CAPÍTULO SEGUNDO

LA LUCHA CIED: LA INTELIGENCIA EN LAS ACTIVIDADES DE PREVENCIÓN

LA LUCHA CIED (1): LA INTELIGENCIA EN LAS ACTIVIDADES DE PREVENCIÓN

Por Alejandro Morón Zamora

Introducción

A los ataques contra Estados Unidos, el 11 de septiembre de 2001, siguieron una serie de operaciones en el contexto de lo que su Gobierno denominó «guerra global contra el terrorismo» y que supusieron las intervenciones militares en Afganistán e Irak, paradigmas del concepto de «guerra asimétrica».

En una «guerra asimétrica» el adversario (grupos insurgentes, terroristas, talibanes, etc.) no puede infligir una derrota militar contra las fuerzas propias, sin embargo, no renuncia a conseguir sus objetivos, atacando uno de los centros de gravedad más importantes de los países occidentales: la voluntad política de mantener una operación militar o participar en ella. Para ello, realiza una serie de ataques indiscriminados contra fuerzas militares o población civil.

Este adversario constituido por una combinación de voluntades, está formado por redes humanas que se extienden desde el ámbito local al global y utilizan artefactos explosivos improvisados o IED,s *(Improvised Explosive Devices)*. Un arma ya conocida, que ha adquirido una gran relevancia, no sólo por las bajas que producen, sino por el impacto mediático, que a su vez influye en las decisiones políticas, lo que merece un estudio especial.

(1) *Counter Improvised Explosive Device Defeat Organization.*

Este estudio se ha traducido en la generación de doctrina en el ámbito de la Organización del Tratado del Atlántico Norte (OTAN), de las Fuerzas Armadas de Estados Unidos, Reino Unido y otros países, la creación de estructuras conjuntas y combinadas específicas para combatirla –JIEDDO (2), CEO-CIED (3) de la OTAN en España–, y la inversión de millones de euros en investigación y desarrollo para proteger a las fuerzas y mitigar sus efectos.

Los IED,s proliferan porque ofrece al adversario «asimétrico» el arma más eficaz y fácilmente accesible para imponer su voluntad a una fuerza militar numérica y tecnológicamente superior. Son simplemente un método para alcanzar sus objetivos militares y políticos, a corto y largo plazo.

Hasta hace relativamente poco tiempo, la mayoría de los esfuerzos para la lucha Contra-IED (CIED) se centraron en combatir al artefacto. Hoy en día este concepto es mucho más amplio. Es una actividad global, multidisciplinar y multifuncional, y que afecta a todas las áreas de planeamiento, conducción y ejecución de las operaciones.

En este sentido, la finalidad del trabajo es valorar el papel de la función inteligencia en la lucha CIED, estableciendo como hipótesis que la única forma de luchar contra la amenaza que supone el uso de los IED,s es tener una estrategia integrada al más alto nivel, en la que tiene un papel fundamental la predicción y prevención mediante la explotación de la inteligencia específica disponible.

Para ello, se expondrá en primer lugar en qué consiste la amenaza a la que nos enfrentamos, continuando con un recorrido que nos permita ver cómo se está desarrollando la lucha CIED, el examen del papel de la inteligencia en dicha lucha, terminando con la extracción de una serie de conclusiones que nos permita entender el problema y como abordarlo desde el punto de vista de la inteligencia:

> «IED,s are the enemy's equivalent of artillery and artillery has always been the largest killer on the battlefield.»
>
> General Montgomery C. Meigs, USA
> *Ex director del JIEDDO*

(2) *Joint Improvised Explosive Device Defeat Organitation.*
(3) Centro de Excelencia CIED de la OTAN.

La amenaza IED

Generalidades

Un IED es un artefacto colocado o fabricado de manera improvisada, incorporando agentes destructivos, letales, nocivos, pirotécnicos o incendiarios, y diseñados para destruir, incapacitar, hostigar o distraer (4). Son armas de empleo táctico que, en la actualidad, pueden llegar a tener un efecto en el nivel estratégico, por sí solas o, si se combinan con una campaña de información.

Su concepto no es nuevo, pero la combinación de sus efectos y su difusión en los medios de comunicación (televisión, prensa escrita, Internet, etc.) produce un impacto directo en la percepción de la población, la cual, puede influir en las decisiones que afectan a una operación al más alto nivel. Por tanto, sus efectos van más allá de los destructivos, ya que, manifiesta el poder del adversario, mientras demuestra la debilidad propia, destacando la incapacidad para prevenirlos.

En consecuencia, los IED,s son una elección muy lógica por parte de un adversario asimétrico para usar contra fuerzas convencionales, cuando no pueden equipararse a ellas ni en número y ni en tecnología.

EL ATAQUE IED

Un IED puede ser empleado de muchas formas diferentes, pueden estar diseñados para matar o herir, dañar o destruir vehículos, infraestructuras o una combinación de todo lo anterior para causar alarma o crear inseguridad; pueden usar explosivos comerciales, militares, o caseros, municiones militares o sus componentes.

Para entender mejor como se emplean es necesario un conocimiento básico y para ello es muy útil establecer una clasificación. En el marco de la OTAN y en la mayoría de los países se establecen dos criterios básicos, en función del método de colocación y de los dispositivos de iniciación que utilizan.

Los métodos de emplazamiento de un IED pueden ser diversos los más generales son:

– Depositado o enterrado. Se entiende cuando son colocados o arrojados a mano para atacar un objetivo, inmediatamente o esperando su llegada.

(4) AJP-3.15: CIED *(Allied Joint Doctrine for Countering Improvised Explosive Device)*.

– Transportado en Vehículo (VBIED). Cuando se emplea cualquier tipo de vehículo, incluidas las bicicletas, los automóviles, camiones, aviones, barcos, Vehículos Aéreos no Tripulados (UAV) y sumergibles.
– Proyectado. Por su forma improvisada de proyectarlo aunque se empleen materiales reglamentarios.
– Transportado por Personas (PBIED). Cuando una persona carga con un IED usando un chaleco, cinturón, mochila, etc. En muchas ocasiones es iniciado por la misma persona que lleva el artefacto (ataque suicida).
– Enviado. Por correo o entregado por otro medio que implique aquellos ajenos a la organización.

Los dispositivos de iniciación más comunes los podemos agrupar en tres clases:

1. Activado por el operador o terrorista. Mediante un dispositivo de control que permite la separación entre la carga explosiva principal y el punto de activación, ofreciendo la posibilidad de elegir el momento óptimo para crear el mayor efecto sobre el objetivo. Existe una gran variedad de dispositivos de iniciación los más empleados son por cable y radio control:
   – Activado por Cable (CWIED). El punto de activación y el iniciador de la carga explosiva principal están unidos por un cable eléctrico.
   – Activado por Radio Control (RCIED). Mediante un transmisor en el punto de activación y de un receptor asociado que detona la carga.
2. Activado por temporizador. Tras estudiar nuestras rutinas, se puede emplear un temporizador para activar el artefacto al paso de una patrulla o convoy.
3. Activado por la Víctima (VOIED). Cuando el artefacto se inicia por las acciones de una persona. Existen una gran variedad que pueden incluir la presión, alivio de presión, tensión, alivio de tensión, pasivos o activos, infrarrojo, cable, sensible a la luz, a la inclinación, espoleta de proximidad y acústicos, etc. Pueden elegir un objetivo específico (artefacto colocado en una carretera) o estar colocados para proteger infraestructuras *(bobby traps)*.

Los tipos de IED,s se pueden emplear solos, combinando varios de ellos del mismo o diferente tipo, con un sólo dispositivo iniciación o varios y con otros sistemas de armas para producir ataques complejos. Los posteriores ataques que se realizan después del principal, normalmente, están destinados al personal que responde al ataque inicial (equipos de desactivación, personal de evacuación, etc.).

