la misma, independientemente de su

afiliación a la red. Este elemento de CARVER no requiere una evaluación separada del objetivo potencial para cada red. Al igual que la criticidad, la accesibilidad se habrá evaluado si el analista ha realizado un CFA para la red como parte del análisis de la red. El resultado del CFA simplemente tendría que aplicarse a la matriz CARVER (red) para cada objetivo potencial.

d. Recuperabilidad. La recuperabilidad es la cantidad de tiempo que la red necesita para reparar o reemplazar un CR que está afectado por una capacidad de amenaza. La recuperabilidad se analiza durante CFA para determinar la vulnerabilidad de un CR para la red. Dado que CARVER (red) se aplica para evaluar los objetivos potenciales con cada red afiliada, la evaluación de la recuperabilidad será diferente para cada red. Lo que afecta la recuperabilidad es la función de la red de regenerar miembros o reemplazar los activos necesarios con sustitutos adecuados. El resultado de CFA se puede utilizar para completar esta parte de la matriz CARVER (red).

e. Vulnerabilidad. Un objetivo es vulnerable si el elemento operativo tiene los medios y la experiencia para atacarlo con éxito. Al determinar la vulnerabilidad de un objetivo, es necesario comparar la escala del componente crítico con la capacidad del elemento atacante para destruirlo o dañarlo. La evaluación de la vulnerabilidad de un objetivo potencial está respaldada por el análisis realizado durante el CFA y puede usarse para completar esta parte de la matriz CARVER (red). La vulnerabilidad de un objetivo potencial constará de un solo valor. Independientemente de la red de afiliación, la vulnerabilidad se centra en evaluar las capacidades disponibles para llevar a cabo acciones efectivas sobre el objetivo.

f. Efecto. Esto evalúa el efecto potencial sobre la estructura, función y sostenimiento de una red al involucrar al CR en su relación con cada red afiliada. El nivel de efecto debe considerar tanto el efecto de primer orden sobre el objetivo mismo como el efecto de segundo orden sobre

la estructura y función de la red. El personal conjunto también debe considerar la duración durante la cual se mantendrá el efecto en la red al atacar al objetivo.

Considere los aspectos identificados en las consideraciones de adaptabilidad para la evaluación de CV durante el CFA.

g. Reconocibilidad. La reconocibilidad es el grado en que un CR puede ser reconocido por un elemento operativo y/o una recopilación de inteligencia en diversas condiciones. La reconocibilidad de un objetivo potencial seguirá siendo la misma, independientemente de la red de afiliación.

6.- EVALUACIÓN DE RED NACIONAL

a. El propósito del análisis de objetivos convencional (y el uso de CARVER) es determinar los sistemas o subsistemas críticos del enemigo a atacar para destruir o degradar progresivamente la capacidad de guerra y la voluntad de luchar del adversario. En las operaciones contra redes amenazantes, el comandante determina los efectos deseados en la red (neutralizar, interrumpir o derrotar, etc.) y si la capacidad y la oportunidad para atacar eficazmente están disponibles.

b. Utilizando el análisis de red, un comandante identifica los nodos de amenazas críticas que operan dentro del OE. Un análisis CARVER determina la viabilidad de atacar cada nodo (idealmente simultáneamente). Si bien cada valor de CARVER es subjetivo, el análisis detallado permite a los planificadores asignar un valor realista. Por ejemplo, el comandante determina que los ataques letales directos a los campos de entrenamiento terrorista no son una opción para el JFC debido a limitaciones o restricciones diplomáticas o políticas (ver Figura IV-6). Luego, el comandante y el estado mayor analizan otros aspectos de la red y, por ejemplo, determinan si pueden alterar el

material necesario para el entrenamiento, impedir el movimiento de los alumnos o instructores al lugar de entrenamiento, o influir en otros grupos para que nieguen el acceso a la red. área.

c. El JFC y su personal analizan metódicamente cada nodo de red identificado y asignan una calificación numérica a cada uno. En este ejemplo teórico (ver Figura IV-7), se determina que las células de comunicaciones y quienes financian las operaciones de amenazas constituyen los mejores objetivos para atacar. El método y en qué medida la fuerza conjunta atacará estos nodos depende del estado final deseado de las actividades de la CTN y de las capacidades y autoridades de la fuerza conjunta. En este caso particular, el JFC se coordinará con otros instrumentos del poder nacional estadounidense y socios internacionales para atacar las células de comunicaciones y los canales e instituciones bancarias.

d. La planificación de operaciones contra redes de amenazas no difiere de la planificación militar estándar. Estas operaciones aún apoyan la misión más amplia del JFC y rara vez son independientes. La identificación de redes de amenazas requiere un análisis detallado y una consideración de los efectos de segundo y tercer orden. Es importante recordar que la propia organización amenazante es el objetivo final y sus redes son simplemente un medio para lograrlo. Neutralizar una red determinada puede resultar más beneficioso para el cumplimiento de la misión del JFC que destruir un único nodo de red multiusuario. Los planes más eficaces exigen operaciones simultáneas en redes centradas en múltiples nodos y funciones de red. La simultaneidad de múltiples líneas de operación (LOO) y líneas de esfuerzo (LOE) pone una amenaza a la defensiva y altera los planes de manera más eficiente que los esfuerzos fragmentados contra nodos individuales. El análisis CARVER proporciona un método para el análisis de nodos de red y criterios de selección de objetivos.

7.- CONTRARRESTAR LAS REDES DE AMENAZAS A TRAVÉS DE LA PLANIFICACIÓN DE FASES

Como se analizó anteriormente, los comandantes ejecutan actividades de la CTN en todos los niveles de la guerra. Los JFC pueden planificar y realizar actividades de CTN a lo largo de todas las fases de una operación determinada. Al comprender las diversas redes de amenazas en la OE a través del JPP, los JFC y su personal desarrollan una serie de medidas prudentes (factibles, adecuadas y aceptables).

Las acciones del CTN se ejecutarán en conjunto con otras actividades escalonadas. Dado el rápido ritmo de las operaciones y el constante cambio de OE, los comandantes deben poder ejecutar varias actividades de la CTN simultáneamente y no sólo de forma secuencial. Dado que los comandantes pueden encontrarse simultáneamente dirigiendo operaciones de configuración en un área, dominando actividades en otra y disuadiendo operaciones en otra más, las opciones CTN del JFC deben ser adaptables a múltiples situaciones y completamente sincronizadas. Por ejemplo, la sobreasignación de recursos finitos, como las plataformas de inteligencia de señales (SIGINT), a una sola fase de una operación puede afectar negativamente el éxito en otra fase. Las redes de amenazas se pueden contrarrestar utilizando una variedad de enfoques y medios. Al principio de la operación o campaña, el concepto de operaciones se basará en un esfuerzo internacional sincronizado e integrado (USG, PN y HN) para garantizar que las condiciones en el OE no potencien una red de amenazas y le nieguen a la red los recursos que necesita. requiere ampliar sus operaciones e influencia. A medida que la amenaza aumente y las condiciones se deterioren, el plan se ajustará para incluir una gama más amplia de acciones y un aumento en el nivel y el enfoque de la focalización en los nodos críticos de la red identificados: personas y actividades. Se debe mantener una presión constante sobre las funciones críticas de la red para negarles la

iniciativa y alterar su ritmo de funcionamiento. La Figura IV-8 muestra la construcción de la fase del plan de operación hipotético para operaciones conjuntas. Es posible que algunas fases no se utilicen durante las actividades del CTN.

a. Forma (Fase 0)

