



Lesson 1.6 Improvised Explosive Devices (IED) Fundamentals

Content

- IED Basics
- IED Threat System
- Force Protection Considerations
- Counter-Explosive Ordnance (EO) Strategy

Learning Outcomes

- Understand the fundamentals of an IED device
- Explain the three components of an IED threat system
- Explain how to assess and analyse IED threats
- Describe the three pillars of Counter-Explosive Ordnance (EO) Strategy *

*also know as, Counter IED in many TCC/PCCs doctrine

IED Basics

IED Definition



- Placed or fabricated
- Improvised manner
- Destructive, lethal, noxious, pyrotechnic or incendiary chemicals
- To destroy, incapacitate, harass or distract
- May incorporate military stores, remnants of conflict
- Often devised from non-military components

Only challenge for IED manufactures is imagination



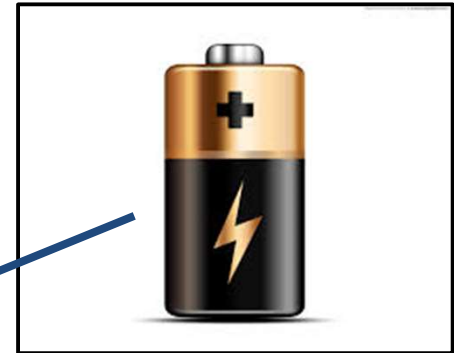
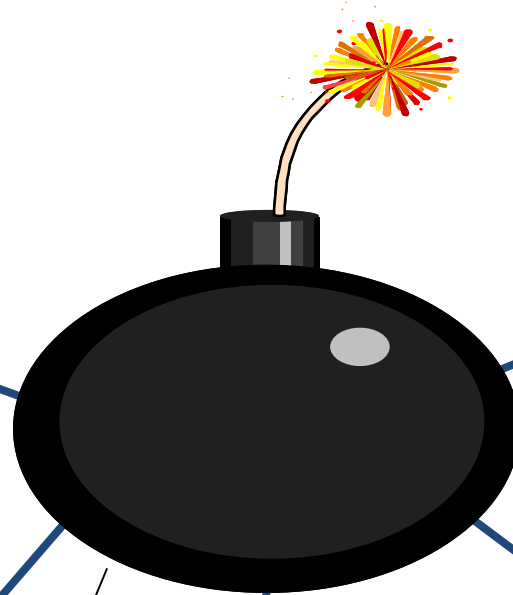
IED Characteristics

- An evolutionary threat
- Ingenuity in manufacturing and deployment
- Easy access to building methods (online)
- Low tech
- Methods vary regionally

Components of an IED



Container



Power Source



Explosives



Switch



Initiator

Enhancements

Component - Explosives

Military

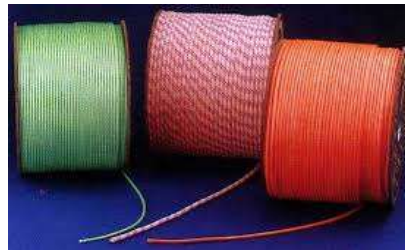
- Mortars
- Projectiles
- Landmines
- Bulk C4/SEMTEX

Commercial

- Detonating cord
- Commercial dynamite / TNT
- Ammonium nitrate

Home-made

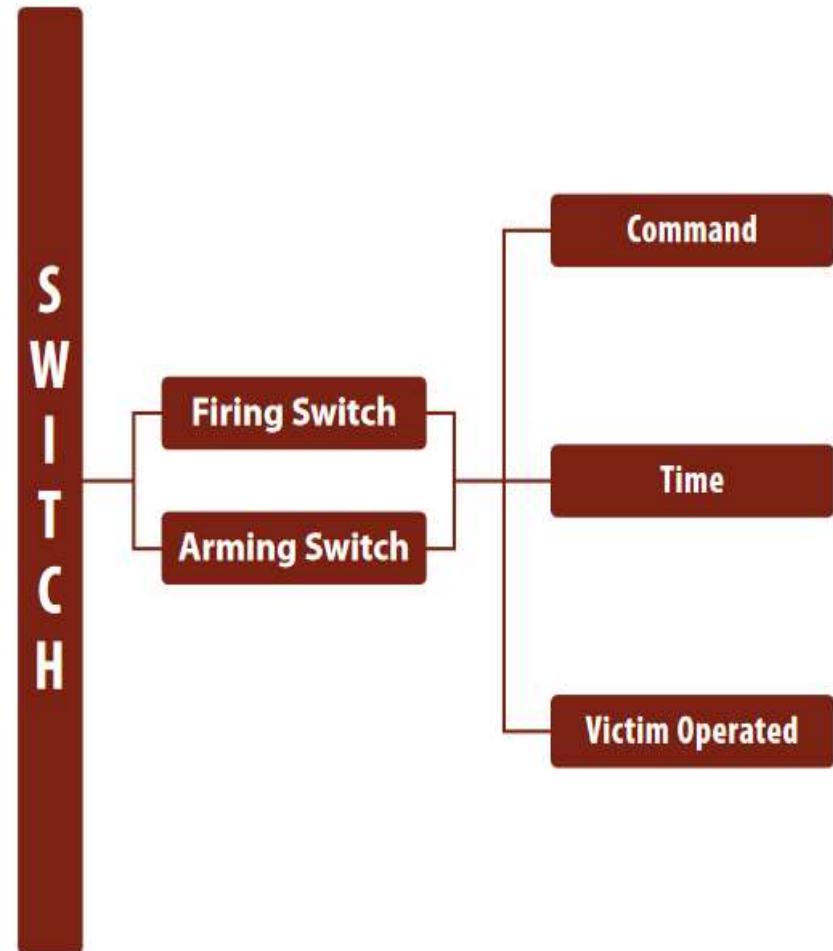
- Ammonium based
- Peroxide based
- Chlorate based
- Other chemicals



