TABLE OF CONTENTS

CHAPTER 1 INTERNATIONAL HUMANITARIAN LAW

1-1 Introduction

International humanitarian law also known as the **LAW OF WAR (LOW)** is a set of rules seeking to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities. The **LOW** includes the ***Protection of Civilians by ...***

1. Reducing Risks from Physical Violence.
2. Securing Rights to Access Essential Service & Resources.
3. Contributing to a Secure, Stable, & Just Environment.

1961

Federal Republic of Nigeria ratified the Geneva Conventions of 1949 (I - IV).

1988

Federal Republic of Nigeria ratified the Additional Protocols of 1977 (I & II).

Figure 1.1 Protecting Civilians From Conflict

▲ *According to the law of war, civilians may not be the object of attacks and must be spared and protected.*

1-2 Law of War - 5 - Foundational Principles

1. **Military Necessity** is a principle justifying the use of all measures needed to defeat the enemy quickly & efficiently that are not prohibited by the **Law of War.** *Military necessity* justifies destroying and seizing persons & property, capturing enemy persons, non-forcible measures (e.g. propaganda & intelligence-gathering); also certain inevitable incidental harms.

▲ *Military Necessity Does Not Justify Actions Prohibited by the Law of War.*

2. **Humanity** is a principle forbidding the unnecessary infliction of suffering, injury, or destruction when accomplishing a legitimate military purpose. *Military necessity* cannot justify actions not necessary to achieve this purpose (e.g. cruelty or wanton violence). Once a military purpose has been achieved, inflicting more suffering is unnecessary.

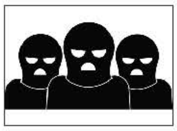
3. **Proportionality** is a principle limiting unreasonable or excessive actions when accomplishing a legitimate military purpose. This principle weighs and determines if expected collateral damage to civilians & civilian objects is acceptable when executing a legitimate & justified military action. In war, incidental damage to the civilians and civilian objects is unfortunate and tragic, but inevitable.

4. **Distinction** is a principle obligating all parties to a conflict to distinguish between the armed forces & the civilian population, and between unprotected & protected objects. All Parties must establish a framework of legal classes for persons and objects in the conflict zone. Parties must distinguish their own persons & objects from civilian (noncombatant) persons & objects to minimize incidental harm.

5. **Honor** obligates belligerents during armed conflict to enforce & implement the **Law of War** in good faith. *Honor* requires a certain amount of fairness in offense & defense while forbidding means, expedients, or conduct that would constitute a breach of trust with the enemy. Opposing military forces must honor the humane treatment of prisoners of war (POW) requiring POWs & Captors treat one another with respect.

1-3 Law of War - 10 - BASIC RULES

1 Fight Only Enemy Combatants



Enemy combatants are usually members of armed groups. Civilians participating in hostilities forfeit protection from attack. Enemy combatants do not need to be armed or awake! However, the **Law of War** requires that only enemy combatants are attacked. Don't attack civilians unless they are conducting acts physically hurting a soldier or unit.

2 Don't Harm Surrendered Combatants

- No cruel, inhuman, or degrading treatment.
- Provide adequate water, food, clothing, & shelter.
- Provide medical care.
- Keep the detention facility clean.
- Respect their person, honor, & beliefs.
- Respect an individual's religious affiliation.

3 Don't Kill or Torture Detainees

- Violating the **law of war** brings dishonor on individuals, units, services, and the country.
- Torture & illegal methods are poor techniques resulting in unreliable information.
- Incentives (e.g. luxury food items) are better ways to obtain reliable information.
- Trained interrogators conduct interrogations.

4 Collect-Care for Sick & Wounded

- As soon as feasible, search & collect wounded & sick.
- Treat humanely & give medical care.
- Collect, Protect, & Decently dispose of the deceased.
- Persons continuing hostile acts are NOT protected.

5 Don't Attack Protected Persons Places & Organizations

- Direct & intentional attacks against civilians, civilian objects & other protected places is prohibited.
- Proportionality Rule - Don't attack military targets if collateral damage & civilian casualties would be excessive in relation to anticipated direct military advantage.
- When attacking, apply practical precautions to avoid collateral civilian casualties & damage.

6 Destroy Only What Mission Requires

- Only damage, destroy, or take private property when strictly necessary for military operations.
- Combatants may use overwhelming force attacking enemy personnel - but must adhere to the *Proportionality Rule* limiting collateral damage & harm to civilians.

7 Don't Steal Private Property

Looting is a war crime. Do not steal from civilians, detainees, the wounded & sick, or the dead. It is dishonorable.