Para realizar un ataque con IED,s, el adversario tiene que llevar a cabo un gran número de actividades. Necesita crear una organización, que incluirá personal, recursos y procedimientos, y al que se denomina Sistema IED. Dentro de este Sistema se pueden identificar un determinado número de subsistemas; éstos son interdependientes aunque algunas actividades concretas se pueden realizar aisladamente.

Este Sistema no es ni lineal ni jerárquico (5), sin embargo sus subsistemas, nodos y elementos están interconectados de muchas y variadas formas. La importancia de los nodos de actividades y las relaciones entre ellos pueden variar a lo largo del tiempo y en el espacio. Es importante destacar que la ejecución del ataque, en sí mismo, es llevada a cabo únicamente por un simple nodo del sistema.

En este Sistema IED se puede identificar tres fases: *planeamiento y adquisición de recursos, ejecución y explotación*. Estas fases siguen un proceso secuencial, aunque lo probable es que se realicen concurrente o simultáneamente, basándose en la estrategia del adversario, figura 1, p. 64.

El planeamiento y adquisición de recursos incluye entre otros el apoyo técnico y financiero, el reclutamiento de personal, el entrenamiento, y la adquisición de los materiales necesarios para la fabricación del IED, el liderazgo, apoyo social, ideológico, etc. Es en esta fase donde se realiza un plan general para llevar a cabo la campaña de ataques.

En la fase de ejecución se realizan aquellas actividades que son necesarias para llevar a cabo el ataque específico. Es decir, una vigilancia para permitir la selección de los objetivos, la confección de un plan más detallado, la realización de ensayos, el traslado del artefacto o sus componentes y el emplazamiento en el lugar elegido para hacerlo detonar en el momento adecuado para producir el efecto deseado.

La explotación de los efectos del ataque se realiza con la finalidad de evaluar y dar publicidad al mismo. La evaluación se realiza para alcanzar dos objetivos; primero, para medir el éxito del IED contra el objetivo y obtener lecciones aprendidas para la confección de futuros artefactos; y segundo, para observar y aprender las respuestas de la fuerza objetivo

(5) La diferencia entre los actuales grupos insurgentes o terroristas con las clásicas organizaciones «guerrilleras», que estaban perfectamente estructuradas y jerarquizadas.

para conocer sus Tácticas, Técnicas y Procedimientos (TTP,s). Dar publicidad al ataque IED es un elemento fundamental en la estrategia del adversario. Las imágenes y otros detalles del ataque IED son grabados y mostrados en los medios de comunicación (televisión, Internet, prensa escrita, etc.), para mostrar su poder, al mismo tiempo que muestra la incapacidad propia para evitarlos. Sin embargo, la explotación que hace el adversario de los IED,s va más allá del ataque, ya que, las imágenes y las declaraciones de los líderes, campos de entrenamiento, etc., son también explotadas para alcanzar sus objetivos.

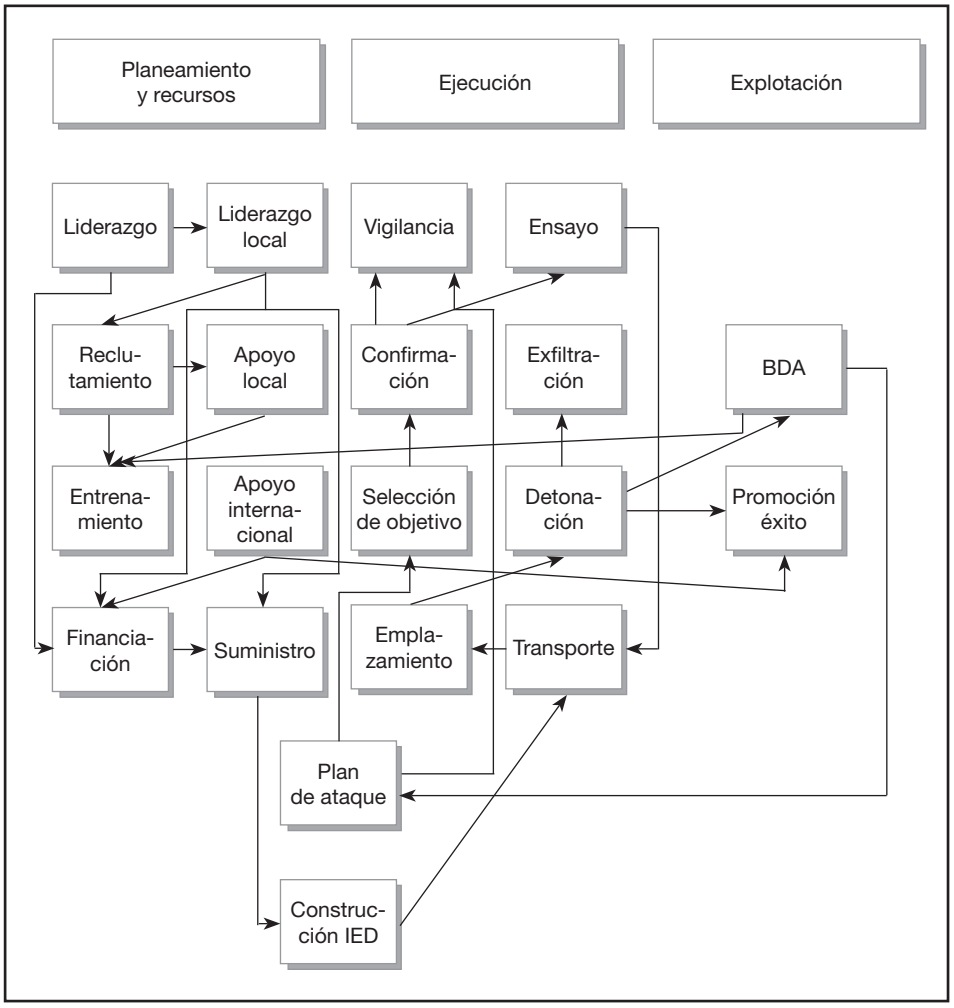

Figura 1.— *Sistema y Subsistemas IED.*

La lucha CIED

Objetivo de la lucha CIED

La lucha CIED se define como un esfuerzo colectivo en todos los niveles de planeamiento y conducción de las operaciones para derrotar el Sistema IED, reducir o eliminar los efectos de los ataques con IED,s, para el cumplimiento de la misión. Estos esfuerzos implican la aplicación de medidas políticas, diplomáticas, legales, militares y de investigación y desarrollo. Es decir, la lucha CIED es la lucha contra un sistema; un sistema de personas que está organizado para utilizar y sacar beneficio de un arma cuyos efectos tienen reflejo en todos los niveles y, por lo tanto, debe integrar todo esfuerzo para derrotar cualquier subsistema, nodo o actividad que lo constituye.

Los pilares de la estrategia CIED

Por la necesidad de un enfoque integral, estructurado y continuo en todos los niveles para llevar a cabo la lucha CIED, podemos considerar tres pilares como herramienta conceptual; *la lucha contra el sistema, la lucha contra el artefacto* y *la instrucción y adiestramiento*; son complementarios, deben aplicarse a todo el espectro de las actividades CIED y, como muestra la figura 2, p. 66, con elementos comunes.

La lucha contra el sistema tiene como finalidad impedir que el adversario haga uso de los IED,s mediante la disrupción y anticipación de la cadena de eventos del sistema. Permite prevenir que un IED pueda ser colocado y detonado, impidiendo el suministro de componentes, financiación, etc. También debe prevenir la explotación que el adversario pueda hacer de las actividades de cualquier elemento del Sistema IED, ya que esta actividad es imprescindible en la estrategia del adversario.

La lucha contra el artefacto se refiere al dispositivo una vez que está preparado para su uso. Incluye localizar el artefacto y sus correspondientes componentes; identificar los indicios previos a un ataque; el despliegue adecuado de medios CIED para su neutralización; y el empleo de TTP,s (como el mantenimiento de distancias de seguridad) y medios técnicos y materiales (perturbadores, blindaje, etc.).