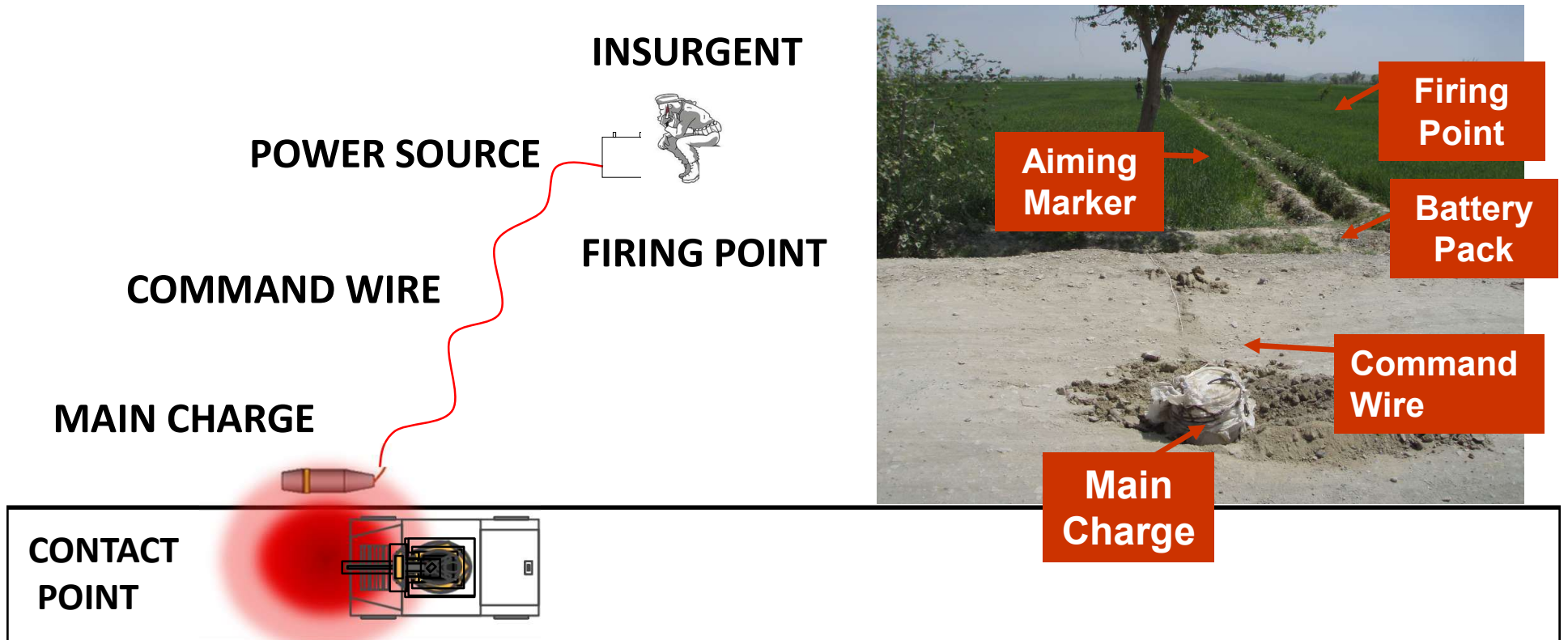


Component - Switch

- Device for making, breaking, or changing a connection in an IED. A switch can have multiple functions (i.e., firing and arming)
- ✓ **Firing switch-** initiates explosion train
- ✓ **Arming switch-** prevents an IED from arming until ready and allows functioning

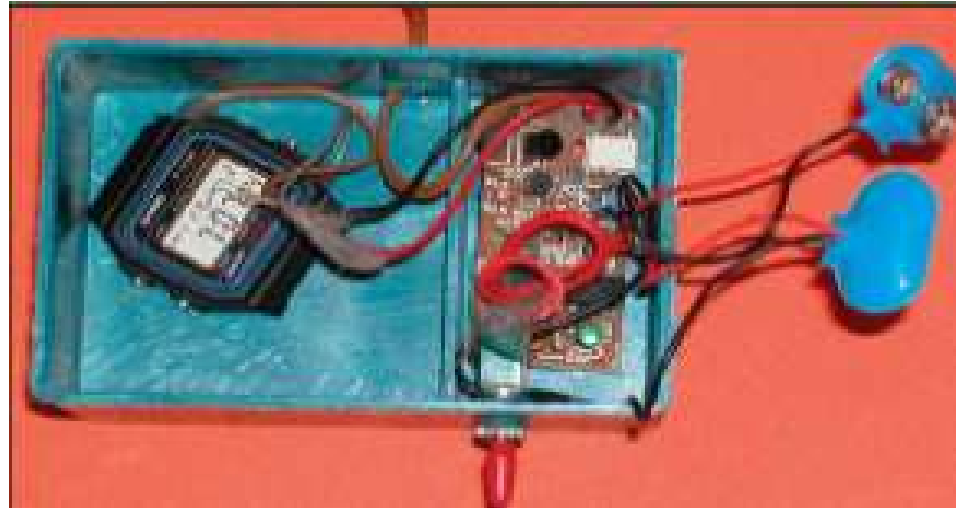


Switch - Command



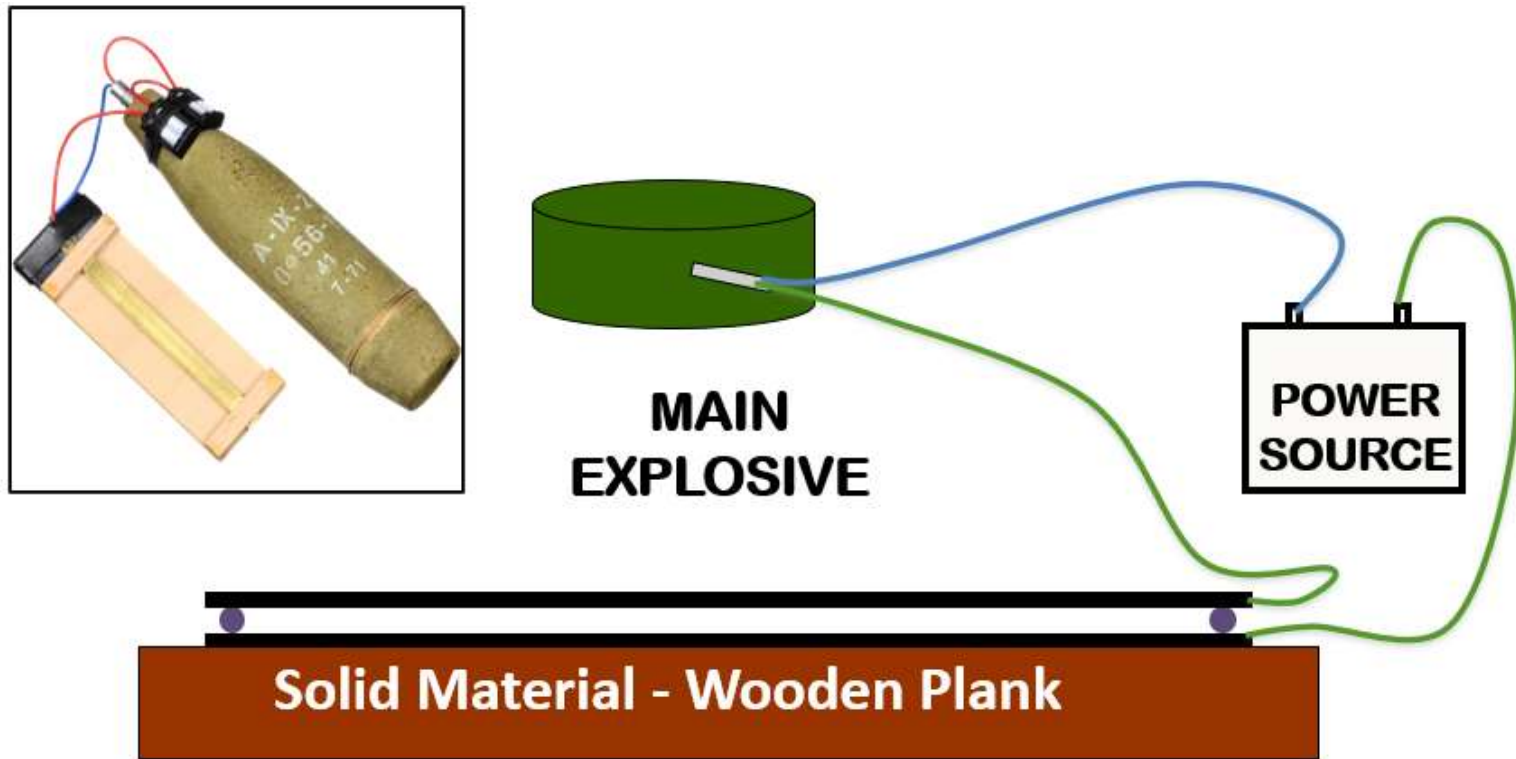
- Aggressor retains control
- Optimum effect on intended target
- Types include wire, pull, and radio-controlled