CHAPTER 2 INTELLIGENCE FUNDAMENTALS

2-1 Intelligence Disciplines

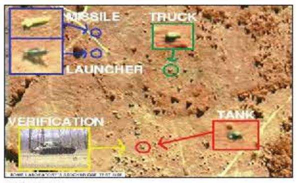
Geospatial Intelligence (GEOINT) is the analysis and visual representation of security-related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information. GEOINT encompasses all aspects of imagery. It includes information technically derived from the analysis of spectral, spatial, temporal, radiometric, phase history, and polarimetric data fused into an informative intelligence product. GEOINT can be collected on stationary and moving targets by electro-optical related sensor programs (active & passive) and non-technical means by personnel in the field.

GEOINT

Human intelligence (HUMINT) is a category of intelligence derived from information collected and provided by human sources. This discipline is primarily executed through human interaction by covert agents, spies, reconnaissance scouts, and tactical units. Typical HUMINT activities include conversations, interviews, and interrogations with persons suspected of having access to vital national security information.

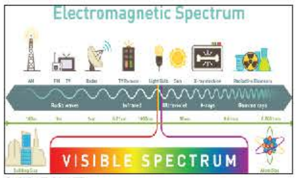
HUMINT

Imagery Intelligence (IMINT) is an intelligence-gathering discipline wherein imagery is analyzed (exploited) to identify information of intelligence value. Imagery used for defense intelligence purposes consists of satellite imagery or aerial photography. IMINT includes representations of objects reproduced electronically or by optical means on film, electronic displays, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. It is collected from satellites, aircraft, remote-piloted vehicles (RPVs), unmanned aerial vehicles (UAV) , unmanned aircraft systems (UAS), and ground-based photography.



IMINT

Measurement and Signature Intelligence (MASINT) is an intelligence discipline focused on capturing & measuring the intrinsic characteristics and components of an object or activity. These characteristics allow the object or activity to be detected, identified, or characterized each time it is encountered.



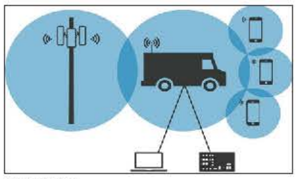
MASINT

Open-Source Intelligence (OSINT) is the collection & analysis of data gathered from accessing publicly available information contributing to the production of actionable intelligence. This discipline often includes internet & social media sites, traditional news broadcasts & newspapers, professional journals & academic papers, public government information, and commercial data.

Search
images

OSINT

Signals Intelligence (SIGINT) is intelligence-gathering by interception of signals including communications between people (COMINT) or from electronic signals not directly used in communication (ELINT).



SIGINT

2-3 Imagery Intelligence (IMINT)

IMINT involves evaluating, manipulating, and analyzing of one or more images to extract information related to an information requirement. Exploited information and subsequent results are normally disseminated via a report. The phases of exploitation include one time-dominant and two non-time-dominant phases.

First-Phase (Time-Dominant). The exploitation of newly acquired imagery within a specified time from receipt of imagery. The purpose of time-dominant exploitation is to satisfy priority requirements of immediate need and/or to identify changes or activities of immediate significance. Time-dominant exploitation and reporting are accomplished as soon as possible according to validated intelligence requirements, but not later than 24 hours after receipt of imagery.

Second-Phase (Non-Time-Dominant) The detailed non-time-dominant exploitation of imagery scheduled within the bounds of analytic requirements and timelines of need (typically within one week after receipt of imagery). Second-phase exploitation provides an organized and comprehensive account of the intelligence derived from validated intelligence requirements tasking.

Third-Phase (Non-Time-Dominant) In-depth, long-range analysis that includes all available sources of imagery. This phase includes detailed & authoritative reports on specified installations, objects, & activities. Third-phase exploitation timelines are not bounded and typically exceed one week after receipt of imagery. This phase incorporates supporting information from other intelligence disciplines and typically results in finished Geospatial Intelligence.

Electro-Optical (EO) photographic stills captured with an EO sensor, specifically a high-resolution camera equipped with a telephoto zoom lens. This form of imagery detects the magnitude and color of emitted or reflected light. It uses the visual spectrum, so anything that impacts this spectrum, such as dust, smoke, haze, clouds, rain, fog, light level, or angle of illumination, will affect the quality of the image.

Infrared (IR) Imagery is the remote sensing of the radiant temperature associated with a target by measuring the temperature differences between terrain features and surrounding objects on the ground, producing a near-optical-quality infrared image. IR sensors can operate day or night under favorable weather conditions; less effective during day/night transition periods or when backgrounds and targets have negligible differences in temperature.

EO Sensor

Advantages

- Familiar view of the environment.
- Superior resolution to thermal systems.
- Detailed analysis & mensuration.
- Stereoscopic viewing.