La instrucción y adiestramiento abarca las acciones para garantizar una capacidad CIED en todas las estructuras, integrada en la formación básí-

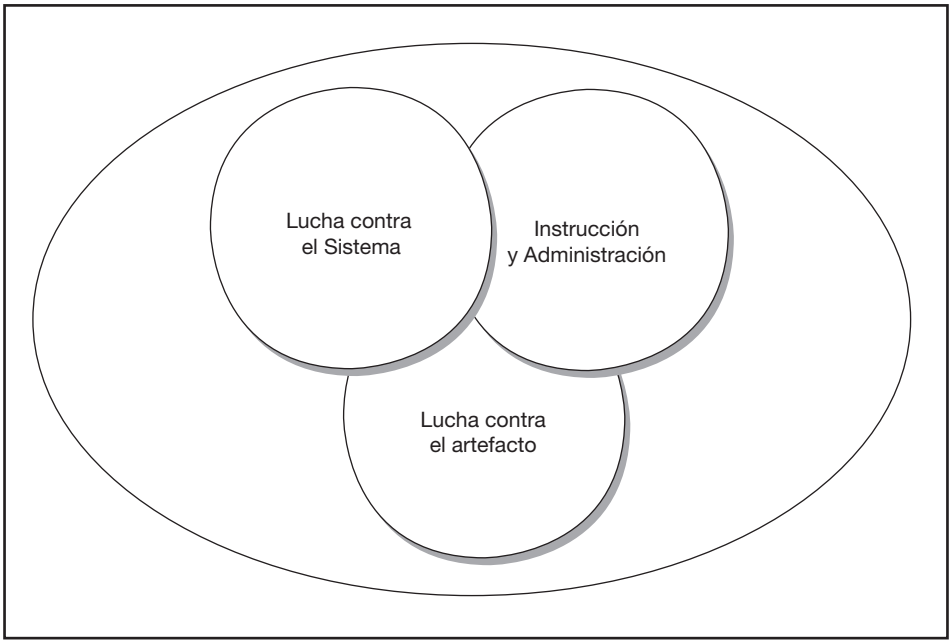

Figura 2.— *Pilares de la estrategia CIED.*

ca, adiestramiento de unidades, específica para cada operación e intrateatro (6). También implica que la inteligencia disponible sobre TTP,s del adversario se difundan rápidamente a las fuerzas propias para que sus TTP,s puedan ser modificadas y sean lo más actualizadas, adecuadas y eficaces posible. Se estima que, en las operaciones, el éxito se debe en un 60% a la instrucción y adiestramiento en TTP,s, el 30% a la tecnología y el 10% al azar (7).

Actividades clave CIED (8)

Dentro de los pilares de la estrategia descritos en el apartado anterior existen una serie de actividades que forman la base de la lucha CIED. Éstas son: *predecir* las acciones del Sistema IED del adversario; *prevenir* la ejecución de los mismos; *detectar* actividades, materiales, componentes

(6) De conformidad con MC-0458/1, esta formación debe ser impartida según los estándares de la OTAN, y es responsabilidad de la OTAN, especialmente del mando aliado de transformación, armonizar y estandarizar la educación y la formación.
(7) AJP-3.15: CIED *(Allied Joint Doctrine for Countering Improvised Explosive Device)*.
(8) Esta denominación es la que aparece en el borrador del concepto nacional de la lucha CIED.

y dispositivos; *neutralizar* los artefactos y/o los dispositivos de iniciación; *mitigar* los efectos de los IED,s en caso de que se produzcan detonaciones; y *explotar la información* de todas las actividades del Sistema IED y de los propios artefactos, mediante el registro y análisis de la información pertinente (9). En la figura 3, p. 68, se representa de forma esquemática la manera en que se pueden aplicar estas actividades en toda la amplitud del Sistema IED.

PREDECIR

La predicción trata de anticiparse a las actividades del Sistema IED. La inteligencia juega un papel fundamental en esta actividad ya que mediante un minucioso y continuo análisis de inteligencia, se debe establecer un conocimiento de los nodos, de sus probables actividades y secuencia de acontecimientos. Algunas fuentes limitan esta actividad a la fase de planeamiento y adquisición de recursos, sin embargo, abarca toda la amplitud de actividades del Sistema. Esto favorece un conocimiento más profundo y global del Sistema y su entorno, y así, se pueden crear escenarios futuros, adelantarse al ciclo de decisión del adversario y, determinar cuáles son sus futuras actividades, dónde y cómo van a operar sus nodos, la evolución de sus TTP,s, dónde volcaran sus esfuerzos y dónde serán sus ataques y como serán éstos.

PREVENIR

La prevención tiene un carácter proactivo u ofensivo, e implica la acción contra los nodos o conexiones del sistema para hacer que el adversario no pueda llevar a cabo ataques IED con éxito. El conocimiento adquirido durante las acciones desarrolladas durante la predicción alimenta el proceso de *Targeting* (10) que, es en definitiva, la actividad que permite mantener la iniciativa en el teatro de operaciones. De esta manera se previene que el adversario coloque y detone los artefactos por la destrucción, eliminación o neutralización de los nodos o conexiones que conforman el sistema. También puede implicar la acción contra los nodos que realizan la explotación del ataque y, así, prevenir que el adversario pueda sacar provecho del mismo.

---

(9) Estas actividades varían en número, concepto y ámbito de aplicación en función de las fuentes que se consulten, por ejemplo, el Reino Unido establece también en su Joint Doctrine Note 5/06 *Countering Improvised Explosive Devices,* la *disuasión.*

(10) Adquisición y asignación de objetivos.