Switch - Time



- **Functions after a set time**
- **Widely used against infrastructure targets**
- **Types include mechanical, chemical, and digital**

Switch - Victim Operated



- Activated by unsuspecting individual
- Types include pressure, pressure-release, sensor, tension, tension-release, collapsing circuit, membrane switch

Other Components



Power Source: A device that stores or releases electrical or mechanical energy to the electrical initiator



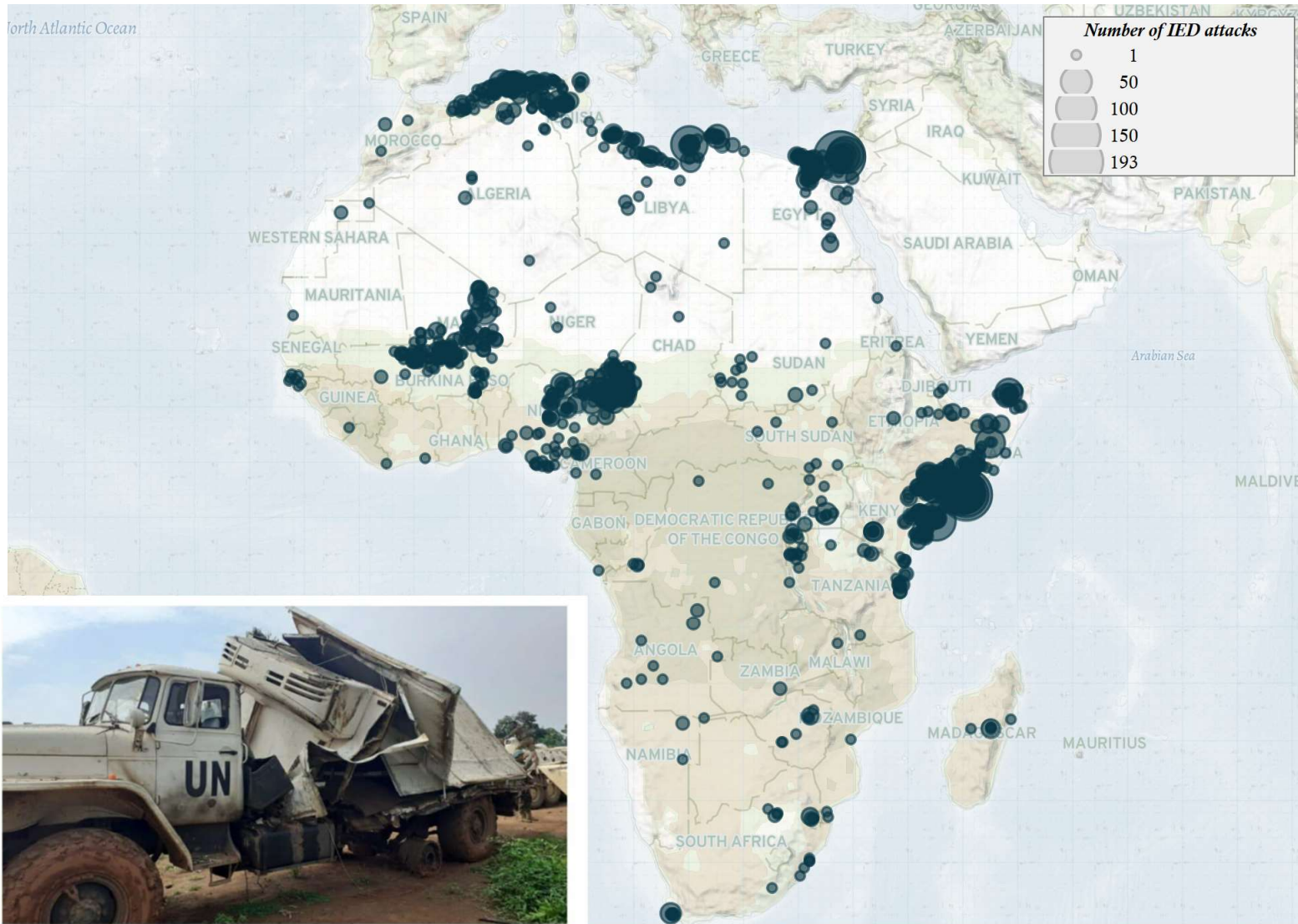
Initiator: Component used to start a detonation or deflagration



Container: Item with a void into which components of an IED are placed. To contain components of an IED or act to **conceal** the components and / or **confine** the explosive material which can produce directional effects