Disadvantages

- Restricted by terrain & vegetation.
- Day use only.
- Reduced picture size.

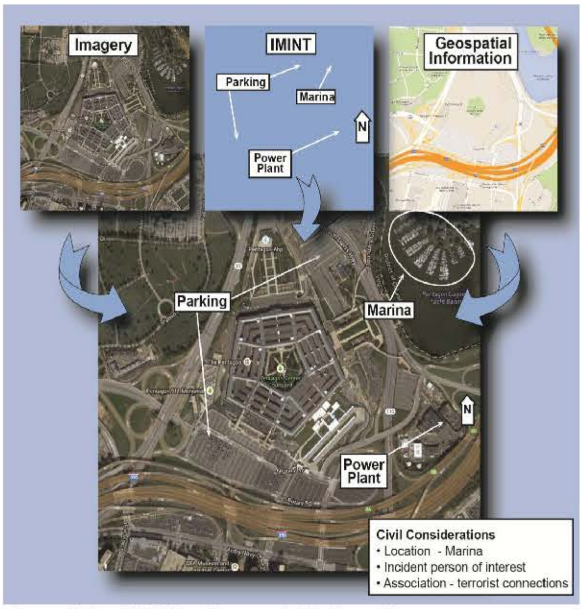
IR Sensor

Advantages

- Passive sensor - impossible to jam.
- Camouflage penetration.
- Good resolution.
- Night viewing

Disadvantages

- Efficacy during thermal crossover.
- Interpretability.
- Requires skilled analyst.
- No cloud penetration.



Civil Considerations
- Location - Marina
- Incident person of interest
- Association - terrorist connections

Figure 2.2 IMINT + Geospatial Information

2-4 Basic Elements of Aerial Photo Interpretation

Aerial or traditional orthogonal (straight down) imagery is different from ground-based photos.

Most people view objects from the ground. Aerial photos are taken at scales most people are not used to viewing.

» **Tone** (Color or Hue) refers to the spectral reflectance characteristics of objects, such as brightness or color.

» **Size** measures the surface dimensions of objects, including height, length-width, slope Scale determines if an object is a small pond or a large lake.

» **Shape** describes the form or configuration of an object. Refined geometric shapes are generally human-made, whereas natural shapes tend to have irregular shapes. Agricultural areas are often rectangular while natural streams are linear with irregular bends & curves.

» **Texture** is the frequency of tonal or color change which determines apparent roughness vs. smoothness of an image region depending on the angle of illumination & surface. Grass, cement, and water generally appear "smooth" while a forest canopy may appear "rough".

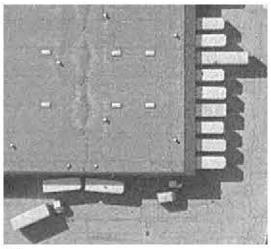
» **Pattern** is the spatial arrangement of individual objects into distinctive, recurring forms. The random pattern formed by a natural forest vs. evenly spaced rows of a tree orchard.

» **Shadows** may reveal details about size and shape not apparent from an orthogonal (overhead) view.

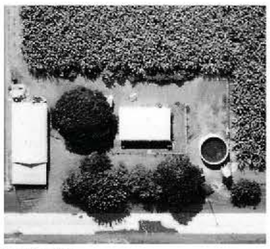
» **Site** refers to topographic or geographic location; identifying vegetation types & landforms.

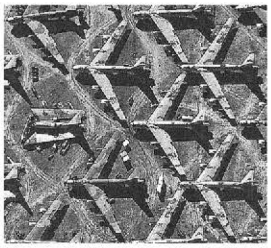
» **Association** aids in identifying objects based on routine proximity of certain distinct objects. Cooling towers identifying location of a power-plant.

Tone

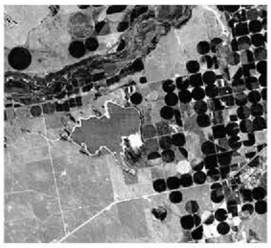

Size

Shape


Texture


Pattern

Shadows


Site

Association

The IPB Process results in intelligence products that used during the military decision-making process (MDMP) to assist in developing friendly COAs and decision points for the commander. Additionally, the conclusions reached and the products (which are included in the intelligence estimate) developed during IPB are critical to planning information collection and targeting operations.

IPB products include:

- Threat situation templates with associated COA statements and high-value target (HVT) lists.
- Event templates & associated event matrices.
- Modified combined obstacle overlays (MCOOs), terrain effects matrices, and terrain assessments.
- Weather effects work aids—weather forecast charts, weather effects matrices, light and illumination tables, and weather estimates.
- Civil considerations overlays and assessments.