(1) La acción unificada es la clave para dar forma a la OE. El objetivo es negar a la red de amenazas los recursos necesarios para expandir sus operaciones y reducirlas hasta un punto en el que ya no representen una amenaza directa a la estabilidad regional/local, al tiempo que influye en la red para que reduzca o redirija sus objetivos amenazantes. Las operaciones de configuración contra las redes de amenazas consisten en esfuerzos para influir en sus objetivos, disuadir el crecimiento, el patrocinio estatal, el refugio o el acceso a los recursos a través de los esfuerzos unificados de socios interinstitucionales, regionales e internacionales, así como de las autoridades civiles de la HN. Se toman acciones para identificar elementos clave en la OE que pueden usarse para aprovechar el apoyo al gobierno u otras redes amigas que deben controlarse para negarle a la amenaza una ventaja operativa. Se debe analizar el OE para identificar el apoyo a la red de amenazas, así como el de las redes amigas y neutrales relevantes. Los socios interinstitucionales/internacionales ayudan a identificar los componentes clave de la red, niegan el acceso a recursos (generalmente externos al país) y persuaden a otros actores (legítimos e ilícitos) para que suspendan el apoyo a la amenaza. SIGINT, la inteligencia de código abierto (OSINT) y la inteligencia humana (HUMINT) son las principales fuentes de inteligencia de información procesable. Es necesario reforzar la legitimidad del gobierno en el área operativa. Los esfuerzos para reforzar al gobierno buscan identificar las fuentes de fricción dentro de la sociedad que pueden reducirse mediante la intervención gubernamental. Las iniciativas del DOD podrían incluir ayudar a la HN a llevar a cabo la explotación del sitio y establecer un programa de base

de datos biométrica para los participantes en amenazas conocidas. Las operaciones en la fase 0 establecen las condiciones para las fases siguientes; dar forma a las percepciones de amenazas, redes amistosas y neutrales; e intentar aislar e influir en las redes de amenazas a través de medios diplomáticos, informativos, militares y económicos. Por ejemplo, el JFC puede dar forma a la OE influyendo en las percepciones de la audiencia objetivo (red neutral) sobre los beneficios de oponerse a la red de amenazas y apoyar a su propio gobierno y fuerza conjunta (red amiga). Muchas actividades de configuración de la fase I deben coordinarse durante la fase 0 debido a amplios requisitos legales e interinstitucionales. Las operaciones técnicas especiales, las operaciones en el ciberespacio, el engaño militar y MISO son IRC eficaces que se utilizan para moldear la toma de decisiones del adversario y del adversario potencial. Debido a la competencia de recursos y la posible falta de IRC disponibles, ejecutar IO durante la fase 0 puede ser un desafío. Por esta razón, se debe considerar cómo se pueden integrar los IRC como parte del enfoque de todo el gobierno para dar forma efectiva al entorno de información y lograr la información del comando de objetivos. La configuración de las operaciones también puede incluir actividades de cooperación en materia de seguridad diseñadas para fortalecer las capacidades y capacidades de la PN o regionales que contribuyan a una mayor estabilidad.

La configuración de las operaciones debe centrarse en cambiar las condiciones que fomentan el desarrollo de adversarios y amenazas.

(2) Durante la fase 0 (conformación), el análisis de la red de amenazas del J-2 proporciona inicialmente una descripción amplia de la estructura de la organización de amenazas subyacente; identifica las funciones críticas, los nodos y las relaciones entre las actividades de la amenaza y la sociedad en general; y pinta un cuadro de las relaciones “en promedio”. Busca desarrollar detalles sobre la estructura interna y

las relaciones externas de la red. Algunas de las acciones de la CTN requieren esfuerzos sostenidos y a largo plazo, como abordar el reclutamiento en comunidades específicas a través de programas de desarrollo. Es esencial que la amenaza se desvincule del apoyo dentro de las sociedades afectadas. Los elementos críticos en las redes operativas de la amenaza deben identificarse e interrumpirse para afectar su ritmo operativo. Incluso cuando las fuerzas están comprometidas, el comandante continúa dando forma a la OE utilizando diversos medios para eliminar la amenaza y emprender acciones, en cooperación con socios interinstitucionales y multinacionales, para reforzar el gobierno legítimo a los ojos de la población.

(3) El J-2 busca identificar y aprovechar fuentes de información que puedan proporcionar detalles sobre la red de amenazas y su relación con las estructuras políticas, económicas y sociales regionales/locales que pueden apoyarla y sostenerla. Estas fuentes de información incluyen departamentos y agencias del Gobierno, personal y organizaciones de la HN (incluidas las autoridades civiles) y la PN, y fuerzas de operaciones especiales (SOF) con experiencia en el país. Las ONG pueden servir como fuente de información, aunque en algunos casos pueden ser reacias a coordinarse con el gobierno de los Estados Unidos porque puede existir la percepción de que la coordinación comprometería su neutralidad, independencia y seguridad.

(4) Compartir información e inteligencia con socios es primordial, ya que la recopilación, explotación y análisis contra redes de amenazas requiere mucho más tiempo que contra adversarios militares tradicionales. El intercambio de información con los socios debe equilibrarse con la seguridad de las operaciones y no puede realizarse en todos los casos. El intercambio de inteligencia entre CCDR a través de zonas regionales y funcionales proporciona una imagen global de las redes de amenazas que no están limitadas por la geografía. Los

esfuerzos de inteligencia dentro de la fase de configuración muestran vínculos de la red de amenazas en términos de liderazgo, organización, tamaño, alcance, logística, financiamiento, alianzas con otras redes y membresía. Esto ayuda enormemente al JFC a comprender las redes de amenazas y el CTN.

b. Disuadir (Fase I). La intención de esta fase es disuadir la acción, la formación o el crecimiento de la red de amenazas demostrando capacidades y determinación de socios, aliados, multinacionales y fuerzas conjuntas. Muchas acciones en la fase de disuasión incluyen actividades de cooperación en materia de seguridad e IRC y/o se basan en actividades de cooperación en materia de seguridad de la fase 0. Una mayor cooperación con socios y aliados, fuerzas multinacionales, socios interinstitucionales e interorganizacionales, organizaciones internacionales y ONG ayudan a aumentar el intercambio de información y Proporcionar una mayor comprensión de la naturaleza, las capacidades y los vínculos de las redes de amenazas. Fase I, comienza con actividades de coordinación para influir en las redes de amenazas en múltiples frentes. El JFC tiene la capacidad de mejorar la disuasión a través de una acción unificada colaborando con todos los elementos amigos y creando una red amigable de organizaciones y personas con capacidades de gran alcance y la capacidad de responder con presión en múltiples puntos contra la red de amenazas. Las actividades de disuasión ejecutadas en la fase I también preparan para la fase II mediante la realización de acciones en todo el OE para aislar las redes de amenazas de los santuarios, los recursos y las redes de información y aumentar su vulnerabilidad ante operaciones posteriores de fuerzas conjuntas.

c. Aprovechar la iniciativa (Fase II). Los JFC buscan aprovechar la iniciativa mediante la aplicación de capacidades de fuerza conjunta en múltiples LOO. En las operaciones de combate tradicionales, esto implica ejecutar operaciones ofensivas lo antes posible, obligar al

adversario a culminar la ofensiva y establecer las condiciones para operaciones decisivas. En la CTN, la confrontación ofensiva directa suele ser menos efectiva o deseable que los enfoques indirectos. Las redes de amenazas rara vez presentan objetivos abiertos. La destrucción de un solo nodo o celda podría tener poco impacto en las operaciones de la red cuando se compara con el costo de las operaciones y/o el potencial de daños colaterales. Esto no significa que nunca se utilice poder letal, pero sí significa que la aplicación de la fuerza sin la intención de provocar la muerte o una destrucción física grave integrada en todos los sistemas PMESII y contra múltiples enlaces y nodos de redes de amenazas a menudo constituirá la mayoría de las operaciones. Como en las operaciones ofensivas tradicionales contra un adversario tradicional, varias operaciones crean condiciones para la explotación, la persecución y, en última instancia, la destrucción de esas fuerzas y su voluntad de luchar.

d. Dominar (Fase III). La fase de dominación contra las redes de amenazas se centra en crear y mantener una presión abrumadora contra el liderazgo, las finanzas, los recursos, la narrativa, los suministros y la motivación de la red. Esta presión en múltiples frentes debería incluir presión diplomática y económica a nivel estratégico y presión informativa a todos los niveles. Luego se sincronizan con operaciones militares llevadas a cabo en toda la OE y en todos los niveles de guerra para lograr el mismo resultado que las operaciones tradicionales: destruir la cohesión y la voluntad del enemigo. Las operaciones contra redes de amenazas se caracterizan por dominar y controlar la OE mediante una combinación de guerra tradicional, guerra irregular, empleo sostenido de capacidades interinstitucionales

y IRC. Las actividades de estabilidad se llevan a cabo en coordinación con la HN y el DOS según sea necesario para garantizar una transición sin problemas a la siguiente fase y aliviar el sufrimiento. En misiones que no son de combate, las actividades de la fuerza conjunta buscan

controlar la situación o la OE. Las actividades de la Fase III podrán establecer las condiciones para una pronta conclusión favorable de las operaciones o establecer las condiciones para la transición a la siguiente fase.