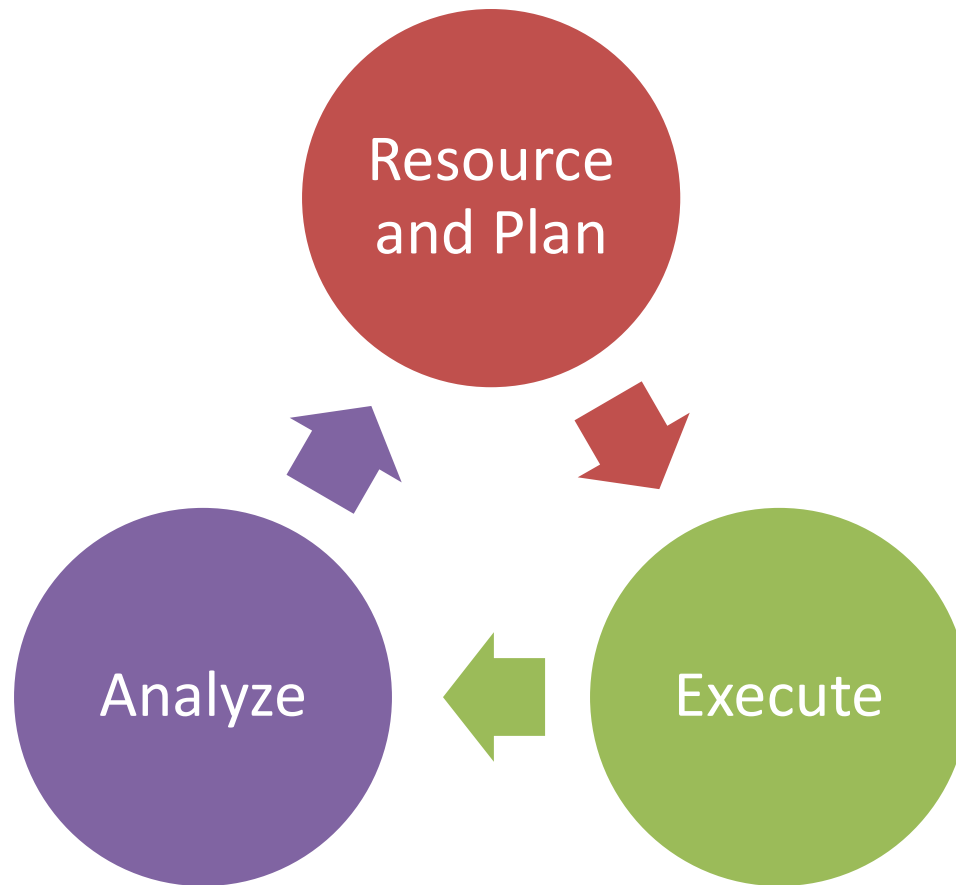
IED Threat System

IED Attacks Since 1997

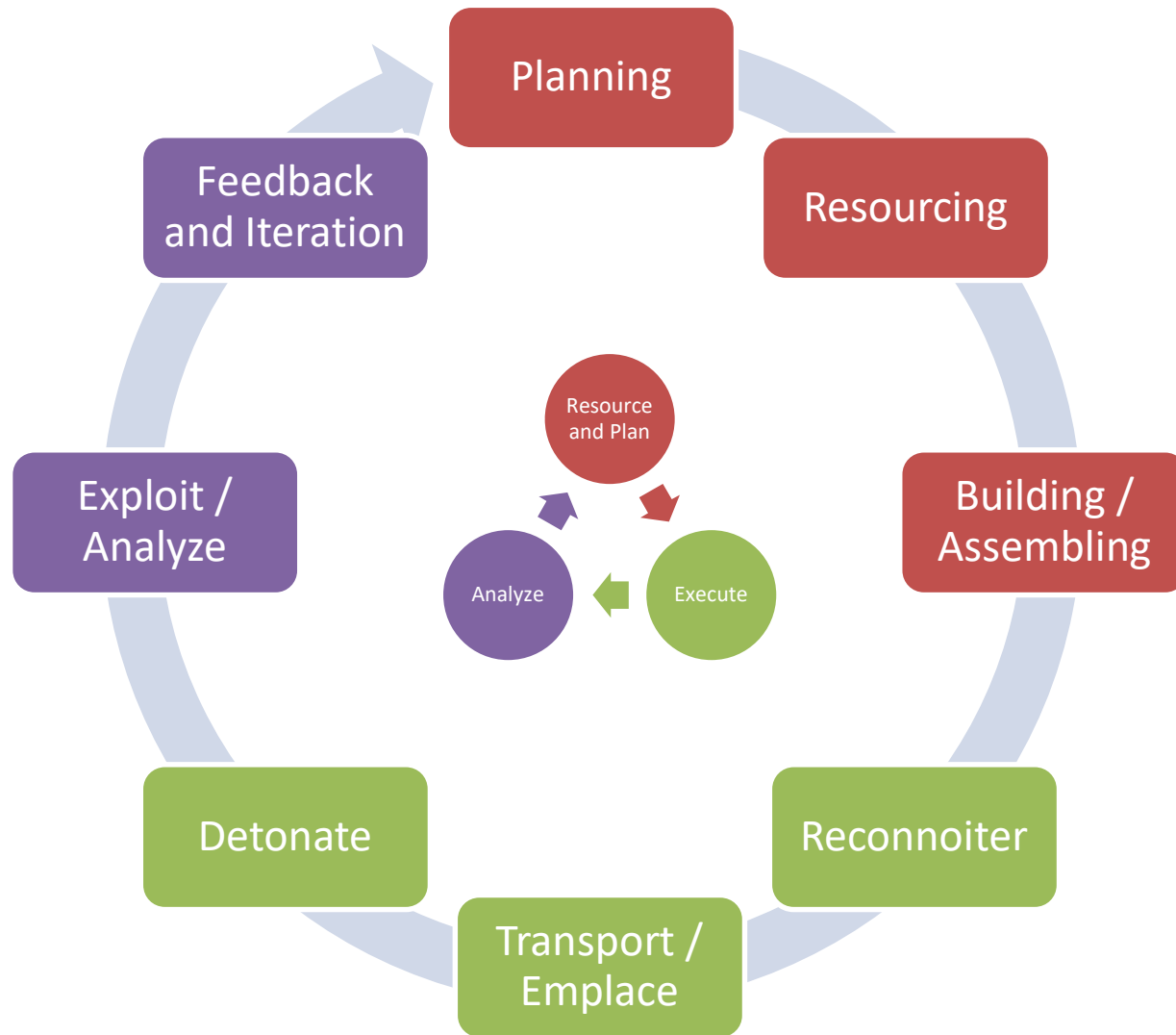


IED Threat System

A basic model of actions necessary to plan, make, emplace, detonate, access IEDs

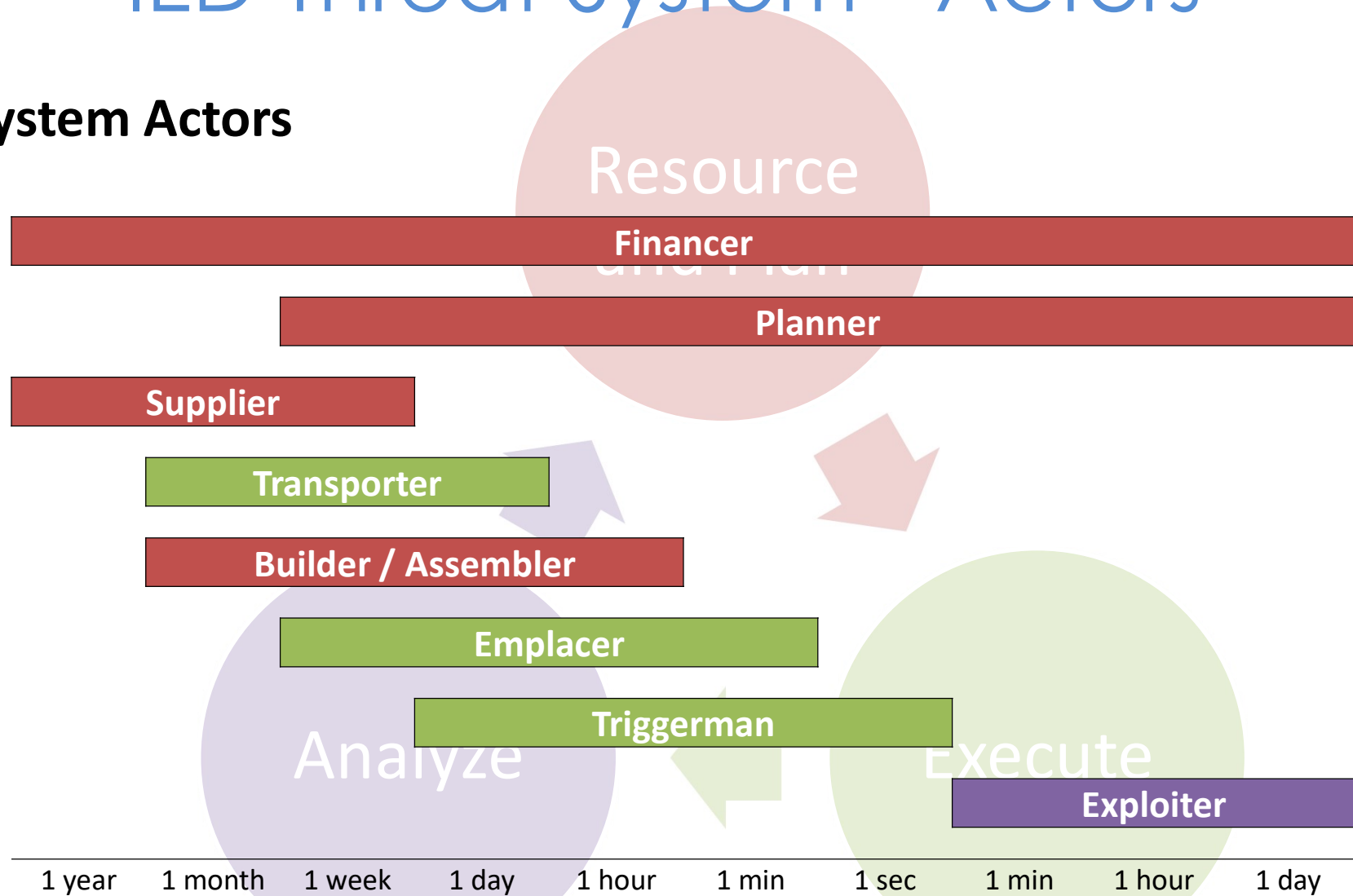


IED Threat – Resource & Plan



IED Threat System - Actors

System Actors



IED Threat – Resource & Plan

Planning

- How to use it to help cause
- Formal planning with leaders (IED effort)
- Informal planning by local groups (specific IED event)