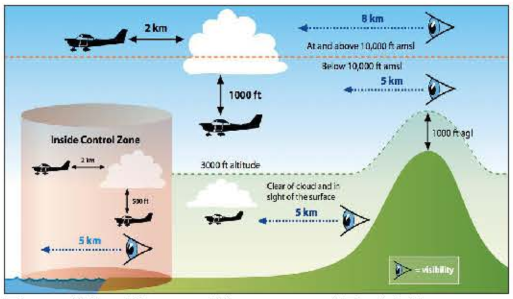


Figure 3.5 Airspace Management Restrictions

Air Domain

The air domain is the operating medium for fixed-wing and rotary-wing aircraft; air defense systems; and **UAS**. Air Avenues of Approach (AAs) are different from maritime and ground AAs. Analysis of the air domain is critical for identifying airspace restrictions and terrain restrictions within the land domain.

- View it as a medium for using capabilities. For example, how does or will the air domain affect the use of civilian & military aircraft, civilian & military UAS / drones, weather monitoring systems, air corridors, fly-over rights, and broadcasting rights.
- Think about relationships. For example, what is the air domain's relationship to the weather, the electromagnetic spectrum & communications, and its effects on performance (considering altitude, barometric pressure, and humidity).

Effective IPB Must

- A continuous process with all staff members providing input.
- Account for all domains, the information environment, & the electromagnetic spectrum.
- Define the commander's area of interest (AOI) by its geographic boundaries focusing collection & analysis within the AOI.
- Describe how the enemy, terrain & weather, and civil considerations will affect friendly & threat operations.
- Include relevant aspects of the OE for decisive, shaping, and sustaining operations.
- Support each step of the MDMP with IPB products.
- Determine how the interactions of friendly & threat forces and local populations affect each other. Create outcomes that positively affect friendly operations. This aspect of IPB is a collaborative effort by the Commander and the entire staff.
- Support the operational framework: physical, temporal, cognitive, & virtual.
- Facilitate the Commander's ability to visualize the desired end state & a broad concept of how to shape current conditions into that end state.
- Support the Commander in directing the intelligence effort.
- Facilitate understanding of threat characteristics and the threat's goals, objectives, & COAs.

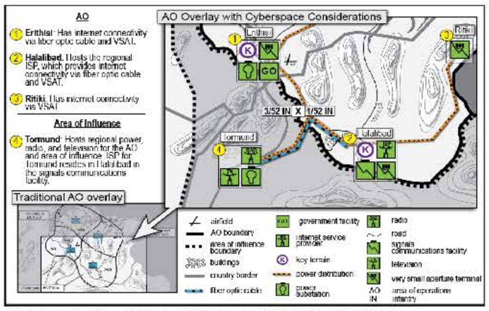

AO
1 Erthisi: Has internet connectivity via fiber optic cable and VSAT.
2 Halalibad: Hosts the regional ISP, which provides internet connectivity via fiber optic cable and VSAT.
3 Ritiki: Has internet connectivity via VSAT.
Area of Influence
4 Tormund: Hosts regional power, radio, and television for the AO and area of influence. ISP for Tormund resides in Halalibad in the signals communications facility.
AO Overlay with Cyberspace Considerations
Erthisi
Ritiki
GO
3/52 IN
X
1/52 IN
Tormund
Halalibad
Traditional AO overlay
airfield
AO boundary
area of influence boundary
buildings
country border
fiber optic cable
government facility
internet service provider
key terrain
power distribution
power substation
radio
road
signals communications facility
television
very small aperture terminal
AO area of operations
IN infantry

Figure 3.6 Area of Operations & Interest

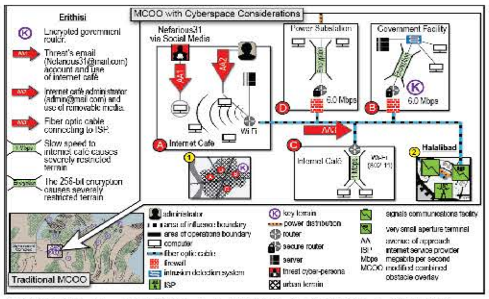

Erithisi
Encrypted government router.
AA1 Threat's email (Nefarious31@mail.com) account and use of internet café
AA2 Internet café administrator (admin@mail.com) and use of removable media.
AA3 Fiber optic cable connecting to ISP.
Slow speed to internet café causes severely restricted terrain
Encryption The 256-bit encryption causes severely restricted terrain
MCOO with Cyberspace Considerations
Nefarious31 via Social Media
AA1
AA2
Wi-Fi
A Internet Cafe
Power Substation
D
6.0 Mbps
Government Facility
B
6.0 Mbps
AA3
C
Internet Café
Wi-Fi (802.11)
1 Mbps
2 Halalibad
1
Traditional MCOO
administrator
area of influence boundary
area of operations boundary
computer
fiber optic cable
firewall
intrusion detection system
ISP
key terrain
power distribution
router
secure router
server
threat cyber-persona
urban terrain
signals communications facility
very small aperture terminal
AA avenue of approach
ISP internet service provider
Mbps megabits per second
MCOO modified combined obstacle overlay

Figure 3.7 MCOO + Logical Network & Cyber

CHAPTER 4 ISR FUNDAMENTALS

4-1 Intelligence, Surveillance & Reconnaissance Principles

Overview.