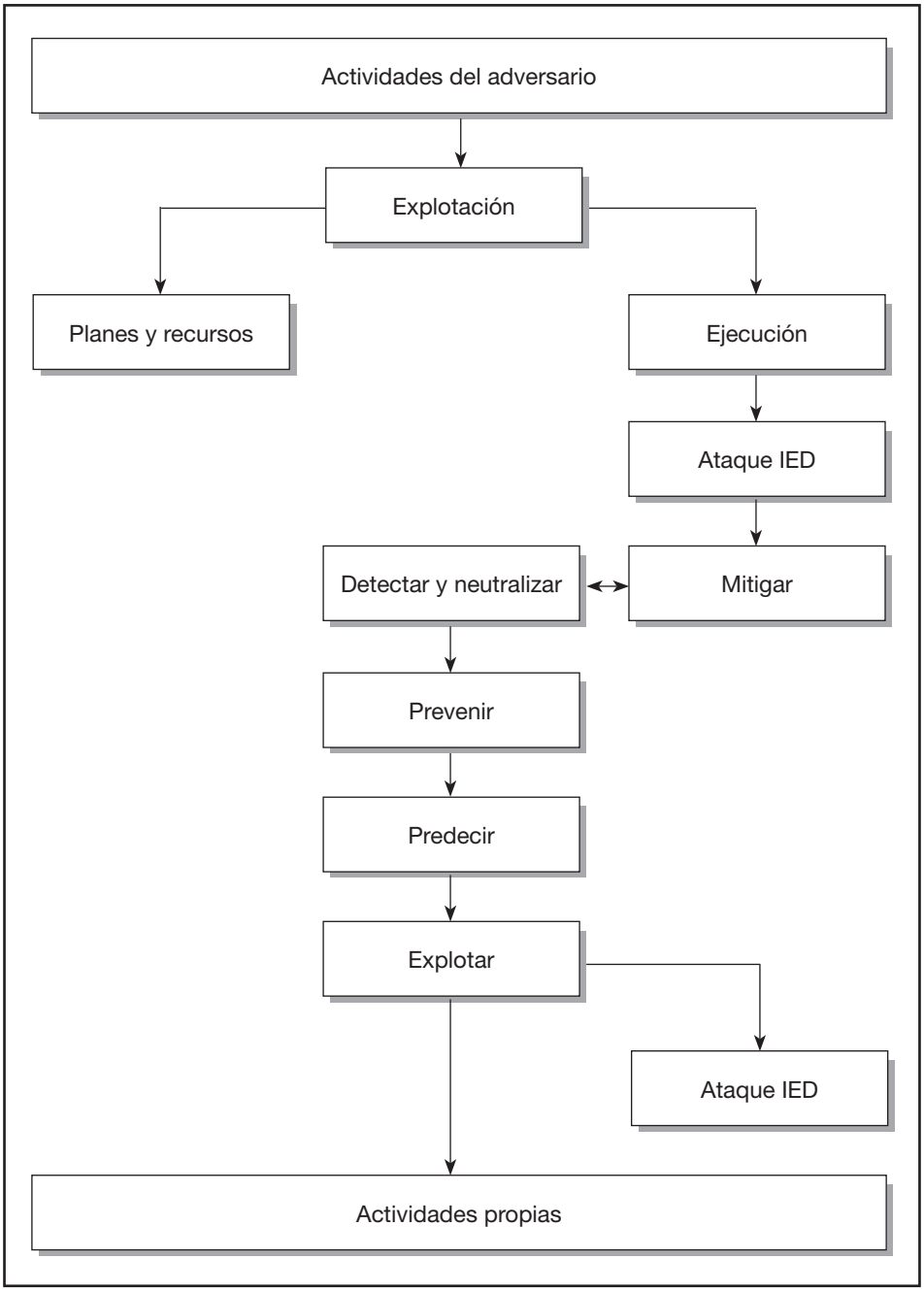

Figura 3.— *Aplicación de las actividades clave contra el Sistema IED.*

DETECTAR

Las actividades de prevención no evitarán totalmente el empleo de IED,s por parte del adversario. Por lo tanto, una actividad fundamental será detectar los indicios de que se va a producir un ataque, de un IED después de haber sido colocados y de las actividades y personas implicadas en el mismo. Para ello, tanto las TTP,s propias, como el material y equipo desempeñan un papel importante. Los productos de inteligencia son muy útiles para esta actividad, ya que, la difusión de TTP,s del adversario, las zonas más probables de ataque, etc., ayudaran a las fuerzas a detectar aquellos indicios que los preceden. Tanto los indicios como los productos variaran en función del nivel de planeamiento y conducción considerado.

NEUTRALIZAR

Una vez colocado, es necesario neutralizar el artefacto para impedir su funcionamiento, de modo que las fuerzas y la población local pueda operar con seguridad. La neutralización puede ser temporal o permanente:

– *Neutralización temporal*. Este efecto se consigue con la perturbación electrónica (11) que impide la detonación del artefacto, aunque la detección no haya tenido lugar. No proporciona una protección absoluta, ya que, el adversario intentará contrarrestar su efecto tanto con procedimientos tácticos, como por nuevos conocimientos y medios técnicos.
– *Neutralización permanente.* Una vez que han sido detectados, deben ser neutralizados permanentemente, lo antes posible o cuando la actividad operativa lo permita. Normalmente se llevará a cabo por equipos de especialistas IEDD *(International Enhanced due Diligence)*.

MITIGAR

Consiste en ser capaz de minimizar los efectos resultantes de un ataque (12), cuando las actividades para predecir, prevenir y detectar no han impedido la colocación y detonación de un IED. Mitigar puede incluir medidas técnicas, tácticas, de procedimiento y actividades de información:

(11) Subdivisión de las Contramedidas Electrónicas (ECM), que se define como: «La deliberada radiación o reflexión de energía electromagnética con el objeto de menoscabar la eficacia de los dispositivos electrónicos hostiles».
(12) Tanto los físicos como aquellos derivados de la explotación que hace el adversario del mismo.

– Medidas técnicas. Abarcan medidas de protección para interrumpir o reorientar la energía y los fragmentos de las explosiones.
– Medidas tácticas. Abarcan la adopción de despliegues que consideren distancias de seguridad y posicionamiento de las tropas.
– Medidas de procedimiento. Incluyen procedimientos de reconocimiento de zona, de respuesta ante un ataque, etc. Éstos estarán directamente relacionados con el material y equipo.
– Información. Trata de las medidas a adoptar para contrarrestar las actividades que realiza el adversario para explotar el éxito de un ataque; dando difusión y publicidad de toda la información e imágenes disponible, de la muerte y destrucción deliberada infligidas a las fuerzas militares y población local y sus posesiones por el uso indiscriminado de IED,s.

EXPLOTAR LA INFORMACIÓN

En la explotación los escenarios y los materiales relacionados con un evento IED (13), se registran y analizan, con el fin de conocer, los dispositivos y componentes utilizados, las capacidades de los autores, sus TTP,s y las actividades del Sistema. La explotación puede tener lugar en cualquier momento dentro de las actividades del Sistema IED, pero debe hacerse todo lo posible para llevar a cabo la explotación tan pronto como sea posible en la de cadena de acontecimientos, con el fin de proporcionar inteligencia para adelantarse al ciclo de decisión del adversario y adoptar la medidas oportunas para prevenir el resto de actividades antes de que se produzcan. En la figura, 4 puede observarse el sistema de explotación de la OTAN.

Es decir, la información obtenida en la explotación es sensible al tiempo y requiere un proceso para que en cada nivel se elaboren los productos que se necesiten para responder de manera adecuada en cada uno de ellos, todo esto en una estructura integrada para que la información llegue a todos los niveles y sea convenientemente explotada. La fusión de los productos de la explotación con otros productos de inteligencia es muy importante para el éxito de las otras actividades clave. A su vez el material y la información para la explotación se pueden obtener de cualquiera de ellas.

(13) Evento IED es todo suceso que implique un IED o sus componentes (un alijo de material, una entrega, una búsqueda, neutralización, etc.).

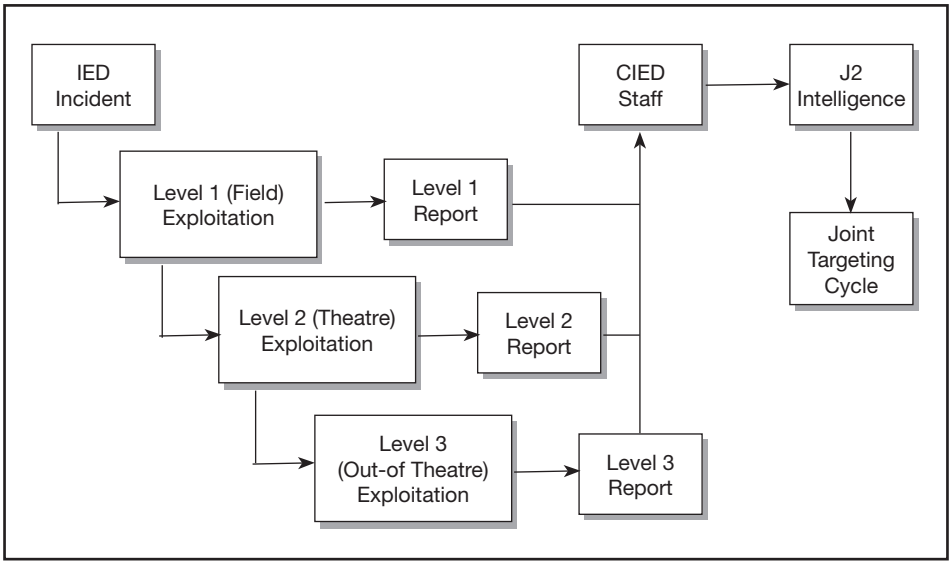

Figura 4.— *Sistema de explotación de la información de OTAN.*

La organización de los cuarteles generales para la lucha CIED

La organización de los carteles generales en cada nivel tendrá que proporcionar las capacidades para poder llevar a cabo el planeamiento y conducción de operaciones CIED y las actividades de seguridad que implican las operaciones en un ambiente con ataques IED.