IED Threat – Resource & Plan

Group / Attackers Planning

Advantages and disadvantages of using an IED

Planning Considerations

- Strategic, regional, local leadership coordination
- IED strategies and objectives
- Effects on attacker group status/control
- Public opinion

Planning Decisions

Funding
Resourcing
Expertise
Building
Reconnaissance
Target selection

IED Threat – Resource & Plan

Resourcing

- Finance
- Technical support
- Recruitment
- Training
- Material collection
- Manufacturing



IED Threat – Resource & Plan

Attackers /Group Resourcing

What is needed and how do they get it?

IED Components

- Vehicles, drivers, emplacers
- Recon / surveillance expertise
- Experts: building, assembling, training, recruiting, transporting
- Intelligence, safe houses, storage for materials

Means to Obtain

- Funding (legal or illegal)
- Stealing, gathering
- Soliciting or coercing police, military, government, other groups

IED Threat – Resource & Plan

Building & Assembling

- Builders/“bomb-makers”
- Skilled in electronics and chemistry
- Assembly requires less skill than building



IED Threat – Resource & Plan

Build and Assemble

How are the devices made?

IED Building

- Alter military ordnance
- Alter commercial explosives
- Make home-made explosives
- Create/alter detonators
- Fabricate switches / circuitry
- Sew the vests
- Train bomb assemblers

IED Assembly

- Explosives, container, detonator, power supply
- Preposition IED and delivery system
(Example, suicide vest or vehicle)

IED Threat – Execute

Reconnoiter

- Decide on targets (target assessment)
- Decide on target of opportunity based on pre-determined indicators



IED Threat – Execute

Target Selection

What is the target and how will the IED attack it?

Targets

- Convoy movement patterns, timings, routes, composition
- Locations of installations- purpose, activities, key individuals, defense
- Response to attack or actions taken by responders

Attack Preparation

- complex attack coordination
- Transportation
- Actions prior to detonation
- Actions during a detonation
- Ingress and egress routes
- Actions if discovered or disrupted

IED Threat – Execute

Transport / Emplace

- IED moved directly for attack or pre-positioned
- IED emplaced without full assembly (e.g.: no battery until attack)
- IED armed before attack



IED Threat – Execute

Transport and Emplace

How are the IEDs and personnel put into position?

Moving to the Target

- IED components
- Assembled IED
- Communications
- Observer or video operator
- Triggerman (if needed)
- Bomber (if needed)

Emplace and Arming the IED

- Dig hole, run wire, aim device
- Obtain line or sight
- Cover / conceal device
- Position triggerman
- Position cameraman
- Finish assembly / arm IED

IED Threat – Execute

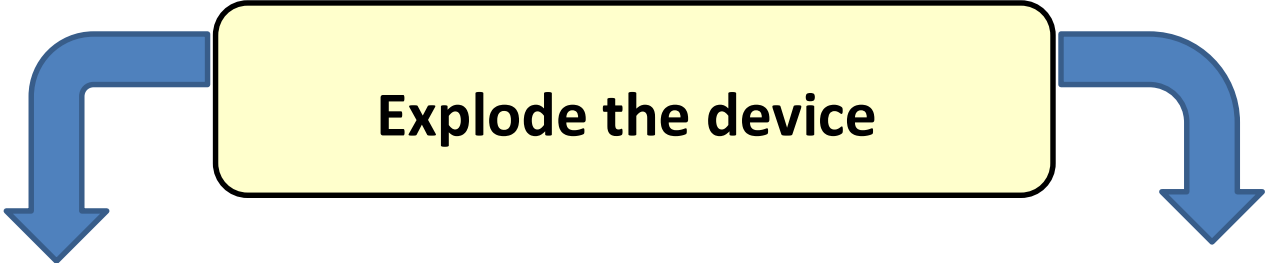
Detonate

- Detonation- single, multiple, or part of a complex attack
- Could include hoax devices to draw in first responders
- Failed detonations allow EOD to exploit



IED Threat – Execute

Detonate



Explode the device

Actions of the threat group

- **Single IED**
- **Multiple IEDs**
- **Hoax devices**
- **Explodes as designed**
- **Fails to explode**
- **IED group personnel /material captured, killed, flee**

Actions at the target area

- **Device exploitation**
- **Render safe IED**
- **First responders arrive**
- **Host nation military/police arrive**
- **Presence of local civilians and bystanders**

IED Threat – Analyze

Exploit & Analyze

- Attackers use of media to enhance narrative
- Videos of attacks spread via internet
- Enemy media gives UN units opportunity to gain intel



IED Threat – Execute

Exploit

Broadcast the attack to advertise narrative and attempt to leverage thoughts and actions

Recruit / Coerce

- Recruit allies / associates
- Enhance power of group
- Gain moral & local support
- Cause UN to change TTPs
- Force UN withdrawal or impact morale
- Weaken governance

How to use media?

- Professionals
- Amateurs
- Social media
- Print, video, audio, internet
- IED Information Operations (training, advertising)
- Adjust training / TTPs

Force Protection Considerations



FP Considerations

- FP Planning- COAs to reduce impact or likelihood
- Maintain vigilance / force readiness
- Intelligence - reconnaissance
- Response procedures
- Training



FP Considerations – Mission Analysis



Within the unit's current location; potential areas of transit; and the deployment in the tactical area of operations

- 1. Analysis of the Operational Environment (AOE)**
- 2. Actor Evaluation-** Identification of Key Actors- Potential IED Attackers / groups using IEDs, specifically: Planners (strategy), Suppliers, Transporters, Builders, Emplacers, Triggermen, Exploiters
- 3. Threat Analysis**
 - a) Overview-How Actors / Group Interact in the OEE
 - b) Key Elements
 - c) Threats identified current location, transit route areas, TAO assigned / potential
 - d) Matrix- Each threat determines 5 Ws
- 4. Risk Analysis**
 - a) Vulnerability assessment
 - b) Capability assessment – Assistance / Support
 - c) Danger level assessment
 - d) Risk analysis matrix

FP Considerations – Develop Information Acquisition Plan (IAP)

- A tool to capture ‘direction’ from leadership
- Assigns tasks to collection assets / units
- A living document updated as requirements change
- Many call it a Collection or Reconnaissance Plan