Intelligence, Surveillance & Reconnaissance (ISR) is the term presently applied to a combined arms enabling operation that combines what was previously described as reconnaissance and surveillance (a maneuver task) with the production and dissemination of intelligence (a staff task). ISR is a continuous operation focused on the collection of relevant information that is analyzed to create intelligence to inform the Commander's visualization and support the operations cycle.

ISR plays a huge part in the production of intelligence — the product gained by analyzing combat information for its relevance to the unit's mission — has always been critical to successfully accomplishing the mission. Today information is a critical element of combat power. The speed, reliability, and availability of combat information has changed considerably from past methods and new methods continue to evolve with technological advancements in automation systems.

Working Principles

- Initiate reconnaissance & surveillance early and conduct them continuously.
- Initiate appropriate reconnaissance & surveillance forward.
- Focus reconnaissance on CCIR and decision points (DPs).
- Integrate ground reconnaissance with surveillance assets.
- Integrate the staff in reconnaissance & surveillance planning.
- Maximize / optimize employment of reconnaissance & surveillance assets.
- Report, analyze, and disseminate information rapidly and accurately – to those who need to know it.

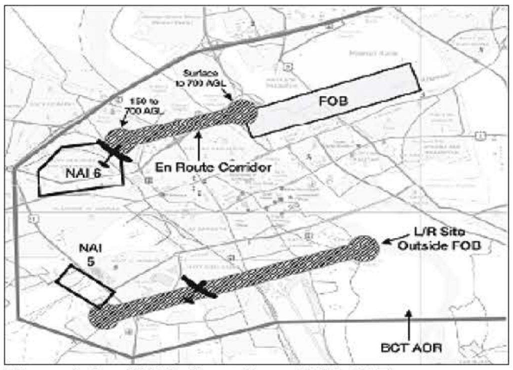


Figure 4.1 SUAS Operations BCT AOR

ISR Annex Information Items

- Area of Operations (AO) for reconnaissance.
- Mission statement.
- Task organization.
- Key requirements.
- Line of departure / line of contact.
- Initial named areas of interest.
- Routes to are of operations and passage of line instructions.
- Communications, automation architecture, and logistics support.
- Fire support measures.
- Medical evacuation plan.
- Fratricide avoidance measures.

Battalion ISR Planning

- A combined arms focus to the ISR plan.
- Subject matter expertise in respective battlefield operating systems.
- Augmentation to the reconnaissance platoon (engineers, artillery observers).
- Combat support and combat service support.
- Communications network planning.
- Information requirement submissions.

4-2 ISR Support to Protection (Base Defense)

Overview.

ISR missions preserve the effectiveness and survivability of mission-related military & nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of an Operational Area. Protection aims to integrate all organic capabilities safeguarding the force (personnel and equipment), noncombatant personnel, base systems, and physical infrastructure. This is accomplished by Commanders and Staff synchronizing, integrating, & organizing capabilities and resources to prevent or mitigate the effects of Threats & Hazards. ISR supports protection tasks through careful implementation following IPB, CARVER assessments, and Commanders' guidance.

Typical Protection Tasks

- Employ Camouflage, Cover & Concealment.
- **Harden Facilities.**
- Identify & Assess Hazards.
- Security: Deter / Detect / Assess / Respond.
- Collect, Analyze, & Disseminate Threat Information.
- Assess & Reduce Critical Vulnerabilities.
- **Establish Local Security.**
- Establish Civil-Military Partnerships.
- **Conduct Area & Base Security Operations.**
- Conduct Threat & Incident Response Planning.
- Conduct Exercises, Evaluate & Assess Plan.
- **Conduct Area & Base Security Operations.**
- Protect and Maintain Critical Infrastructure.
- Conduct Response Force Operations .
- Secure Supply Routes & Convoys.
- **Conduct Operational Security.**

Key Tasks

- **Area Security** protects friendly forces, installations, routes, & actions within a specific area preserving Commander's Freedom of Action.
- **Hardening** strengthens the survivability of high-value areas & assets reducing vulnerability for catastrophic loss against direct & indirect Attacks.
- **OPSEC** protects Essential Elements of Friendly Information (EEFI) by identifying observable actions by hostile forces or adversary INTEL systems & employing deception to ensure only desired events reach hostile forces.
- **Local Security** employs measures necessary to nullify & reduce the effectiveness of hostile attacks or base sabotage.