e. Estabilizar (Fase IV). La fase de estabilización es necesaria cuando no existe una autoridad de gobierno civil legítima y en pleno funcionamiento o cuando las redes de amenazas han obtenido control político dentro de un país o región. En los casos en que la red de amenazas está alineada con el gobierno, su derrota en la fase III puede dejar a ese gobierno intacto y puede no ser necesaria la estabilización o habilitación de la autoridad civil. Después de neutralizar o derrotar las redes de amenazas (que pueden haber estado funcionando como un gobierno en la sombra), es posible que se requiera que la fuerza conjunta unifique los esfuerzos de otras multinacionales, organizaciones internacionales, ONG o departamentos y agencias del gobierno de los Estados Unidos que apoyan o contribuyen en actividades de estabilidad. proporcionar gobernanza local, hasta que las entidades locales legítimas estén funcionando. Los esfuerzos de estabilización ayudan a que una HN pase de la inestabilidad (y particularmente del conflicto violento que a menudo la acompaña) a una mayor estabilidad (y una reducción de manteniendo o restableciendo un entorno seguro y proporcionando servicios gubernamentales esenciales, reconstrucción de infraestructura de emergencia o ayuda humanitaria.

Los esfuerzos de estabilización implican esfuerzos integrales por parte de Estados Unidos y sus socios para estabilizar a los Estados-nación en crisis, desarrollar sus capacidades para mantener la ley y el orden, proteger la actividad económica y mitigar las condiciones que permiten el poder y la influencia de las redes de amenazas.

f. Habilitar Autoridad Civil (Fase V). Esta fase se caracteriza predominantemente por el apoyo de fuerzas conjuntas a la gobernanza

civil legítima en la HN. Dependiendo del nivel de capacidad de la HN, las actividades de la fuerza conjunta durante la fase V pueden realizarse a instancias o instrucciones de esa autoridad. El objetivo es que la fuerza conjunta permita la viabilidad de la autoridad civil y su prestación de servicios esenciales al mayor número de personas de la región. Esto incluye coordinar acciones de fuerza conjunta con agencias multinacionales y de la HN que las apoyan o apoyan y continuar con operaciones financieras integradas y actividades de cooperación en materia de seguridad para influir favorablemente en la actitud de la población objetivo con respecto a los objetivos de las autoridades civiles locales.

La creación de fuerzas policiales y sistemas judiciales y penitenciarios sólidos y receptivos necesarios para establecer y mantener el Estado de derecho es de particular importancia para resistir el aumento de las redes de amenazas. Esto se complementa con instituciones políticas representativas de la HN que puedan abordar las necesidades básicas de la población. Idealmente, el estado final deseado es una HN con suficientes instituciones en funcionamiento para mantener el estado de derecho y prevenir el resurgimiento de redes de amenazas.

CAPÍTULO V

ACTIVIDADES PARA CONTRASTAR LAS REDES DE AMENAZA

1.- EL DESAFÍO

Una red de amenazas puede estar operando durante años en segundo plano y de repente explotar en escena. Identificar y contrarrestar redes de amenazas potenciales y reales es un desafío complejo.

a. Las redes de amenazas pueden adoptar muchas formas y tener muchos participantes distintos, desde terroristas hasta organizaciones criminales e insurgentes, con base local o transnacional, como se muestra en la Figura V-1. CTN no es una lucha localizada dentro de límites geográficos identificables. Muchos de nuestros adversarios se han extendido transnacionalmente para facilitar sus operaciones y aumentar su capacidad de supervivencia. Las redes de amenazas pueden aprovechar las tecnologías, las redes sociales, los sistemas financieros y de transporte globales y los sistemas políticos fallidos para construir un sistema de apoyo fuerte y altamente redundante. Operar en una región proporciona a la amenaza una gama mucho más amplia de recursos, refugios seguros y flexibilidad para reaccionar ante los ataques y procesarlos. Para contrarrestar una amenaza transnacional, Estados Unidos y sus socios deben buscar la cooperación multinacional y operaciones conjuntas para lograr la disrupción y cooperar con las HN dentro de una región específica para identificar, describir y mitigar completamente, a través de operaciones multilaterales, las redes transnacionales que amenazan a toda una región. y no sólo las HN individuales.

Derrotar las amenazas transnacionales requiere la sincronización, coordinación e integración de todos los instrumentos del poder nacional estadounidense en cooperación con socios regionales y multinacionales.

b. Las operaciones exitosas se basan en la capacidad de las fuerzas amigas para desarrollar y aplicar una comprensión detallada de la estructura y las interacciones de la OE a la planificación y ejecución de una amplia gama de capacidades para reforzar la legitimidad de la HN y neutralizar la capacidad de la amenaza para amenazar a esa sociedad.

2.- APUNTAR A LAS REDES DE AMENAZAS

a. El comandante y el estado mayor deben comprender la condición deseada de la red de amenazas en relación con los objetivos del comandante y el estado final deseado como primer paso para atacar cualquier red de amenazas. El ciclo de focalización conjunta descrito en el JP 3-60, Focalización Conjunta, se ha utilizado para desarrollar la Figura V-2, y las fases de ese ciclo se han asociado a los pasos de los procesos de planificación y focalización.

b. El estado final militar que se desea está directamente relacionado con las condiciones de la OE. Las redes humanas interrelacionadas comprenden el aspecto humano del OE, que incluye la amenaza redes que hay que contrarrestar. El objetivo real de las redes de amenazas comienza temprano en el proceso de planificación, ya que todas las acciones tomadas deben apoyar el logro de los objetivos del comandante y el logro del estado final. Para alimentar la segunda fase del ciclo de focalización, la red de amenazas debe analizarse mediante mapeo de red, análisis de enlaces, SNA, CFA y análisis de nodos. Una diferencia importante que se debe tener en cuenta es que los ataques convencionales generalmente se realizan durante operaciones o conflictos militares, donde gran parte de los ataques a la red de amenazas son realizados por departamentos y agencias del gobierno y las PN conforme a las leyes nacionales e internacionales, respectivamente.

c. La segunda fase del ciclo de selección conjunta tiene como objetivo comenzar el desarrollo de listas de objetivos para una posible participación. JIPOE es uno de los insumos críticos para apoyar el desarrollo de estos productos, pero debe incluir una cantidad sustancial de análisis sobre la red de amenazas para identificar adecuadamente los nodos críticos, CC (funciones de red) y CR de la red. El personal también debe utilizar este nivel de información para comenzar a desarrollar un plan de evaluación para la red de amenazas. De manera similar a desarrollar un plan de evaluación de operaciones como parte del proceso de planificación, las métricas para evaluar las redes deben desarrollarse temprano en el ciclo de focalización.

d. Las redes operan como entidades integradas: el todo es mayor que la suma de sus partes. Identificar y orientar la red y sus componentes funcionales requiere paciencia.

Una red hará todo lo posible para proteger sus componentes críticos. Sin embargo, la naturaleza interrelacionada de las funciones de la red significa que un ataque a un nodo puede tener un efecto dominó a medida que la red se reconstituya. Cada vez que una red se reorganiza o se adapta, puede exponer una porción mayor de sus miembros (nodos), relaciones (enlaces) y actividades. La recopilación de inteligencia debe estar en condiciones de explotar cualquier efecto del esfuerzo de selección de objetivos, que a su vez debe ser continuo y multinodal. Las acciones para atacar a los CV deben sincronizarse e integrarse con la operación o campaña conjunta general contra el enemigo. Los esfuerzos conjuntos de ataque de fuerzas deben emplear un enfoque integral, aprovechando la fuerza militar y las capacidades de las agencias civiles que mantienen una presión continua sobre múltiples nodos y enlaces de la estructura de la red. Hay algunos casos en los que CC y requisitos específicos pueden estar separados de los patrones operativos generales del enemigo y estar sujetos a ataque.

e. Los productos analíticos para redes de amenazas respaldan la decisión de qué objetivos se agregarán o eliminarán de la lista de objetivos y los detalles para el empleo de capacidades contra un objetivo. El personal debe considerar las siguientes preguntas al seleccionar objetivos para atacar dentro de una red de amenazas:

(1) ¿A quién o a qué dirigirse? El análisis de la red proporciona al comandante y al estado mayor la información para priorizar objetivos potenciales. Dependiendo del efecto deseado para una red, el nodo seleccionado para apuntar puede ser una persona, un recurso clave u otro objeto físico que sea crítico para producir un efecto específico en la red.