PLANEAMIENTO Y CONDUCCIÓN DE LAS OPERACIONES

El personal que realiza actividades relacionadas con CIED en un cuartel general debe asegurar que las consideraciones, contramedidas y líneas de acción estén plenamente integradas y sincronizadas en el planeamiento de todas las operaciones. Por lo tanto debe estar implicado en todos los procesos del Grupo de Planeamiento de las Operaciones.

Del mismo modo, para la conducción de las operaciones, debe participar en el centro de operaciones del cuartel general del nivel que se trate, para asegurar la coordinación y sincronización de las actividades CIED con el resto de las operaciones.

ORGANIZACIÓN DEL ÁREA DE CIED

En la organización de un cuartel general que desarrolle operaciones CIED se deben sopesar las ventajas y desventajas de agrupar al personal que realice directamente actividades CIED en un mismo órgano o distribuirlos en la medida de lo posible en las diferentes secciones del Estado Mayor. Es decir, crear una célula permanente o establecer un grupo de trabajo específico.

Tanto en un caso como en otro, al agrupar el personal CIED se debe poner bajo el mando un jefe CIED. La entidad de esta célula dependerá del tamaño del cuartel general, del grado de amenaza y del carácter de la operación, como mínimo debería incluir las funciones principales de EOD *(Explosive Ondwance Dispposal)*, explotación y ECM (14). Puede incluir individuos o células de alguna o todas las divisiones del cuartel general, pero es particularmente probable que sea necesario dedicar en exclusiva una célula de inteligencia.

La posición del jefe CIED y el personal que realiza actividades CIED dentro del cuartel general se puede establecer de acuerdo con uno de los siguientes tres modelos:

1. *Estado Mayor Especial*. Cuando exista una gran amenaza, organizar la estructura CIED a este nivel asegurara que se consideren las operaciones CIED al más alto nivel de toma de decisiones.
2. *Nivel División/Sección de Estado Mayor.* Organizar la estructura CIED dependiendo directamente del jefe de Estado Mayor aseguraría su consideración al más alto nivel en el planeamiento y conducción de operaciones.
3. *Dentro del área de operaciones del Estado Mayor* (15). Organizar el personal CIED dentro del área de operaciones, subordinado al jefe de la misma ofrece la ventaja de un mayor nivel de cooperación, aunque se puede reducir el nivel de influencia directa del jefe CIED.

CAPACIDADES PRINCIPALES CIED

Existen una serie de capacidades que cobran especial importancia y que están, directa y exclusivamente, para apoyar a las actividades CIED y

(14) Según el AJP-3.15.

(15) Tradicionalmente la célula CIED ha estado subordinada al área de ingenieros de la División de Operaciones.

deberían estar organizadas o controladas por personal especializado. Éstas son las que se describen a continuación:

– EOD. Siempre que haya amenaza IED es importante que la capacidad EOD pueda efectuar una respuesta eficaz también con suficientes equipos IEDD (16). Agrupar la célula dentro del área CIED logrará sinergia y eficacia, ya que optimiza la coordinación de la función EOD con la explotación CIED. Los objetivos de las dos funciones (neutralización de artefactos por un lado y preservación y recuperación de material técnico y forense por el otro) se oponen el uno al otro, pero el entendimiento y cooperación mutuos aseguraran que los artefactos se neutralicen con seguridad a la vez que se logra un máximo nivel de explotación de información.
– Explotación CIED. El personal que realiza actividades de explotación CIED debe cotejar los informes de explotación de todos los niveles y asegurarse de que sirven a la inteligencia para posteriores análisis, ya que son componentes importantes para el resto de actividades clave. Es más, junto con el proceso de inteligencia, alimenta el proceso de *Targeting* y así apoya las actividades de *prevención*. Además se encarga de difundir los cambios y desarrollos en las TTP,s del adversario para mejorar las propias e integrarla en la instrucción y adiestramiento.
– ECM. Hay dos funciones particulares de ECM que deben llevarse a cabo por el área CIED, ambas requieren un enlace eficaz entre el área de inteligencia y comunicaciones. Por un lado se encarga del seguimiento, registro y difusión del uso del espectro electromagnético de los RCIED,s, para que todos los elementos de la fuerza tengan la información actualizada y puedan emplear sus ECM,s en consecuencia. Por otro, asegurar que las medidas ECM usadas en el teatro han sido declaradas para supervisar y coordinar su uso, y así, asegurar el empleo del espectro electromagnético y el riesgo que suponen las interferencias mutuas.

ÁREAS DE ESTADO MAYOR RELACIONADAS CON CIED

Estas áreas tienen una perspectiva más amplia de las operaciones que la propia CIED pero tienen un papel importante que jugar en la ejecución de las actividades clave. Las más importantes son:

(16) Las capacidades EOD e IEDD no son las mismas, las últimas requieren un nivel de formación y experiencia más alto.

– Inteligencia. La misión del área de inteligencia no es otra que la propia misión genérica de inteligencia aplicada a CIED. Esto es, dirigir el esfuerzo de obtención, obtener, elaborar y difundir inteligencia.
– Operaciones. El área de operaciones planea y conduce las operaciones CIED. Y además, proporciona las orientaciones sobre todas las TTP,s y programas de formación utilizados en el teatro.
– Guerra Electrónica (EW). Colabora en la definición de la amenaza de RCIED,s. Propone medidas de protección y asegura el empleo del espectro electromagnético por parte de las fuerzas propias. Es especialmente importante la coordinación de los medios de protección con el empleo de las comunicaciones.

Otras áreas relacionadas con la lucha CIED son: ingenieros, protección de la fuerza, Operaciones de Información (INFOOPS), Operaciones Psicológicas (PSYOPS), Cooperación Cívico-Militar (CIMIC), etc. Todas, más aquellas que se consideren necesarias. Para conseguir el efecto sinérgico, es necesario que la estructura CIED establezca los foros de

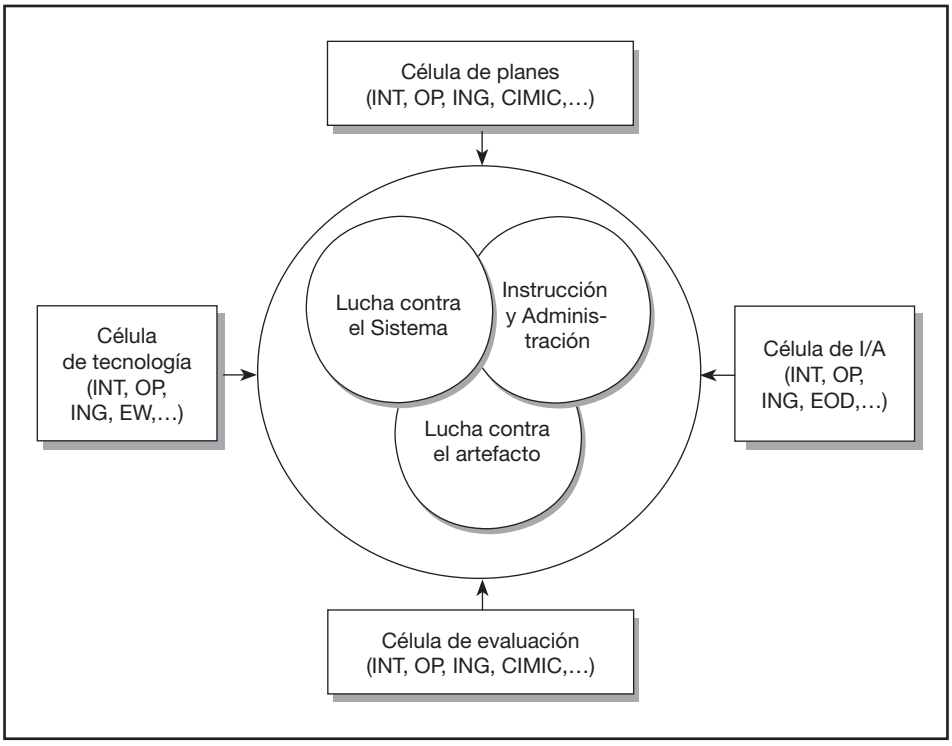

Figura 5.— *Grupo de Trabajo CIED.*

coordinación para integrar todas las actividades CIED. En la figura 5 se expone como puede organizarse un grupo de trabajo CIED.