5 Protection Principles

- **Comprehensive**. All-inclusive utilization of complementary & reinforcing tasks and systems.
- **Integrated**. Unified with other activities, systems, & capabilities horizontally & Vertically.
- **Redundant**. Primary & Alternate protection capabilities for critical vulnerabilities.
- **Enduring**. Dynamic & continuous process monitoring changes in the operational environment.
- **Layered**. Deliberately sequenced across multiple domains, e.g. G2, Base HQ, Patrols, Guard Towers, UAS, QRF.

Local Security Measures

Protection tasks conducted by local & organic units protecting against Level I-III Threats. Local security involves avoiding detection or deceiving threats about Friendly Force positions & intentions. It prevents a unit from being surprised through Active & Passive Measures

Active Security Measures

- Guard Towers.
- Patrols.
- Unmanned Aircraft System.
- Alert Levels & Stand-to Times.

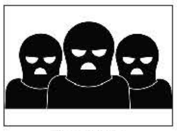
Passive Security Measures

- Camouflage & Concealment.
- Noise & Light Discipline.
- Operational Security.
- Movement & Emissions Control.
- Night Vision Goggle (NVG) Use.

Threat vs. Hazard

Threat. Any combination of actors, entities, or forces that have the capability & intent to harm military forces or national interests. Threats may include indigenous individuals, groups, paramilitary or military forces, and those of a foreign country.

Level I



Bandits

Terrorists

Level II

Small Tactical Units, Special Operations Teams, Combat Reconnaissance Teams, Irregular Forces.

Level III

Large tactical force operations, including airborne, heliborne,amphibious, infiltration, & major air operations.

Hazard. A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. Hazards are usually predictable & preventable and can be reduced through effective risk management efforts

Protection Planning

Planning is the first step towards developing an effective scheme of protection and planning is a **CONTINUOUS PROCESS**, reframing the Operational Environment as new threats emerge.

Effective Planning Steps

- Identifying Threats and Hazards (T&H).
- Assess the T&H to determine operational risks.
- Develop mitigating risk reduction measures.
- Integrate **Protection Tasks** (risk mitigation actions) into a comprehensive scheme of protection that includes mitigating measures.

Three Basic Assessments: Threats & Hazards , Asset Criticality & Asset Vulnerability.

- **Threats & Hazards**: Insurgents, separatists, bandits, civil disturbance, health & safety.
- **Criticality**: Key Assets required to accomplish a mission & impact if there is a temporary or permanent loss.
- **Vulnerability**: Determine the magnitude & effect on an installation, personnel, a unit, or other site.
- **Assessment Steps.**
  - List key Assets & Capabilities.
  - Determine if critical functions can be substantially duplicated with other elements of the command or an external resource.
  - Determine the time required to substantially duplicate key assets & capabilities.
  - Set response priorities for threats towards personnel, physical assets, & information.

Protection Priorities involve important decisions differentiating between critical assets & important assets. Seldom are there sufficient resources to simultaneously provide the same level of protection for all assets.

Critical Asset is a specific capability of such extraordinary importance that its incapacitation or destruction would have a catastrophic effect on the organization to function effectively and complete its mission. The lack of a replacement may cause a critical asset to become a top priority for protection.

A **Protection Cell & Work Group** uses information derived from the Commander's Guidance, Intelligence Preparation of the Battlefield, and the critical asset list to create a Protection Priority List (PPL) using the ***CARVER-P Methodology.***

The **Defended Asset List (DAL)** includes assets from the PPL actively defended with available resources.