(2) ¿Cuáles son los efectos deseados en el objetivo y la red? Comprender las condiciones en el OE y las condiciones futuras deseadas para lograr los objetivos respalda la decisión sobre qué tipo de efectos se desean en el objetivo y en la red de amenazas en su conjunto.

Los efectos deseados en la red de amenazas deben estar alineados con la intención del comandante de respaldar los objetivos o condiciones de la red de amenazas para alcanzar el estado final deseado.

(3) ¿Cómo se producirán esos efectos deseados? El conjunto de capacidades letales y no letales puede emplearse con la decisión de atacar a un objetivo, ya sea directa o indirectamente. Además de la capacidad de emplear sistemas de armas convencionales, el personal debe considerar las capacidades no letales que estén disponibles.

3.- EFECTOS DESEADOS EN LAS REDES

a. Los efectos del daño causado a un enemigo o adversario por disparos letales se clasifican como leves, moderados o graves. La participación en la red toma en consideración los efectos de las capacidades letales y no letales. La Figura V-3 ilustra los efectos de primer, segundo y

tercer orden que se deben considerar al seleccionar atacar objetivos dentro de una red.

b. Cuando los comandantes deciden generar un efecto en una red atacando nodos específicos, la intención puede no ser causar daño, sino moldear condiciones de naturaleza mental o moral. El resultado esperado al dar forma a estas condiciones es apoyar el logro de los objetivos del comandante. Los efectos deseados seleccionados son el resultado de la visión del comandante sobre las condiciones futuras de las redes de amenazas y dentro de la OE para lograr los objetivos. La selección de los efectos deseados en una red se lleva a cabo como parte del objetivo de selección, que incluye la consideración de las capacidades a emplear que se identificaron durante el análisis de capacidades del ciclo de selección conjunta de objetivos. El personal puede considerar los siguientes efectos para CTN. Los términos que se utilizan para describir los efectos deseados de CTN incluyen:

(1) Neutralizar. Neutralizar es una tarea de misión táctica que resulta en hacer que el personal o el material enemigo sea incapaz de interferir con una operación en particular. La estructura de la red de amenazas existe para facilitar su capacidad de realizar funciones que apoyen el logro de sus objetivos. La neutralización de una red completa puede no ser factible, pero a través del análisis, el personal tiene la capacidad de identificar partes clave de la estructura de la red de amenazas a las que apuntar, lo que resultará en la neutralización de funciones específicas que pueden interferir con una operación en particular.

(2) Degradar. Degradar es reducir la efectividad o eficiencia de una amenaza.

La efectividad de una red de amenazas está asociada con su capacidad de funcionar como se desea para lograr los objetivos de la amenaza. Contrarrestar la eficacia de una red se puede lograr eliminando los CR

que la red requiere para facilitar un CC identificado, identificado mediante la aplicación de CFA para la red.

(3) Interrumpir. Interrumpir es una tarea de misión táctica en la que un comandante integra fuegos directos e indirectos, terreno y obstáculos para alterar la formación o el ritmo de un enemigo, interrumpir el cronograma del enemigo o hacer que las fuerzas enemigas se comprometan prematuramente o ataquen de manera gradual. Desde la perspectiva de interrumpir una red de amenazas, el personal debe considerar el tipo de operación que se lleva a cabo, las funciones específicas de la red de amenazas y las condiciones dentro del OE que pueden aprovecharse y la posible aplicación de capacidades tanto letales como no letales. Además, el personal debe considerar el impacto potencial y la duración del tiempo que la interrupción de la red de amenazas presentará en las oportunidades para que las fuerzas amigas aprovechen una oportunidad potencial. Si la interrupción resulta en la eliminación de nodos clave de la red, el personal también debe considerar los medios y el tiempo necesarios para su reconstitución.

(4) Destruir. Destruir es una tarea de misión táctica que físicamente hace que el combate de una fuerza enemiga sea ineficaz hasta que se reconstituya. Alternativamente, destruir un sistema de combate es dañarlo tan gravemente que no pueda realizar ninguna función o restaurarse a una condición utilizable sin ser reconstruido por completo. Destruir una red de amenazas que sea adaptable y esté establecida transnacionalmente es un desafío extremo que requiere la colaboración total del Departamento de Defensa y las agencias intergubernamentales, así como la coordinación con las naciones asociadas.

La destrucción aislada de células puede ser más plausible y podría lograrse con la aplicación integral de capacidades letales y no letales. Es necesario un análisis detallado de la celda para establecer una línea

de base (condiciones previas a la operación) con el fin de evaluar si las operaciones han resultado en la destrucción de la porción seleccionada de una red.

(5) Derrota. La derrota es una tarea de misión táctica que ocurre cuando una red de amenazas o una fuerza enemiga ha perdido temporal o permanentemente los medios físicos o la voluntad de luchar. El comandante o líder de la fuerza derrotada no está dispuesto o no puede seguir el COA adoptado por ese individuo, cediendo así a la voluntad del comandante amigo, y ya no puede interferir en un grado significativo con las acciones de las fuerzas amigas. La derrota puede resultar del uso de la fuerza o de la amenaza de su uso. La derrota se manifiesta en algún tipo de acción física, como rendiciones masivas, abandono de posiciones, equipos y suministros u operaciones retrógradas. Un comandante o líder puede crear diferentes efectos contra un enemigo para derrotar a esa fuerza.

(6) Negar. Negar es una acción para obstaculizar o negar al enemigo el uso de territorio, personal o instalaciones para incluir destrucción, remoción, contaminación o construcción de obstrucciones. Un ejemplo de negación es destruir el equipo de comunicaciones de la amenaza como medio para negar su uso del espectro electromagnético. Sin embargo, la duración de la negación dependerá de la capacidad del enemigo para reconstituirse.

(7) Desviar. Desviarse es desviarse o de un camino o COA. Una desviación es el acto de atraer la atención y las fuerzas de una amenaza desde el punto de la operación principal; un ataque, alarma o finta desvía la atención. El desvío hace que las redes de amenazas o las fuerzas enemigas consuman recursos o capacidades críticas para las operaciones de amenazas de una manera que sea ventajosa para las operaciones amigas. Los desvíos desvían la atención de las redes de amenazas o de las fuerzas enemigas de operaciones amigas críticas e impiden que las fuerzas de amenazas y sus recursos de apoyo se

empleen para el propósito previsto. Los desvíos también pueden causar rutas más tortuosas a lo largo de las líneas de comunicación, lo que resulta en retrasos para las fuerzas enemigas.

4.- ESTRATEGIAS DE PARTICIPACIÓN

a. Recurso de contador. Un enfoque de contrarrecursos puede debilitar progresivamente la capacidad de la amenaza para realizar operaciones en el OE y requerir que la red busque un sustituto adecuado para reemplazar los recursos eliminados o limitados. Al igual que una organización militar, la red de una amenaza o la organización de una amenaza es más que su estructura C2. Debe tener un suministro asegurado de reclutas, alimentos, armas y transporte para mantener su posición y crecer. Si bien el liderazgo proporciona orientación a la red, es la infraestructura financiera y logística la que sostiene la red. La mayoría de las redes de amenazas son de naturaleza transnacional y obtienen apoyo financiero, apoyo material y reclutas de una audiencia mundial.

Si bien el aparato de inteligencia de la fuerza conjunta puede apuntar a una porción razonable de la base de sostenimiento y las actividades de la red de amenazas en el área operativa, los resultados duraderos requieren una cooperación activa por parte de socios interinstitucionales e internacionales dirigida contra las actividades transnacionales de la red. Un enfoque de contrarrecursos se centra en acciones amigables de contrared multinodal que privan a la red de los recursos necesarios para realizar operaciones de manera consistente y libre.

b. Decapitación. La decapitación es la eliminación de nodos clave dentro de la red que funcionan como líderes. El liderazgo objetivo está diseñado para impactar el C2 de la red.

El análisis detallado de la red puede proporcionar al personal una indicación de cuánto tiempo necesitará la red para reemplazar al liderazgo una vez que sean eliminados de la red. Desde una perspectiva histórica, la eliminación de un único líder de una red humana adaptativa ha tenido efectos a corto plazo en la red. Captar a un miembro de la red que ocupa una posición de liderazgo puede proporcionar información y conocimientos adicionales sobre la red Bastones.