La inteligencia en la lucha CIED

Una vez expuesta la amenaza a la que nos enfrentamos y como se está desarrollando la lucha CIED, principalmente en el ámbito de la OTAN, vamos a centrarnos en el papel que tiene la inteligencia en el proceso. Conceptualmente la predicción parece ser responsabilidad del personal de inteligencia y la prevención de operaciones, pero hay que considerar que el área de inteligencia tiene mucho que aportar en la prevención, como veremos a continuación.

En una primera parte se van a exponer unas consideraciones sobre la función inteligencia en las actividades de predicción y prevención; a continuación se especificarán algunas particularidades de la información e inteligencia necesarias para estas actividades dentro del ciclo de inteligencia, en concreto del proceso de contrainteligencia.

La inteligencia en las actividades de prevención de la lucha CIED

En el nivel estratégico, el ciclo de inteligencia, debe proporcionar el conocimiento necesario para aislar el Sistema IED adversario de sus influencias, financiación y suministros exteriores; en los niveles operacional y táctico, se pone a disposición de los responsables en la aplicación de las actividades clave contra toda la amplitud del Sistema IED adversario, figura 6, p. 76.

Los productos de inteligencia sobre el Sistema IED que requiere cada actividad es diferente, sin embargo, la información y la inteligencia debe de tratarse de una forma global pues lo adquirido y/o elaborado por los elementos involucrados en una determinada actividad son de interés para desarrollar otras actividades contra el Sistema. Por ejemplo, la inteligencia proporcionada por la información obtenida en la neutralización de un artefacto, puede ser de utilidad para identificar el personal implicado en el suministro y la fabricación, y así favorecer la prevención.

Como ya se ha expuesto en apartados anteriores, para poder contrarrestar la amenaza debemos ser capaces de poder llevar a cabo las activi-

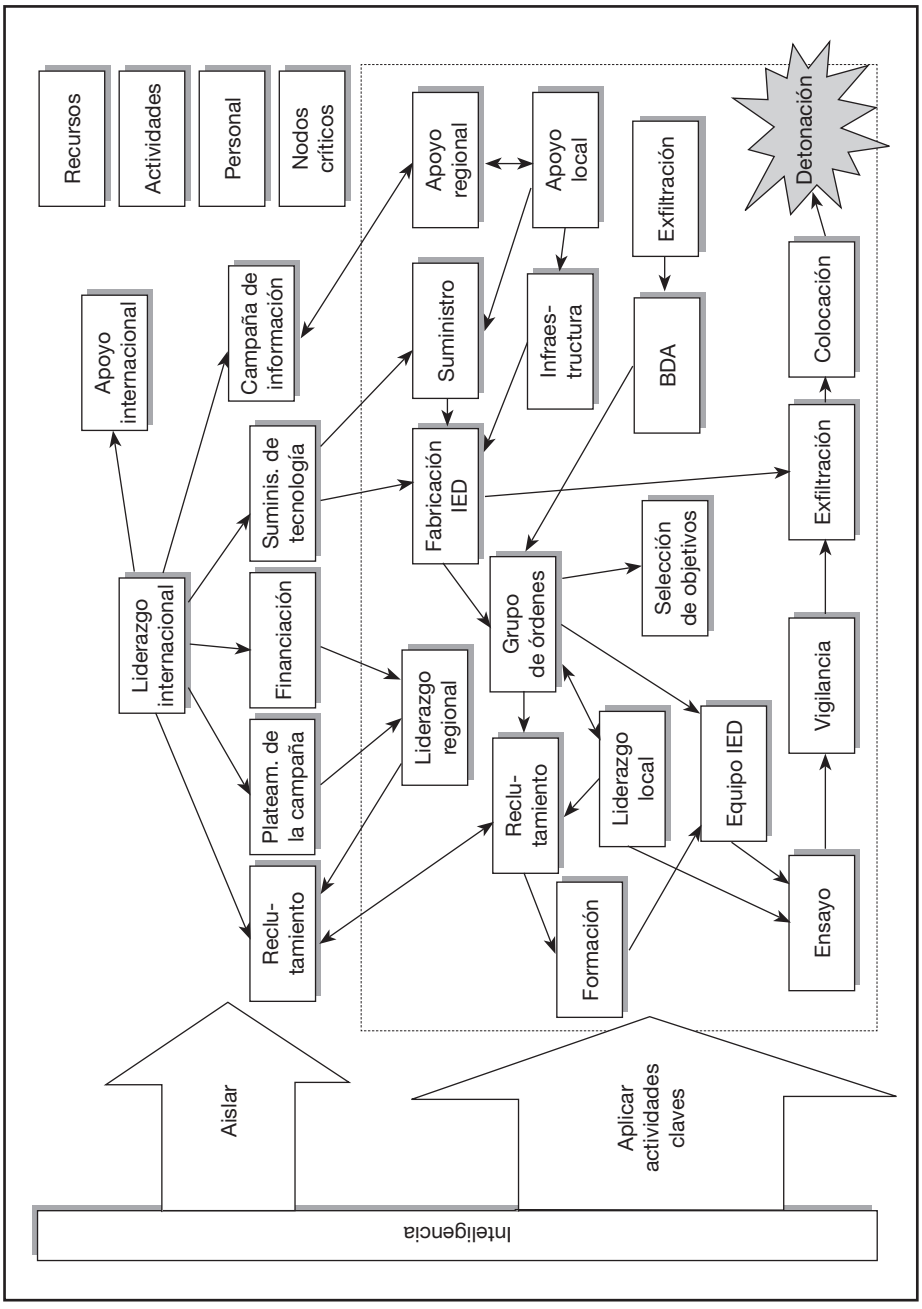

Figura 6.– *La inteligencia en apoyo a la lucha CIED.*

dades clave, es decir, predecir, prevenir, detectar, neutralizar y mitigar. La explotación se nutre y nutre de información a todas y cada una de estas actividades. Ahora bien, las actividades de prevención requieren de una predicción previa y ésta requiere un minucioso y continuo análisis de inteligencia para desarrollar y mantener un profundo conocimiento de todas las partes del Sistema IED. Siendo la explotación de información de las actividades del Sistema IED, entre otras, una importante fuente de información para el proceso de inteligencia.

La predicción y la prevención son actividades que se centran fundamentalmente en la lucha contra la red de nodos, personas y actividades que constituyen el Sistema IED. En gran medida esta red de nodos y personal que desarrollan las actividades necesarias para ejecutar un ataque IED, pueden coincidir con nodos y personal del adversario, grupos insurgentes o terroristas, que desarrollarán actividades de otro tipo contra las fuerzas propias. Las actividades del adversario conducentes o no a la ejecución de un ataque IED incluirán, entre otras, la vigilancia y observación de nuestras fuerzas y sus actividades, para estudiar nuestras vulnerabilidades y determinar la selección de sus objetivos y el momento adecuado para ejecutar el ataque sobre los mismos.