Key IED Actors

Transporter

Builder

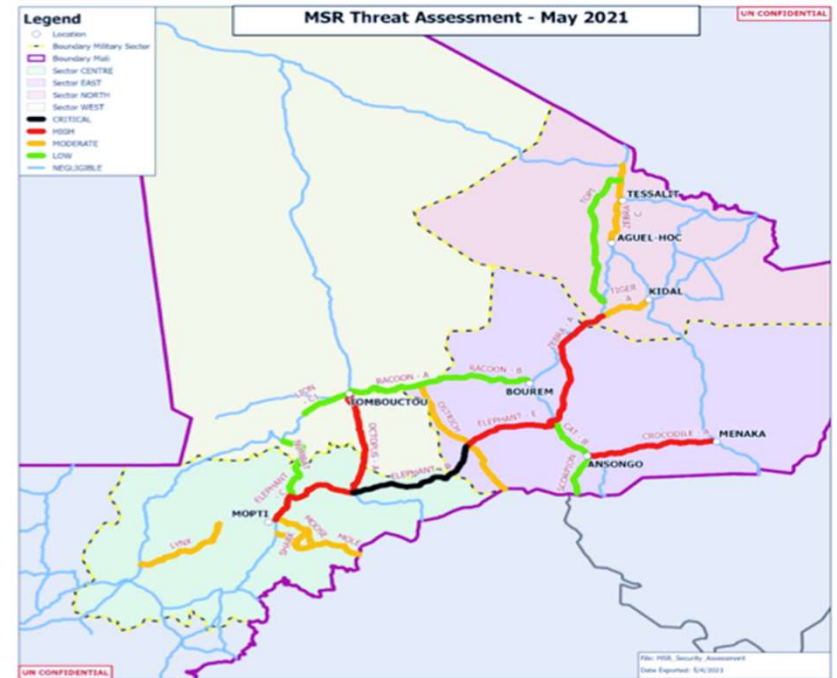
Emplacer

Triggerman

Exploiter

FP Considerations – Robust Routes Analyse

- IED attacks and incidents frequently occur along routes and roads
- Requires continues -Physical, Human, Information Terrain and threat analyses
- FP planning is key prior risk mitigation





FP Considerations – Share TTPs

STAY ALIVE!

1ST TIME

2ND TIME

3RD TIME

DON'T SET PATTERNS

Contact: 2362208X, F.unen, C.eli@unmaail.com

STAY ALIVE!

**WEAR YOUR HELMET
STRAP IN CORRECTLY
TIE DOWN LOOSE OBJECTS**

Contact: 2362208X, F.unen, C.eli@unmaail.com

STAY ALIVE!

1ST TIME

2ND TIME

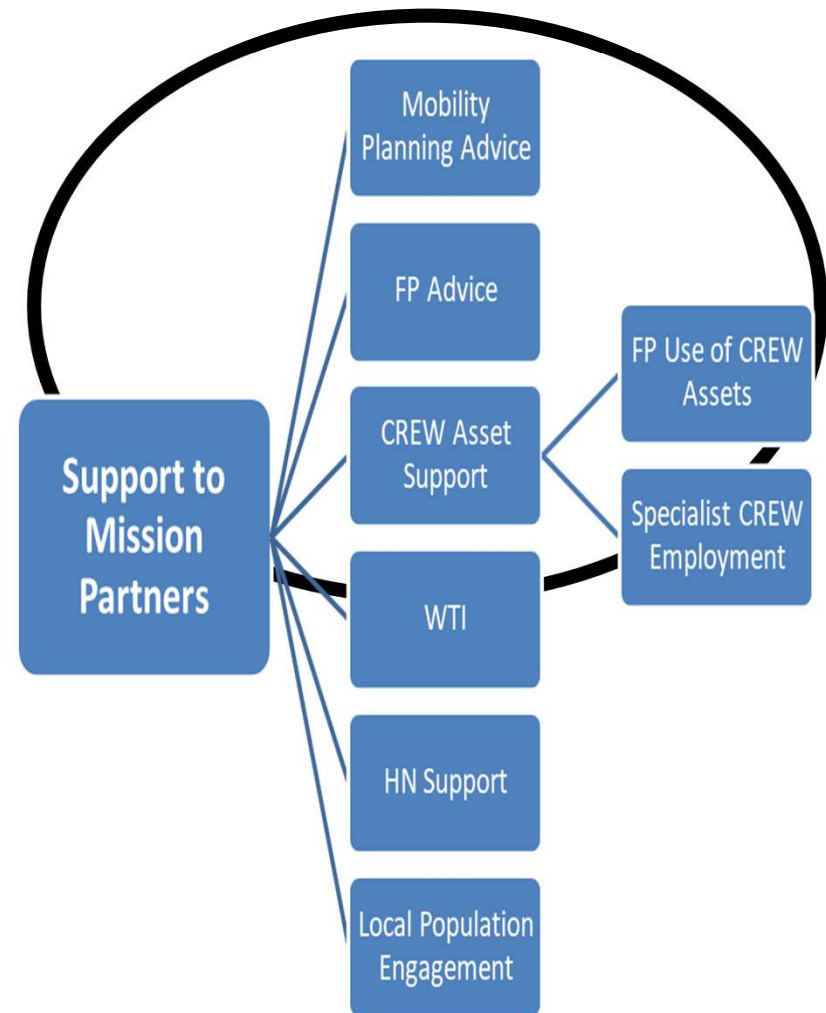
3RD TIME

DON'T SET PATTERNS

Contact: 2362208X, F.unen, C.eli@unmaail.com

FP Considerations – EOD

- Conventional munition disposal (CMD) and IED disposal (IEDD)
- Mobility
- FP advice
- Electronic warfare countering RCIED threats – CREW assets
- Technical /tactical analysis IED incidents