También se debe considerar el impacto potencial de las personas que reemplazarán a un líder que sea destituido. Al atacar los nodos, enlaces y actividades de las redes de amenazas, el JFC debe considerar los efectos de segundo y tercer orden en grupos amigos y neutrales que comparten funciones de redes y células. Además, se deben considerar los efectos en cadena en toda la red y sus células. Los efectos de involucrarse en una red deben analizarse y considerarse antes de tomar la decisión de participar. En la Figura V-4 se ilustra un ejemplo de la profundidad y amplitud del análisis necesario cuando se ataca una red de amenazas. Debe recordarse que el liderazgo es sólo uno de los muchos objetivos analizados por el DOD y los socios interinstitucionales para un compromiso letal y no letal y, a menudo, es simplemente un punto de entrada para descubrir toda la red.

c. Fragmentación. Una estrategia de fragmentación es la extirpación quirúrgica de nodos clave de la red que produce un efecto fragmentado en la red con la intención de interrumpir la capacidad de funcionamiento de la red. Aunque fragmentar la red tendrá efectos inmediatos, el personal debe considerar cuándo es apropiado este tipo de estrategia. La eliminación de nodos dentro de la red puede tener impactos en los esfuerzos de recolección, dependiendo del nodo al que se dirige. El flujo de información, así como aspectos del C2, están directamente relacionados con la comprensión de las relaciones que existen dentro de la red. La visualización de la estructura de la red se

puede lograr utilizando productos de análisis de redes. Un ejemplo de un producto de análisis de red que se puede proporcionar al personal antes y después de la selección. Como se analizó anteriormente, el personal debe desarrollar un plan de evaluación para comprender los efectos de involucrar a las redes y determinar si se están logrando los objetivos del JFC.

d. Contramensajes. Las redes de amenazas se forman en torno a algún tipo de catalizador que motiva a individuos de una audiencia receptiva a unirse a una red. El aspecto desafiante de un catalizador es que los individuos lo interpretarán y se relacionarán con él a su manera. Puede haber algunas tendencias entre los miembros de la red que se relacionen con el catalizador de manera similar; Esta perspectiva no es precisa para todos los miembros de la red. Las redes de amenazas han adoptado la capacidad de proyectar sus propios mensajes utilizando varios sitios de redes sociales.

Estos mensajes respaldan sus objetivos y se utilizan como herramienta de reclutamiento de nuevos miembros. Contrarrestar los mensajes de la red de amenazas es un aspecto de contrarrestar una red de amenazas. Los planificadores de IO trabajarán con agencias intergubernamentales seleccionadas para desarrollar los contramensajes apropiados como parte del empleo de los IRC. Estos mensajes están diseñados no sólo para contrarrestar el mensaje de la amenaza, sino también para solicitar apoyo de redes neutrales para fuerzas amigas.

5.- ORIENTACIÓN

a. A nivel táctico, la atención se centra en ejecutar operaciones dirigidas a nodos y enlaces.

Inteligencia precisa, oportuna y relevante respalda este esfuerzo. Las unidades tácticas utilizan esta inteligencia junto con sus

procedimientos para realizar análisis adicionales, plantillas y redes objetivo. En una operación COIN, por ejemplo, las operaciones amigas incluyen esfuerzos para proteger a la población, fortalecer las fuerzas de seguridad de la HN y contrarrestar la ideología y la propaganda del enemigo. Estas acciones contribuyen al esfuerzo general de CTN al servir para aislar la amenaza de los partidarios, proveedores y simpatizantes de su red.

b. La selección de CV de redes de amenazas depende de la situación, la precisión de la inteligencia y la capacidad de la fuerza conjunta para ejecutar rápidamente varias opciones de selección de objetivos para crear los efectos deseados. En las operaciones COIN, los objetivos de alta prioridad pueden ser personas que realizan tareas que son vulnerables a la detección/explotación y afectan a más de un CR. Puede ser más beneficioso analizar el siguiente nodo de la red financiera que está asegurando fondos para el próximo día de pago. El tiempo lo es todo al atacar una red, ya que las oportunidades para atacar los CV identificados pueden ser limitadas.

c. Los objetivos de CTN pueden caracterizarse como objetivos que deben atacarse de inmediato debido a la amenaza significativa que representan o el impacto inmediato que tendrán en relación con la intención del JFC, nodos clave como individuos de alto valor u objetivos de infraestructura de red a más largo plazo (cachés). , rutas de suministro, casas seguras) que normalmente se dejan en el lugar durante un período de tiempo para explotarlas. Los recursos para dar servicio/explotar estos objetivos se asignan de acuerdo con las prioridades del JFC, que se revisan y actualizan constantemente a través del proceso de selección de objetivos conjunto del comando. Esta asignación se valida mediante una reunión diaria de sincronización de activos de la junta de coordinación conjunta de focalización. El método de selección utilizado para atacar a estos objetivos es deliberado o dinámico.

(1) Orientación dinámica. Una parte esencial de cualquier esfuerzo de selección de redes es una célula de selección de objetivos urgente compuesta por personal de operaciones y de inteligencia con acceso directo a los medios de enfrentamiento y la autoridad para actuar sobre objetivos previamente aprobados. La focalización dinámica facilita la participación de objetivos que han sido identificados demasiado tarde o no seleccionados a tiempo para ser incluidos en la focalización deliberada y que cumplen con criterios específicos para lograr los objetivos establecidos.

(2) Focalización deliberada. La célula conjunta de bomberos tiene la tarea de observar un cronograma extendido para las amenazas y el funcionamiento general de las redes de amenazas. Con este tipo de investigación deliberada de las redes de amenazas, la célula puede identificar catalizadores de las operaciones y el mantenimiento de la red de amenazas que tradicionalmente no habían sido atacados a gran escala. Con un flujo constante de inteligencia sobre acciones y movimientos individuales, la célula examinará qué facilitó cualquier número de eventos, como actividades terroristas, criminales y narcóticas; servicios públicos fallidos; y corrupción gubernamental. También se centrará en cómo estos eventos impactaron en última instancia no sólo las operaciones del JFC en apoyo del plan general de operación/ campaña conjunta, sino también los esfuerzos internacionales de desarrollo y ayuda y el gobierno y la población locales. Este tipo de análisis normalmente revelará una red de relaciones y asociaciones interconectadas de las cuales sólo un pequeño porcentaje puede verse afectado por ataques y acciones letales. Cuando se complementa con el departamento y agencia apropiados del gobierno de los Estados Unidos, operaciones especiales y analistas de inteligencia, la célula de fuego conjunto puede planificar la explotación de las relaciones y asociaciones de la red de amenazas utilizando todos los medios disponibles para reducir su contribución a la efectividad general de la red. El J-2, junto con el grupo de trabajo

conjunto de objetivos, completa el análisis del sistema de objetivos y el desarrollo de objetivos para nominar objetivos relacionados con CTN a la junta de coordinación de objetivos conjuntos para su aprobación y posterior ejecución en forma de guardia o deliberada.

d. El ciclo de selección conjunta de objetivos respalda el desarrollo y la persecución de redes de amenazas. Los comandantes de las fuerzas terrestres y marítimas normalmente utilizan un proceso interrelacionado para mejorar la planificación conjunta del apoyo de fuego y la interfaz con el ciclo conjunto de selección de objetivos conocido como metodología de decidir, detectar, entregar y evaluar (D3A). D3A incorpora las mismas funciones fundamentales del ciclo de focalización conjunta que el proceso y las funciones de encontrar, reparar, rastrear, apuntar, atacar y evaluar (F2T2EA) dentro de la fase 5 del ciclo de focalización conjunta. La metodología D3A facilita la sincronización de maniobras, inteligencia y apoyo de fuego. Las metodologías F2T2EA y F3EAD admiten la orientación dinámica. Si bien el modelo F3EAD se desarrolló para la focalización basada en la personalidad, solo se puede aplicar una vez que el JFC haya aprobado la lista conjunta integrada de objetivos priorizados. Dependiendo de la situación, es posible que se requieran múltiples metodologías para crear el efecto deseado.

e. F3EAD. F3EAD facilita la focalización no sólo en individuos cuando el momento es crucial, sino también, más importante aún, la generación de objetivos de seguimiento a través de la explotación y el análisis oportunos. F3EAD facilita la sinergia entre operaciones e inteligencia a medida que refina el proceso de selección de objetivos. Es un ciclo continuo en el que la inteligencia y las operaciones se retroalimentan y apoyan mutuamente. Ayuda a:

(1) Analizar la ideología, metodología y capacidades de la red de amenazas; ayuda a modelar su funcionamiento interno: personal, organización y actividades.