En este aspecto, el área de inteligencia debe proporcionar la información y las valoraciones sobre las capacidades de obtención del adversario –Inteligencia Humana (HUMINT), Inteligencia de Imágenes (IMINT), Inteligencia de Señales (SIGINT), etc.–, determinar su ciclo decisión en el que son capaces de utilizar la información obtenida, desarrollar las posibles medidas a adoptar para neutralizar o limitar estas capacidades y reducir nuestras vulnerabilidades y, de este modo, proponer las medidas de Protección de la Fuerza y de Seguridad de las Operaciones (OPSEC). Es decir, debe ser el Área de Contrainteligencia y Seguridad (CI&S), dentro del área de inteligencia, el que esté implicado, en mayor medida, en las actividades de predicción y prevención.

Además, si los IED,s son un método de los grupos insurgentes o terroristas para alcanzar sus objetivos políticos y militares y para ello utilizan técnicas subversivas, terroristas, sabotaje, e incluso fuentes de financiación del crimen organizado; debería ser el área de CI&S, a la que le concierne identificar y actuar contra las amenazas Terrorismo, Espionaje, Subversión, Sabotaje, Crimen Organizado (TESSCO), la que estuviera más implicada en estas dos actividades clave de la lucha CIED.

Es decir, podemos concluir que, aunque conceptualmente la prevención es responsabilidad del área de operaciones, el área de CI&S también realiza actividades conducentes a la prevención. Por lo tanto, la elaboración de inteligencia que alimenta las actividades de predicción y prevención debería seguir el proceso o ciclo de contrainteligencia.

El proceso de contrainteligencia en las actividades de Predicción & Prevención (P&P)

Para producir la inteligencia que apoye las actividades P&P en la lucha CIED, toda la información específica disponible debe seguir el proceso que defina e identifique la amenaza, busque lo que se desconoce y la elabore, antes de difundirla, a todos aquellos órganos y estructuras implicados en la misma, es decir, es necesario llevar a cabo el ciclo de contrainteligencia.

FASE DE DIRECCIÓN

Durante esta fase del ciclo se determinan las necesidades de inteligencia, se planea la obtención y, se emiten y controlan las órdenes y peticiones de obtención. Las necesidades de inteligencia que apoyen la lucha CIED irán orientadas a la *predicción* de las actividades del sistema y de sus nodos, y la evolución de la situación. El planeamiento del esfuerzo de obtención debe incluir los órganos apropiados para satisfacer necesidades de inteligencia específicas (SIGINT, IMINT, etc.) y a todas las fuerzas, esto es particularmente importante ya que debe ser misión de toda unidad, por pequeña que sea, obtener información sobre el ambiente que rodea la operación e identificar zonas conflictivas.

Antes de que el proceso de confección del plan de obtención tenga lugar, se deben de identificar los indicadores (17) apropiados en cada nivel que preceden a un ataque IED, por ejemplo, aumento de las comunicaciones entre el personal de los nodos, adquisición de materiales (explosivos, teléfonos móviles, cableado, componentes electrónicos, etc.), aumento de la vigilancia, actividades externas, como aparición de declaraciones de líderes en medios de comunicación social, situaciones que crean inestabilidad, manifestaciones, etc.

(17) AAP-6 define indicadores como: «Un suceso o información que refleja la intención y capacidad de un enemigo potencial para adoptar o rechazar una línea de acción».

Durante esta fase se lleva a cabo el planeamiento de contrainteligencia, apoyándose en el análisis de la misión y en la evaluación preliminar de la amenaza (18). La evaluación preliminar de la amenaza para las actividades de P&P es fundamental porque ésta se debe centrar en:

– Los grupos subversivos y terroristas que actúan en el área de operaciones y que pueden ejecutar ataques de todo tipo incluidos con IED. Es decir, aquellos grupos o individuos que tienen la voluntad y capacidad de atacar.
– Las capacidades de estos grupos para obtener y analizar información sobre nuestras fuerzas y actividades esto proporciona una estimación sobre la información que posee el adversario de las fuerzas propias, por ejemplo, rutinas de las patrullas, TTP,s de respuesta ante ataques, medidas de protección, etc.
– La influencia de actores y eventos externos a la zona de operaciones (sobre todo en los niveles más altos).
– Las vulnerabilidades de las fuerzas propias frente a estas actividades.

Es decir, el plan de contrainteligencia incluye el estudio previo del Sistema que debe abarcar la red de nodos y relaciones entre ellos, sus puntos fuertes, formación, sus TTP,s, capacidades, métodos y probables intenciones, equipos, infraestructura, mecanismos de apoyo (incluidas las fuentes de material IED) u otras acciones con el fin de la previsión específica IED. Al ser un proceso continuo, esto incluirá el estudio de la información e inteligencia técnica sobre IED disponible, procedente de la explotación, ya qué la evolución y desarrollo de la amenaza IED es constante.

LA FASE DE OBTENCIÓN

La obtención de información específica para la lucha CIED en las actividades P&P se puede llevar a cabo tanto por los órganos de obtención ISTAR (19) como por aquellos específicos de contrainteligencia. Además, como ya se ha mencionado, es particularmente importante la información recogida por todas las fuerzas. Las distintas disciplinas pueden aportar la información o inteligencia para colaborar en la lucha de la siguiente forma:

– HUMINT. La explotación de fuentes humanas permite identificar los elementos, las intenciones, la composición, las tácticas, equipo, personal

(18) Es lo que en el AJP-2.0: *Joint Intelligence, Counter-Intelligence and Security Doctrine* se denomina *Counter-Intelligence Estimate.*
(19) Capacidades ISTAR *(Intelligence, Surveillane, Targe, Acquisition and Reonnaissance).*

y capacidades para perpetrar un ataque IED. Además puede proporcionar información de la inminencia del mismo. Cobra, pues, especial importancia en los niveles operacional y táctico.

– IMINT. Los resultados de la explotación de imágenes (fotografías, infrarrojos, láser, sensores y radares) pueden satisfacer gran número de necesidades de inteligencia específicas para la lucha CIED, ya que, se pueden centrar en un determinado tipo de objetivo, tema, o actividad. Además, puede proporcionar apoyo a las patrullas para registrar los acontecimientos relacionados con IED,s. Es de destacar la descentralización de nuevos medios como UAV,s y otros materiales que permiten la adquisición y explotación al más bajo nivel.
– SIGINT. La obtención de información e inteligencia a través Inteligencia de Comunicaciones (COMINT) e Inteligencia Electrónica (ELINT) permite la elaboración de informes pueden permitir la determinación de indicios o indicadores de una actividad del sistema o un ataque. Puede determinar planes hostiles, intenciones y posibles objetivos, así como, identificar el personal hostil y los vínculos entre esas personas dentro de la organización, relaciones entre nodos del sistema y proporcionar indicadores sobre el sentimiento popular y las reacciones a los ataques con IED,s. También puede identificar y proporcionar, al menos, en general lugares de emisores asociados a ataques con IED y el empleo que hace el enemigo del espectro electromagnético para la activación de RCIED,s.
– Unidades de la fuerza. La información de las unidades que reciben los ataques u observan indicios de los mismos debe integrarse en el proceso de obtención a través de informes normalizados para cada operación. En este sentido, será necesario establecer una arquitectura y procedimientos para un adecuado flujo de información. Además, toda relación con la población local puede aportar datos para identificar a los componentes del Sistema, con lo cual el personal que realiza actividades CIMIC, las Unidades de Ingenieros, etc., también deben ser contemplados en el proceso de obtención.

LA FASE DE ELABORACIÓN

Durante esta fase se actualiza la valoración de la amenaza, un producto importante para su neutralización porque el resto de medidas de seguridad emanan de ella. En las operaciones en las que la amenaza de ataques IED son numerosos y variados, cobra mayor importancia su constante revisión, ya que, para subsistir el Sistema IED procurará evolucionar a un ritmo superior.