APPENDIX A

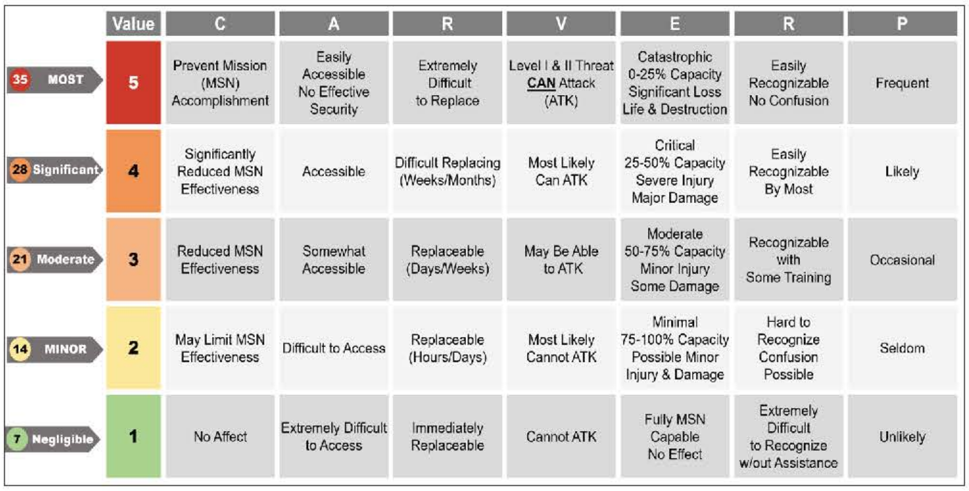
CARVER-P METHODOLOGY

Overview.

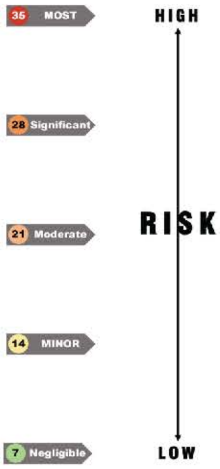
The *Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability + Probability* (CARVER-P) matrix is a valuable tool for conducting criticality and vulnerability assessments of base assets.

The CARVER targeting matrix assesses a potential target from a terrorist perspective to identify what the enemy might perceive as a good (soft or valuable) target. For criticality purposes, CARVER-P helps assessment teams and commanders (and the assets that they are responsible for) to determine assets that are more critical to the success of the mission. This also helps determine which resources should be allocated to protect critical assets (personnel, infrastructure, and information).

Criticality, **A**ccessibility, **R**ecuperability, **V**ulnerability, **E**ffect, **R**ecognizability + **P**robability



	Value	C	A	R	V	E	R	P
35 MOST	5	Prevent Mission (MSN) Accomplishment	Easily Accessible No Effective Security	Extremely Difficult to Replace	Level I & II Threat CAN Attack (ATK)	Catastrophic 0-25% Capacity Significant Loss Life & Destruction	Easily Recognizable No Confusion	Frequent
28 Significant	4	Significantly Reduced MSN Effectiveness	Accessible	Difficult Replacing (Weeks/Months)	Most Likely Can ATK	Critical 25-50% Capacity Severe Injury Major Damage	Easily Recognizable By Most	Likely
21 Moderate	3	Reduced MSN Effectiveness	Somewhat Accessible	Replaceable (Days/Weeks)	May Be Able to ATK	Moderate 50-75% Capacity Minor Injury Some Damage	Recognizable with Some Training	Occasional
14 MINOR	2	May Limit MSN Effectiveness	Difficult to Access	Replaceable (Hours/Days)	Most Likely Cannot ATK	Minimal 75-100% Capacity Possible Minor Injury & Damage	Hard to Recognize Confusion Possible	Seldom
7 Negligible	1	No Affect	Extremely Difficult to Access	Immediately Replaceable	Cannot ATK	Fully MSN Capable No Effect	Extremely Difficult to Recognize w/out Assistance	Unlikely