(2) Identificar los vínculos entre los CC y CR enemigos y los indicadores observables de la acción enemiga.

(3) Centrar y priorizar los activos dedicados a la recopilación de inteligencia.

(4) Proporcionar la inteligencia y los productos resultantes a elementos capaces de realizar rápidamente ataques múltiples y casi simultáneos contra los CV.

(5) Proporcionar la capacidad de visualizar el OE y organizar y sincronizar fuerzas y capacidades.

f. El proceso F3EAD está optimizado para facilitar la selección de nodos y enlaces clave de nivel I (liderazgo de alto nivel enemigo, por ejemplo) y nivel II (intermediarios enemigos que interactúan con los líderes y establecen vínculos con facilitadores dentro de la población). Nivel III

Los individuos (los soldados de infantería poco calificados que son parte de la amenaza) pueden ser fáciles de alcanzar y proporcionar un resultado inmediato, pero son una distracción para el éxito porque son fáciles de reemplazar y su eliminación es sólo un inconveniente temporal para el enemigo. F3EAD se puede utilizar para cualquier función de red que sea un objetivo urgente.

g. El proceso F3EAD se basa en la estrecha coordinación entre los planificadores operativos y la recopilación de inteligencia y la ejecución táctica. Las fuerzas tácticas deberían complementarse con una amplia gama de especialistas para facilitar la explotación in situ y posibles operaciones posteriores.

La explotación de los materiales y del personal capturados normalmente involucrará a especialistas funcionales de recursos superiores e incluso nacionales. El objetivo es realizar rápidamente la explotación y facilitar el seguimiento de los nodos críticos de la red.

6.- CONSIDERACIONES SOBRE FOCALIZACIÓN

a. No existe una regla estricta para asignar objetivos de red por escalón. La consideración principal es cómo crear el efecto deseado en la red en su conjunto. Generalmente, los objetivos de la red se dividen en una de tres categorías: objetivos individuales, objetivos grupales y objetivos organizacionales. El personal de la fuerza conjunta y los componentes del Servicio, a través del proceso de selección conjunta de objetivos, determinan y recomiendan objetivos de red para la aprobación del JFC. Estos se complementan con la selección de nodos y enlaces por parte de socios interinstitucionales, HN y PN.

b. Un objetivo de la focalización en la red puede ser negar a la amenaza su libertad de acción y maniobra manteniendo una presión constante a través de acciones impredecibles contra el liderazgo de la red y los nodos funcionales críticos. Se basa en seleccionar los medios adecuados o una combinación de ellos para neutralizar el objetivo minimizando los efectos colaterales.

c. Si bien los objetivos materiales pueden desactivarse, negarse, destruirse o capturarse, los humanos y sus interrelaciones o vínculos están abiertos a una gama más amplia de opciones de enfrentamiento por parte de fuerzas amigas. Por ejemplo, cuando el objetivo es neutralizar la influencia de un grupo específico, puede ser necesaria una combinación de tareas para crear el efecto deseado.

7.- LÍNEAS DE ESFUERZO POR FASE

a. La focalización es un proceso continuo y en evolución. A medida que la amenaza se adapta a las actividades de las fuerzas conjuntas, la recopilación de inteligencia y la selección de objetivos de las fuerzas conjuntas también deben adaptarse. Emplear un enfoque de contrarrecursos (logísticos, financieros y de reclutamiento) debería aumentar la cantidad de tiempo que le tomará a la organización

reagruparse. También puede obligar a la amenaza a emplear sus recursos ocultos para llenar los vacíos, aumentando así el riesgo de detección y explotación. Durante cada fase de una operación o campaña contra una red de amenazas, hay acciones específicas que el JFC puede tomar para facilitar la lucha contra la red de amenazas.

Sin embargo, estas acciones no son exclusivas de ninguna fase en particular y deben adaptarse a las requisitos específicos de la misión y la OE. El modelo simplificado de la Figura V-6 es ilustrativo y no una lista de pasos de planificación específicos.

b. Durante la fase 0, el análisis proporciona una descripción amplia de la estructura de la organización de la amenaza subyacente, identifica las funciones y nodos críticos e identifica las relaciones entre las actividades de la amenaza y la sociedad en general. Las fuerzas estadounidenses son comúnmente desplegados en apoyo de los objetivos de seguridad del teatro. Estas fuerzas proporcionan una base de información sobre la región para incluir información muy específica que cae dentro de las categorías de PMESII. Las acciones contra la red pueden incluir atacar los recursos transnacionales de la amenaza (dinero, suministros, refugios seguros, reclutamiento); identificar liderazgos clave; proporcionar recursos para facilitar las PN y los esfuerzos regionales; dar forma a las opiniones de las poblaciones nacionales e internacionales sobre grupos amigos, neutrales y amenazantes; y aislar la amenaza de los aliados transnacionales.

c. Durante la fase I, las actividades del CTN buscan brindar un panorama más completo de las condiciones en la OE. Las fuerzas ya empleadas en el teatro de operaciones pueden aprovecharse como fuentes de información para ayudar a construir una imagen más detallada. Es posible que surjan nuevos objetivos como parte de la fase I, y las fuerzas desplegadas para ayudar a alcanzar esos objetivos contribuyen al desarrollo del panorama operativo común. Se lleva a cabo un análisis de red para identificar un conjunto de objetivos que

mantendrá la red de amenazas desequilibrada a través de operaciones de ataque multinodal. Las acciones contra la red de amenazas incluyen apuntar a recursos internos y externos (dinero, suministros, refugios seguros, reclutamiento) identificando liderazgos internos y externos clave; proporcionar recursos para facilitar las PN y los esfuerzos regionales; y moldear las opiniones de las poblaciones nacionales e internacionales sobre la amenaza.

d. Durante la fase II, las actividades de la CTN se concentran en desarrollar objetivos previamente identificados, posicionar la recopilación de inteligencia para explotar los efectos y continuar refinando la descripción de la amenaza y su red de apoyo. Las acciones contra la amenaza continúan e incluyen atacar la infraestructura de la organización mediante ataques coordinados, preferiblemente multimodales, así como IRC dirigidos a apoyar al gobierno y persuadir a los neutrales.

e. Durante la fase III, las actividades de la CTN se caracterizan por un mayor contacto físico y un aumento considerable de una variedad de activos de inteligencia y recopilación de información. La atención se centra en identificar, explotar y atacar el núcleo clandestino de la red. Los activos de recopilación de inteligencia y las capacidades analíticas especializadas brindan apoyo las 24 horas del día a las fuerzas comprometidas. Las acciones contra la red continúan y destacan un aumento en la denegación de recursos; los líderes y actividades clave son objeto de eliminación; y se mantiene una presión multinodal constante. Las actividades continúan para convencer a las redes neutrales de los beneficios de apoyar al gobierno y disuadir a los simpatizantes de las amenazas de brindar apoyo continuo a las redes de amenazas. En última instancia, la red queda aislada del soporte y su capacidad para realizar operaciones se ve gravemente disminuida.

f. Durante la fase IV, las actividades de la CTN se centran en identificar, explotar y apuntar al núcleo clandestino de la red para su eliminación.

Los activos de recopilación de inteligencia y las capacidades analíticas especializadas continúan brindando apoyo a las fuerzas comprometidas; el objetivo es evitar que la amenaza se recupere y se reagrupe. Continúan las actividades de la Fase III del CTN.

g. Durante la fase V, las actividades de la CTN continúan identificando, explotando y apuntando al núcleo clandestino de la red para su eliminación e identificando los intentos de la red de amenazas de reagruparse y restablecer el control. Las actividades de la CTN continúan con el objetivo de garantizar que la red no tenga los recursos para continuar las actividades de la red de mostradores de la Fase III.}

CAPÍTULO VI

EVALUACIONES

1.- GENERALIDADES

Los comandantes y sus estados mayores realizarán evaluaciones para determinar el impacto que las actividades de la CTN pueden tener en las redes objetivo. Otras redes, incluidas las amigas y neutrales, dentro de la OE también deben considerarse durante la planificación, las operaciones y las evaluaciones. El objetivo de este capítulo es evaluar el impacto en las redes de amenazas, para incluir la identificación de posibles efectos de segundo y tercer orden de las operaciones en relación con el logro del estado final deseado del JFC. Los CCMD funcionales con responsabilidades de sincronización global también deberían evaluar eventos y desarrollar opciones para lograr sus respectivos objetivos estratégicos.