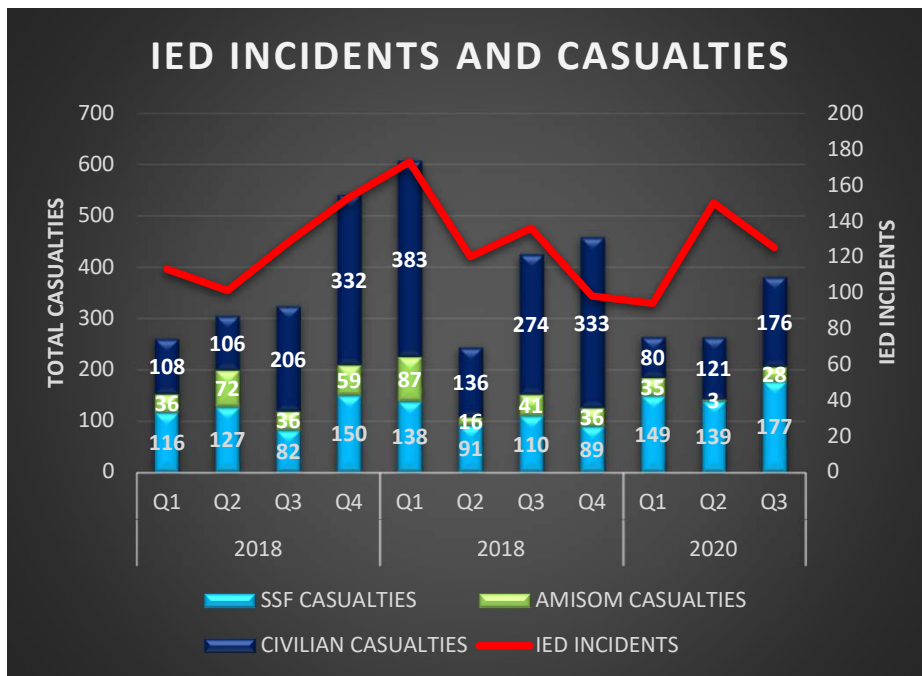


FP Considerations – Trend Analysis



Factors

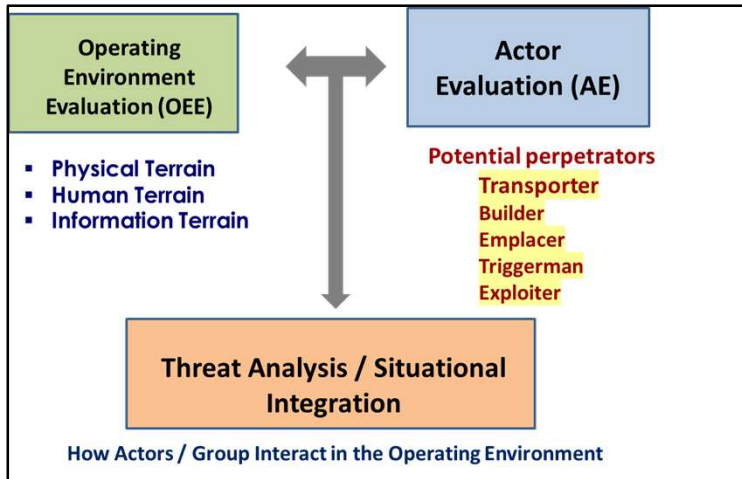
- Changes in IED incidents
- Security forces activities
- Resupply of IED components
- Rotation schedules
- Weather patterns
- Major operations





FP – Key Operational Activities

Predict

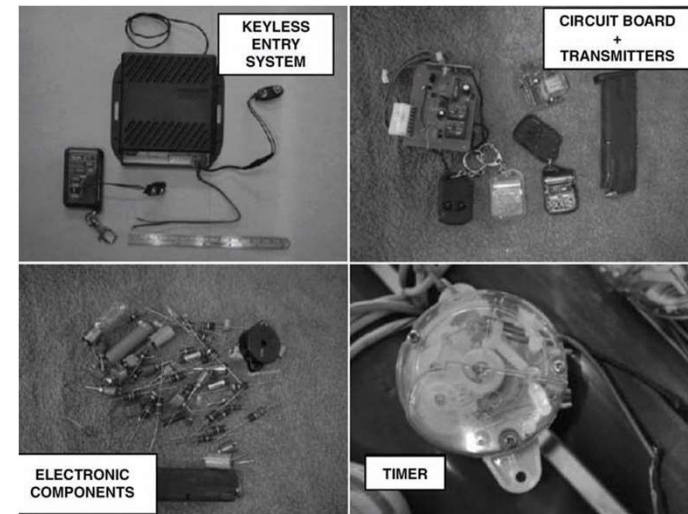


Detect



Exploit

Neutralize



Counter-Explosive Ordnance (EO) Strategy

Also Referred to by UN Military / Police unit as **Counter IED (C-IED)**

Counter-EO Strategy

3 pillars to Counter EO framework



Objectives

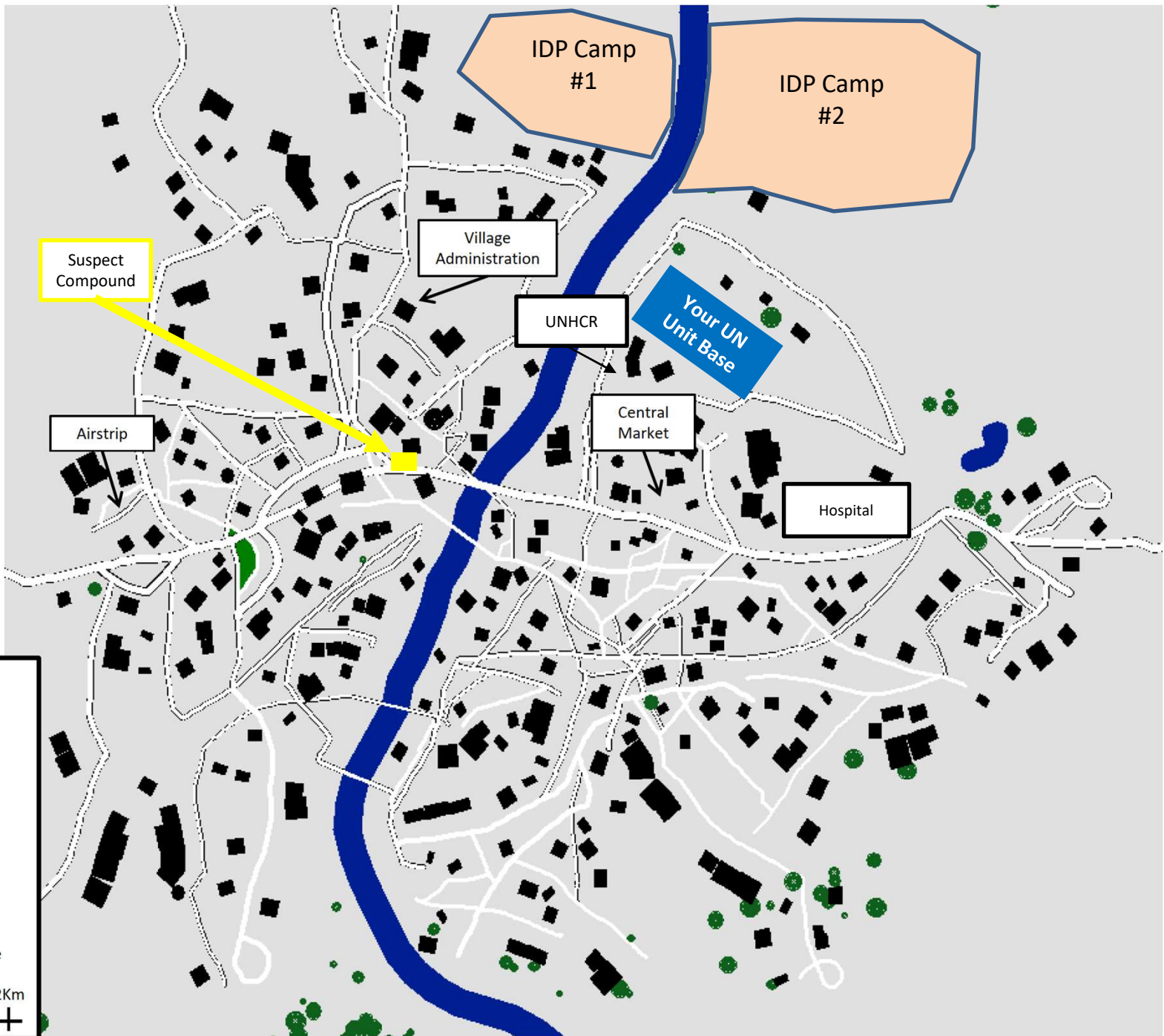
- Secure Environment
- IED threat risk mitigation
- Protection of Civilians
- Force Protection

Take Away

- IEDs are a significant threat to peacekeepers; the trend is increasing
- IEDs categorised by the switch- Victim Operated, Command Initiated, Time Initiated
- Military explosives and commercial products are used
- A threat-based approach, FP planning is key to IED risk mitigation
- The analysis of key actors throughout the life cycle of an IED is an important step in identifying the threat
- EOD helps with training, FP planning, electronic counter systems

Situation

Following an increase in IED attacks in your unit's tactical area of operations, you received information from locals that cars have been coming in and out late at night at a building within their town. Also, strong smells were around an open sewer system. You conducted FP planning and asked the National Police to assist and if possible, neutralise suspected bomb-making activity. One police officer was killed when a box was opened in the workbench. They arrested a bomb maker who gave them info about a location storing IED components and warned all to be careful. The police requested your unit for help in protecting the local population. Your HQs gave you permission to start FP and POC planning and receive EOD and UAS support. What planning should be considered, how best to integrate EOD, UAS and how might you start to develop threats and COAs to mitigate risks to your unit and population?