Tanto las TTP,s, como la red de nodos y actividades del adversario cambian con rapidez, con lo que para poder realizar con eficacia las actividades P&P será fundamental la permanente actualización de los conocimientos adquiridos de los cambios que se produzcan en la red del adversario. En este sentido, es muy importante desarrollar un análisis inteligencia actual sobre los grupos insurgentes o terroristas con el fin de incluir las actividades, objetivos y estructura de apoyo relacionadas con los IED,s.

También es necesario realizar un análisis de tendencias con el fin de predecir futuras actividades del adversario. Ya que, el objetivo del adversario puede ser tanto táctico como político-estratégico; cualquier elemento de la fuerza, de la nación anfitriona o población local es susceptible de serlo, con lo que establecer donde existe una mayor probabilidad o peligrosidad es un paso crítico. Por lo tanto es necesario identificar los patrones asociados con el desarrollo y el empleo de la amenaza. E incluye la predicción de las futuras acciones del adversario y actividades relacionadas con el suministro y adquisición de los componentes necesarios; el uso de técnicas de análisis y elaboración de modelos de predicción, permitirá establecer los probables escenarios de ataque.

Además una evaluación de las vulnerabilidades críticas del Sistema IED del adversario proporcionará información tanto para las medidas de contrainteligencia encaminadas a la neutralización de la amenaza como para el proceso de *Targeting*.

Es decir, durante esta fase deben de elaborarse productos que establezcan la estructura de la red del adversario y como se inserta ésta en las estructuras sociales y administrativas de la zona, y que integren la amenaza IED en el espacio geográfico y humano donde se desarrollen las operaciones y en el que se refleje la predicción de futuros ataques.

LA DIFUSIÓN

La información e inteligencia específica CIED para las actividades de P&P se proporcionara a los elementos implicados en las mismas y a las fuerzas en la medida de sus necesidades a través de informes verbales, escritos y del establecimiento de niveles de alerta. En este sentido la difusión de los productos de inteligencia debe estar perfectamente orientada para: evitar retrasos y que la información pierda su valor para el ciclo de *Targeting*, actualizar las medidas de protección de la fuerza, mo-

dificar las TTP,s propias e incorporarlas a los programas de instrucción y adiestramiento de la fuerza en todos sus niveles. Todo ello, identificando cuales son las necesidades de cada escalón de mando.

La neutralización de la amenaza IED, dentro del proceso general de CI&S, para las actividades de P&P irá orientada principalmente a establecer las medidas de contrainteligencia para actuar contra la amenaza que supone en sí mismo el grupo insurgente o terrorista y sus capacidades de obtención y análisis de información de las fuerzas propias y sus actividades.

Gran parte de la difusión de información e inteligencia y la adopción de medidas de contrainteligencia alimentará el «ciclo *Targeting*» con la *finalidad de prevenir* el ataque IED por la destrucción, eliminación o neutralización de los nodos y sus conexiones.

Además la inteligencia necesaria para las INFOOPS juega un papel fundamental en la prevención. Por ejemplo, la explotación de las vulnerabilidades de la red IED en cualquiera de sus nodos, con una adecuada operación de información, puede disuadir a sus componentes de la participación en el ataque en cualquiera de sus fases.

La explotación de Inteligencia Técnica (TECHINT)

La TECHINT trata de los desarrollos tecnológicos, sus capacidades y futuras aplicaciones. Si comparamos el Sistema IED con un sistema de armas convencional se necesitará inteligencia que proporcione los elementos de juicio para elaborar TTP,s, establecer medidas de protección, y apoyar las operaciones para luchar eficazmente contra el enemigo que la posea. En la actualidad el incremento de la utilización de tecnología en la confección de IED,s hace necesario un análisis sistemático de sus componentes, construcción, producción, efectos y vulnerabilidades. En consecuencia, hoy en día la TECHINT es vital para el conocimiento de las capacidades de los grupos que utilizan los IED,s.

Es decir, la TECHINT posibilita la detección y neutralización de los artefactos, y además permite la predicción y la prevención, ya que, conociendo el proceso de fabricación y las características de los componentes de los IED,s es posible apreciar su desarrollo y despliegue, su funcionalidad e identificar sus vulnerabilidades, para finalmente derrotar el Sistema.

Por lo tanto, la actividad de explotación de la información debe proporcionar a los analistas de TECHINT toda la información disponible, para que se pueda elaborar la inteligencia específica que aporte los conocimientos necesarios para el resto del ciclo de contrainteligencia y así, facilitar un conocimiento más profundo del sistema que será utilizado para desarrollar la actividades de P&P con mayor eficacia.

Conclusiones

El uso de IED,s no es nuevo, lo que ha cambiado es la tecnología empleada y la repercusión que sus efectos tienen, convenientemente explotados por el adversario, sobre la sociedad. Y cómo, en consecuencia, pueden influir en las decisiones al más alto nivel, incluido el nivel político. Esto es algo que el adversario sabe, y la razón del amplio uso de los IED,s para alcanzar sus objetivos. Para ello organiza un *sistema* complejo que le permite llevar a cabo los ataques y explotar sus efectos.

La lucha CIED debe continuar los esfuerzos para *la lucha contra el artefacto* y proporcionar la *instrucción* y el *adiestramiento* adecuados para la protección de las fuerzas. Ahora bien, esto no evitará que el adversario continúe ejecutando ataques con IED,s, por lo tanto, deben mejorarse las capacidades para *la lucha contra el Sistema*. En ese sentido, la predicción y prevención es lo más eficaz, identificando y actuando contra todos y cada uno de sus nodos del sistema que establece el adversario para lograr sus objetivos.

La inteligencia juega un papel fundamental en la *predicción*. *Contrainteligencia y seguridad* realizan actividades que influyen directamente en la *prevención*. Determinadas actividades del Sistema IED pueden ser neutralizadas por medidas de contrainteligencia, siempre convenientemente coordinadas con el área de operaciones y con cualesquiera otras que sean necesarias para mantener el enfoque integral y multidisciplinar de la lucha CIED.

En este proceso juega un papel fundamental la explotación de información e *inteligencia técnica específica* que aporte los datos necesarios sobre las capacidades del adversario, ya que la evolución de la tecnología que utilizan para la fabricación de los artefactos es constante.

Es necesario establecer una *arquitectura CIED* adecuada y plenamente integrada en la estructura operativa, para que se establezca un *flujo de*

información que responda a las necesidades del ciclo de inteligencia y de contrainteligencia, debido a lo crítico de *factor tiempo* en la lucha CIED.

Y, por último, la necesidad de situar una *célula CIED* dentro del área de inteligencia, toda vez que las actividades de análisis de la información obtenida de la actividad de explotación se apoyan normalmente en órganos de análisis técnico de alto nivel que requieren periodos de tiempo superiores. Dicha célula CIED debería contar con personal especializado que asegure el flujo de inteligencia específica, su análisis, así como su integración en el proceso general de inteligencia.

Bibliografía

AJP-2: *Allied Joint Intelligence, Counter Intelligence and Security Doctrine.*

AJP-2.1: *Intelligence Procedures.*

AJP-2.2: *Counterintelligence and Security Procedures.*

AJP- 3(A): *Allied Doctrine for Joint Operations.*

AJP-3.15: *Allied Joint Doctrine for Countering Improvised Explosive Device*.

Joint Operational Guideline for Counter Improvised Explosive Devices Activities.

Organizing for Improvised Explosive Device Defeat at the Operational Level, US Joint Forces Command and Joint Warfighting Center Handbook.

JDN-5/06: *UK Joint Doctrine Note for Countering Improvised Explosive Devices.*

DO2-010: *Doctrina Inteligencia*.

OR5-009: *Orientaciones. Procedimientos de inteligencia, contrainteligencia y seguridad*.

«Apuntes sobre contrainteligencia y seguridad en operaciones», Escuela de Guerra del Ejército.

Concepto cojunto CIED (sexto borrador).