Las redes de amenazas se adaptarán de manera visible e invisible incluso mientras se llevan a cabo la recopilación, el análisis y las evaluaciones, razón por la cual las evaluaciones a lo largo del tiempo que muestran tendencias son mucho más valiosas en las actividades de la CTN que una sola instantánea en un corto período de tiempo. Los CCDR desarrollan estrategias globales y de teatro analizando la OE y desarrollando objetivos que se apoyan mutuamente para establecer mejor las condiciones para alcanzar estados finales estratégicos. Durante largos períodos de tiempo, se puede recopilar información para describir cambios en la organización, estructura, composición, funciones y capacidades operativas de la red de amenazas. Estos datos se pueden utilizar para respaldar una estrategia amplia en el teatro de operaciones, las operaciones en curso de fase 0 y fase I, y como base para respaldar las operaciones en caso de que sea necesario el empleo de fuerzas conjuntas. La evaluación de las actividades de la CTN será parte de la evaluación de la operación o campaña más amplia.

2.- ENTORNOS OPERATIVOS COMPLEJOS

Los entornos geopolíticos complejos, las asociaciones causales difíciles y el desafío del análisis tanto cuantitativo como cualitativo para respaldar la toma de decisiones complican el proceso de evaluación. Cuando las redes de amenazas sólo parcialmente visibles se extienden por grandes áreas geográficas, entre la gente, y están entretejidas en redes amigas y neutrales, evaluar los efectos de las operaciones de fuerzas conjuntas requiere tanto arte operativo como el proceso de planificación.

3.- EVALUACIÓN DE OPERACIONES PARA CONTRARRESTAR REDES AMENAZAS

a. Las evaluaciones de la CTN a nivel estratégico, operativo y táctico y en todos los instrumentos del poder nacional son vitales ya que muchas redes tienen vínculos y capacidades regionales e internacionales. Los objetivos deben desarrollarse durante el proceso de planificación para que se pueda evaluar el progreso hacia los objetivos. Las evaluaciones de las redes de amenazas también serán más desafiantes que las de los adversarios tradicionales, ya que será difícil medir datos concretos sobre cómo las actividades de la CTN impactan cosas como la cantidad de sistemas de armas, la fuerza de las tropas, la moral y la ubicación de las unidades. La interacción dinámica entre redes amigas, amenazantes y neutrales dificulta la evaluación de muchos aspectos de las actividades de la CTN. A medida que los planificadores evalúan comportamientos humanos complejos, recurren a múltiples fuentes en todo el OE, incluidas medidas analíticas y subjetivas, que respaldan una evaluación informada.

b. La detección de cambios en la red en tiempo real es extremadamente desafiante y las conclusiones con altos niveles de confianza son raras. Dado que las redes de amenazas se adaptan rápidamente, las tecnologías, Los sistemas utilizados para respaldar la recopilación a

menudo tienen dificultades para monitorear el cambio. Además, las grandes cantidades de información recopilada requieren recursos (personas) y tiempo para su análisis. Es difícil determinar cómo cambian las redes y aún más difícil determinar si los cambios en las redes son el resultado de acciones de fuerzas conjuntas y, de ser así, qué acciones o acciones combinadas son efectivas. Un indicador útil utilizado en la evaluación surge cuando las redes de amenazas aprovechan las redes sociales para coordinar y realizar operaciones, ya que brinda la oportunidad de obtener una mayor comprensión de la motivación y la ideología de estas redes. Si los analistas de inteligencia pueden acceder a información casi en tiempo real de las entidades de la red de amenazas, entonces esa información a menudo puede fusionarse geoespacialmente para crear una mejor evaluación. Esto depende de tener acceso a datos de red precisos, la capacidad de analizar los datos rápidamente y la capacidad de detectar engaños.

c. Las evaluaciones de CTN requieren que el personal realice análisis de manera más intuitiva y considere evidencia tanto anecdótica como circunstancial. Dado que las amenazas en red operan entre las poblaciones civiles, existe una mayor necesidad de HUMINT. La recopilación de HUMINT requiere mucho tiempo y la confiabilidad de las fuentes puede ser problemática, pero si se emplea adecuadamente y se combina con otras disciplinas, es extremadamente valiosa en la guerra irregular. Los informes de unidad táctica, como los informes de patrulla y los informes de unidad después de la acción, cuando se asimilan en una OE pueden proporcionar la información más valiosa para evaluar el impacto de las operaciones. Existen desafíos a la hora de recopilar, analizar y asimilar información con la suficiente rapidez para informar al JFC para el próximo ciclo de decisiones. OSINT a menudo será más valioso para evaluar operaciones contra redes de amenazas y será la mayor fuente de inteligencia.

La información necesaria para realizar evaluaciones de las actividades de la CTN requiere la aplicación de inteligencia en capas de múltiples fuentes. La diversidad de métodos de recopilación, tipos de información e inteligencia recopilada y metodologías analíticas de estos socios contribuye a una evaluación holística en una OE compleja.

4.- EVALUACIÓN DE LA OPERACIÓN

a. El proceso de evaluación es un ciclo continuo que busca observar y evaluar la OE en constante cambio e informar las decisiones sobre el futuro, haciendo que las operaciones sean más efectivas.

La elaboración de una línea de base es fundamental en la fase 0 y en el proceso inicial de JIPOE para que las evaluaciones sean efectivas. Las evaluaciones retroalimentan el proceso JIPOE para mantener el ritmo en el ciclo de decisiones del comandante. Este es un proceso continuo y la línea de base se restablece para cada ciclo. El cambio es constante dentro del complejo OE y cuando se opera contra múltiples redes de amenazas interconectadas, adaptables.

b. Los comandantes establecen prioridades para la evaluación a través de su guía de planificación, los requisitos de información crítica del comandante (CCIR) y los puntos de decisión. Los requisitos de inteligencia prioritarios, un componente del CCIR, detallan exactamente qué datos debe buscar el plan de recopilación de inteligencia para informar al comandante sobre las redes de amenazas. El proceso de evaluación debe medir el progreso hacia el logro de los objetivos y la consecución del estado final militar. Las actividades de CTN pueden requerir la evaluación de múltiples MOE y medidas de desempeño (MOP), según la actividad de la red de amenazas. Por ejemplo, los JFC pueden optar por neutralizar o interrumpir un tipo de red mientras realizan operaciones directas contra otra red para destruirla.

c. La evaluación precede y guía cada actividad del proceso de operación y concluye cada operación o fase de una operación. Como todo ciclo, la evaluación es continua. El proceso de evaluación no es un fin en sí mismo; existe para informar al comandante y mejorar el progreso de la operación. El proceso de evaluación proporciona un mecanismo de retroalimentación al JFC para brindar orientación y dirección para operaciones futuras y esfuerzos dirigidos a redes de amenazas.

d. Integrada con éxito, la evaluación en las actividades del CTN permitirá:

(1) Describir el progreso hacia el logro de los objetivos del comandante y la consecución de los Estado final del comandante.

(2) Ayuda a comprender cómo está cambiando la OE debido al impacto de actividades CTN sobre estructuras y funciones de redes de amenazas.

(3) Informar la toma de decisiones del comandante para el diseño y planificación operacional, priorización, asignación de recursos y ejecución.

(4) Producir recomendaciones viables que informen al comandante dónde dedicar recursos a lo largo de las LOO y LOE más efectivas.