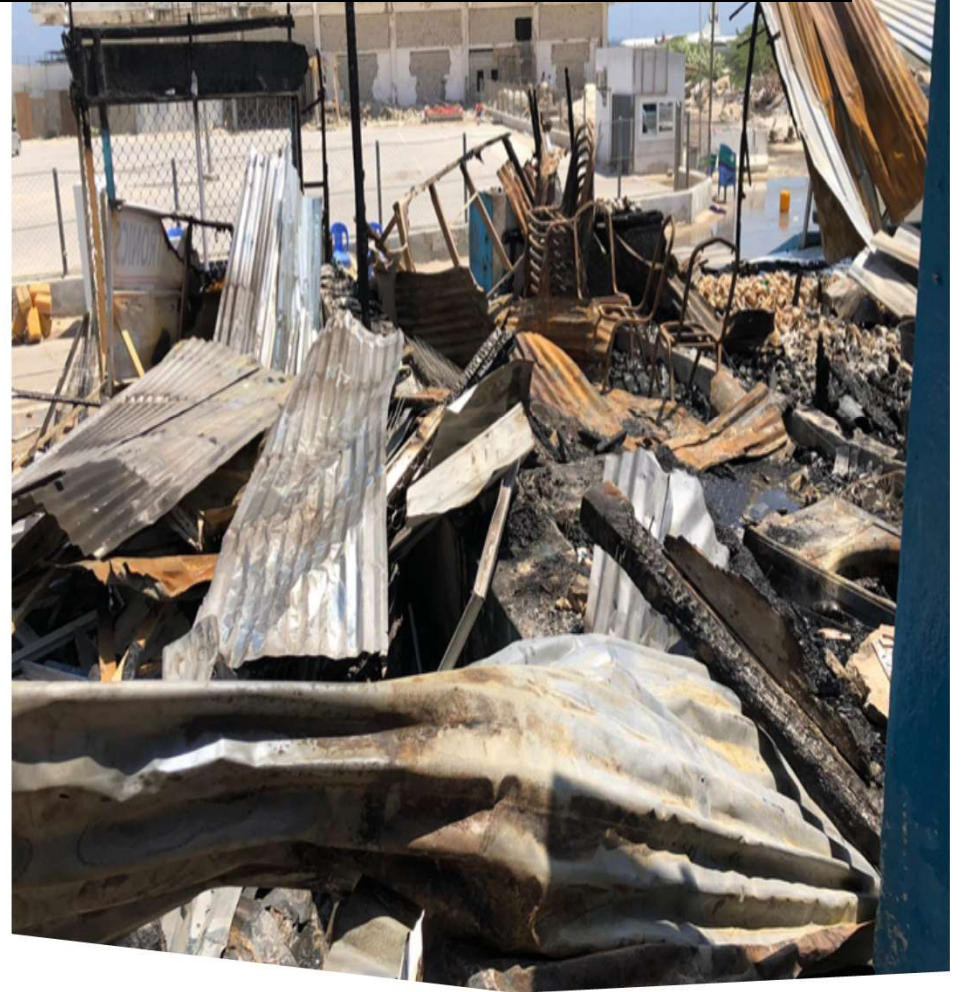


Folsa
Population: 10,000
Elevation: 110 m

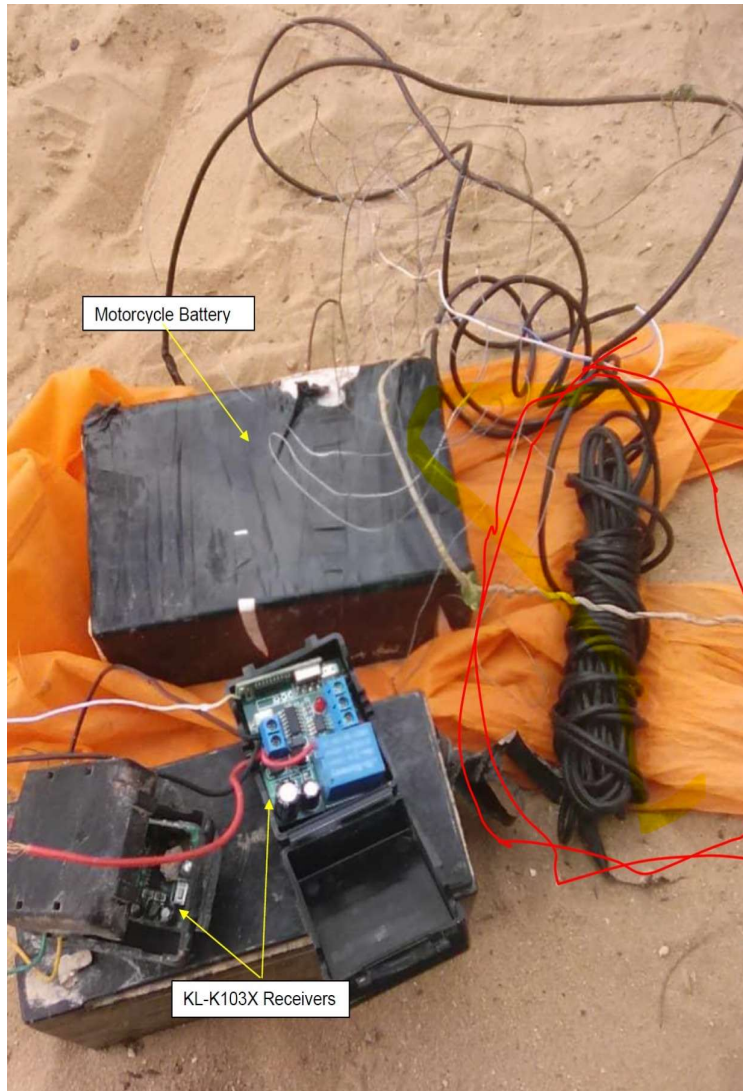
- Buildings
- Unpaved Road
- Track
- River
- UN Operating Base

0 1Km 2Km

where the policeman was killed



Components from the scene



**Recent
UAS Image**



The Compound Measure 50 m by 75 m in a triangular shape and has one entrance from the eastern edge. The compound contains at least 4 buildings. Surveillance was conducted over 40 hours and there was no movement detected into or within the compound for the duration. UAS Asset was then re-tasked by FHQ.

Questions