5.- MARCO DE EVALUACIÓN PARA CONTRARRESTAR LAS REDES DE AMENAZAS

El marco de evaluación describe en términos generales tres actividades principales: organizar, analizar y comunicar. Al realizar cada una de estas actividades, los evaluadores deben estar vinculados al JPP, comprender el plan operativo e informar al proceso de inteligencia qué información se requiere para respaldar los indicadores, los MOE y los MOP. Al evaluar las operaciones de la CTN, los evaluadores se basarán en datos y análisis cuantitativos. Las tendencias a lo largo del tiempo

tendrán un mayor nivel de confianza que las conclusiones a corto plazo. A continuación se presenta una descripción general de la evaluación; para obtener más información, consulte la Publicación de Tácticas, técnicas y procedimientos de la Fuerza Aérea (AFTTP).

a. Organizar los datos

(1) Con base en la OE y el plan de operación o plan de campaña, el comandante y el estado mayor desarrollan objetivos y criterios de evaluación para determinar el progreso. La actividad de organización incluye garantizar que los indicadores estén incluidos dentro del plan de recopilación, que la información recopilada y luego analizada por la sección de inteligencia esté organizada mediante un plan de gestión de la información y que la información esté disponible para el personal para realizar la evaluación.

Múltiples redes de amenazas dentro de una OE pueden requerir múltiples MOP, MOE, métricas y sucursales del plan. Las redes de amenazas que operan en colaboración o entre sí complican el proceso de evaluación. Si las redes de amenazas realizan operaciones o obtienen recursos de fuera del área operativa, habrá una mayor dependencia de otros CCDR o socios interinstitucionales para obtener datos e información. Los datos asociados dentro de la OE pueden organizarse por objetivo, fase, geografía, red, LOE o LOO.

(2) Las métricas deben ser recopilables, relevantes, mensurables, oportunas y complementarias.

El proceso utiliza criterios de evaluación para evaluar el desempeño de las tareas en todos los niveles de la guerra para determinar el progreso de las operaciones hacia el logro de los objetivos. Se requieren análisis tanto cualitativos como cuantitativos. En el caso de las redes de amenazas, los impactos directos por sí solos pueden no ser suficientes, por lo que se requieren impactos indirectos para una evaluación

holística. Las operaciones contra los recursos financieros de una red se pueden juzgar mejor analizando la calidad de los equipos que pueden implementar en el OE. Los esfuerzos contra el reclutamiento pueden requerir un estudio detallado de qué tan bien las guerrillas son capaces de planificar y llevar a cabo operaciones. Desarrollar indicadores para los cambios en la red de amenazas a lo largo de meses también puede ser más valioso que intentar determinar los cambios diarios.

b. Analizar los datos

(1) El análisis de datos es el corazón del proceso de evaluación de las actividades del CTN.

La elaboración de líneas de base es fundamental para respaldar el análisis. La línea de base no sólo debería basarse en la JIPOE inicial, sino que debería remontarse a las operaciones de recopilación y configuración de inteligencia del teatro de operaciones del CCG. Comprender cómo se formaron y adaptaron las redes de amenazas antes de las operaciones de fuerzas conjuntas proporciona a los evaluadores una base de referencia significativamente mejor y ayuda a desarrollar indicadores.

(2) El análisis de datos busca responder preguntas esenciales:

(a) ¿Qué pasó con la(s) red(es) de amenaza como resultado de las operaciones de fuerzas conjuntas? Los ejemplos específicos pueden incluir los siguientes: ¿Cómo han cambiado los enlaces? ¿Cómo se han visto afectados los nodos? ¿Cómo han cambiado las relaciones? ¿Cuál fue el impacto en la estructura y las funciones? Específicamente, ¿cuál fue el impacto en las operaciones, la logística, el reclutamiento, el financiamiento y la propaganda?

(b) ¿Qué operaciones causaron este efecto directa o indirectamente? (¿Por qué sucedió?) Es probable que múltiples instrumentos de

esfuerzos de poder nacional en varias LOO y LOE impactaran las redes de amenazas, y es igualmente improbable que sea discernible una causa y un efecto directos. Sin embargo, con el tiempo y con pensamiento crítico, las tendencias relacionadas con las operaciones y los impactos se harán evidentes. Los analistas deben ser conscientes del peligro de buscar una tendencia que puede no ser evidente. En ocasiones, los eventos pueden tener efectos dramáticos en las redes de amenazas, pero no ser visibles para observadores externos/extranjeros/estadounidenses.

(c) ¿Cuáles son las probables oportunidades futuras para contrarrestar la red de amenazas y cuáles son los riesgos para las redes neutrales y amigas? Las actividades de la CTN deberían centrarse en los CV. Las operaciones de interdicción, por ejemplo, pueden crear oportunidades futuras para perturbar las finanzas.

Las operaciones en el ciberespacio pueden tener como objetivo la propaganda de Internet y crear oportunidades para reducir el atractivo de las redes de amenazas para las poblaciones neutrales.

(d) ¿Qué se necesita hacer para aplicar presión en múltiples puntos a través de los instrumentos del poder nacional (diplomático, informativo, militar y económico) a las redes de amenazas objetivo para lograr el estado final militar deseado por el JFC?

(3) Las unidades militares consideran que las tareas de estabilidad son las más difíciles de analizar, ya que se llevan a cabo entre una población civil. Agregar una dinámica social complica el uso de fórmulas matemáticas y deterministas cuando la naturaleza humana y las interacciones sociales juegan un papel importante en la OE. Las superposiciones entre las redes de amenazas y las redes neutrales, como la población civil, complican las evaluaciones y el análisis de los efectos de segundo y tercer orden.

(4) La causa próxima de los efectos en situaciones complejas puede ser difícil de determinar. Incluso los efectos directos en estas situaciones pueden ser más difíciles de crear, predecir y medir, particularmente cuando se relacionan con cuestiones morales y cognitivas (como la religión y la "mente del adversario", respectivamente). Los efectos indirectos en estas situaciones suelen ser difíciles de prever. Los efectos indirectos a menudo pueden ser involuntarios y no deseados, ya que siempre habrá lagunas en nuestra comprensión del OE. Las acciones impredecibles de terceros, las consecuencias no deseadas de operaciones amigas, la iniciativa y creatividad subordinadas y la niebla y la fricción del conflicto contribuirán a una EO incierta. La simple determinación de efectos no deseados en las redes de amenazas requiere un mayor grado de pensamiento crítico y análisis cualitativo que las operaciones tradicionales. No se pueden ignorar los efectos no deseados en las redes neutrales y amigas.

(5) El análisis estadístico es necesario y permite analizar grandes volúmenes de datos, pero el pensamiento crítico debe preceder a su uso y el análisis cualitativo debe acompañar cualquier conclusión. SNA es una forma de análisis estadístico de redes humanas que ha demostrado ser una herramienta particularmente valiosa para comprender la dinámica de la red y mostrar los cambios de la red a lo largo del tiempo, pero debe complementarse con otros tipos de análisis y análisis de inteligencia tradicionales. Puede apoyar el proceso JIPOE, así como los procesos de planificación, focalización y evaluación. SNA requiere una importante recopilación de datos y, dado que es difícil recopilar datos sobre las redes de amenazas y pueden adaptarse sin ser vistos, se debe utilizar junto con otras herramientas.

Para obtener más información, consulte el Apéndice G, "Análisis de redes sociales".

c. Comunicar la evaluación

(1) La evaluación de las actividades de la CTN sólo es valiosa para el comandante y otros participantes si se comunica de manera efectiva en un formato que permita cambios rápidos en las LOO/LOE y acciones operativas y tácticas para las actividades de la CTN.

(2) Comunicar la evaluación de CTN de forma clara y concisa con información suficiente para respaldar las recomendaciones del personal, pero sin demasiados detalles triviales, es un desafío.

(3) Los productos de evaluación CTN bien diseñados muestran cambios en los indicadores que describen la OE y el desempeño de las organizaciones en lo relacionado con las actividades del CTN.

ANEXO A

ABREVIATURAS Y ACRÓNIMOS

AFTTP	Tácticas, técnicas y procedimientos de la Fuerza Aérea.
C2	Comando y control
CARVER	Criticidad, accesibilidad, recuperabilidad, vulnerabilidad, efectividad y reconocimiento
CCDR	Comandante combatiente
CCIR	Requisito de información crítica del comandante.
CCMD	Comando combatiente
CD	Antidrogas
CFA	Análisis de factores críticos
COA	Curso de acción
COG	Centro de gravedad
COIN	Contrainsurgencia
CR	Requisito crítico
CT	Contraterrorismo
CTN	Contrarrestar las redes de amenazas
CV	Vulnerabilidad crítica
D3A	Decidir, detectar, entregar y evaluar
DOD	Departamento de Defensa
F2T2EA	Encontrar, arreglar, rastrear, apuntar, involucrar y evaluar
F3EAD	Encontrar, arreglar, terminar, explotar, analizar y difundir