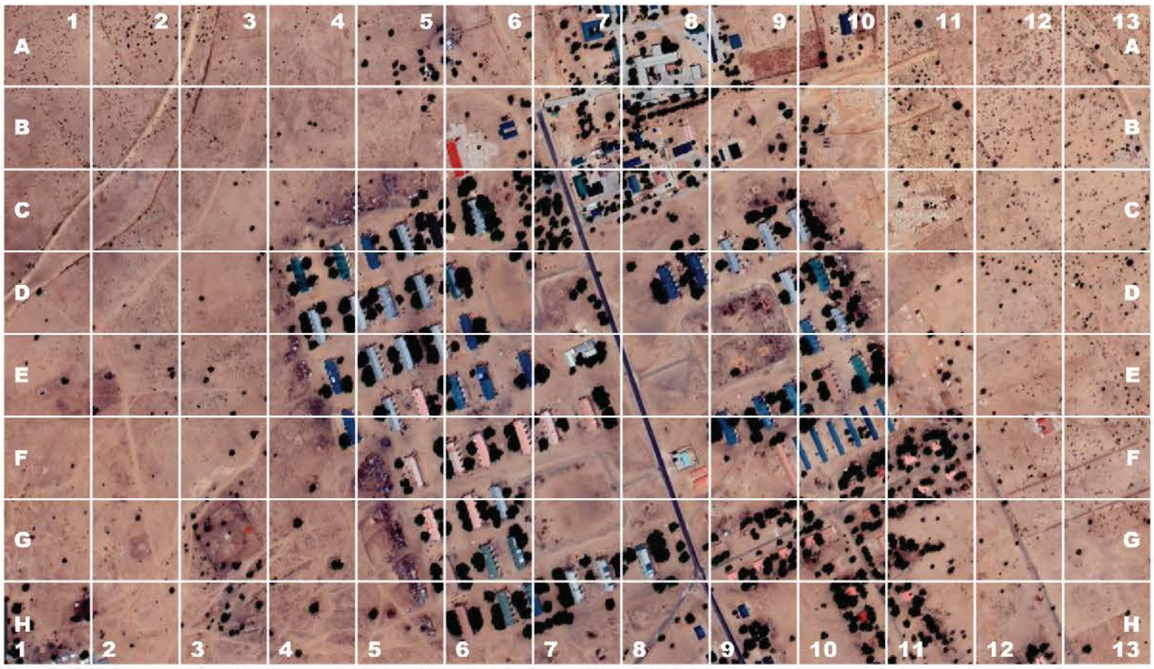
- **Criticality**. How essential an asset or critical system is to the organization.
- **Accessibility**. How hard it would be for an adversary to access or attack the asset.
- **Recoverability**. How quickly you could recover if something happened to the asset.
- **Vulnerability**. How well (or not) the asset could withstand an adversary's attack.
- **Effect**. How much of an impact there would be across your organization if something happened to the asset.
- **Recognizability.** How likely it is that an adversary would recognize the asset as a valuable target.
- **Probability.** How likely an asset will be targeted for surveillance or attack by a credible/ capable threat.

APPENDIX B

GRIDDED REFERENCE GRAPHIC

Overview.

Gridded Reference Graphic (GRG) allows an analyst to create grids for use in partitioning geographic areas of interest. Grids can be defined from a point or area based on dimensions, a reference system, or time and speed. Gridded reference graphics can be used in a variety of operations, including search and rescue, cordon and search, and clearing operations.



Gridded Reference Graphic Example Using Google Earth and PowerPoint

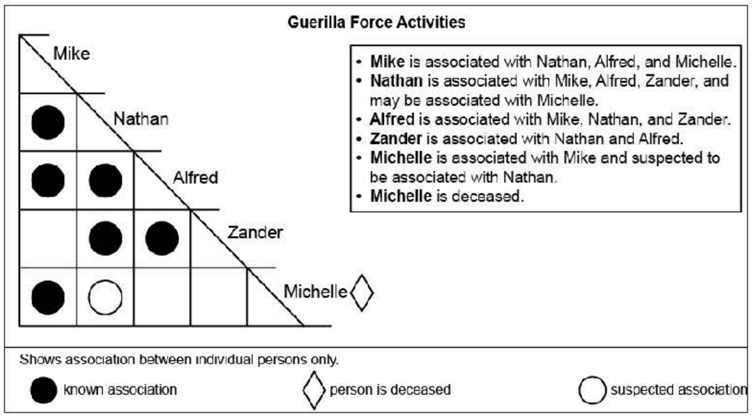
Method

1. Selected Area of Interest using Google Earth open-source software. This case Maimalari Cantonment.
2. Captured Image using *Print Screen* function and pasted into blank PowerPoint presentation slide.
3. Cropped image removing unwanted ancillary data & website page framing.
4. Cut cropped image from main slide & pasted into *Slide Master* template.
5. Close Mater View; screenshot map image should be visible as a background graphic.
6. Inserted & aligned a table over the background image with enough rows & columns to divide map image into equal spatial representations.
7. Applied *No Style / No Grid* to table.
8. Recolored table borders using preferred color & line weight.
9. Added preferred grid reference system using letters and Arabic numerals.
10. Removed map image from background graphics & reinserted on main slide *Sending to Back* below the table.
11. Selected All (table & map image), right clicked and saved as PNG image file that can now be easily exported as a stand-alone image or inserted into Intelligence products.

▲ *Before pasting into Slide Master template, delete preformatted style boxes.*

APPENDIX C

LINK ANALYSIS TOOL / MATRIX



Guerilla Force Activities

Mike				
●	Nathan			
●	●	Alfred		
	●	●	Zander	
●	○			Michelle ◇

- **Mike** is associated with Nathan, Alfred, and Michelle.
- **Nathan** is associated with Mike, Alfred, Zander, and may be associated with Michelle.
- **Alfred** is associated with Mike, Nathan, and Zander.
- **Zander** is associated with Nathan and Alfred.
- **Michelle** is associated with Mike and suspected to be associated with Nathan.
- **Michelle** is deceased.

Shows association between individual persons only.

● known association ◇ person is deceased ○ suspected association

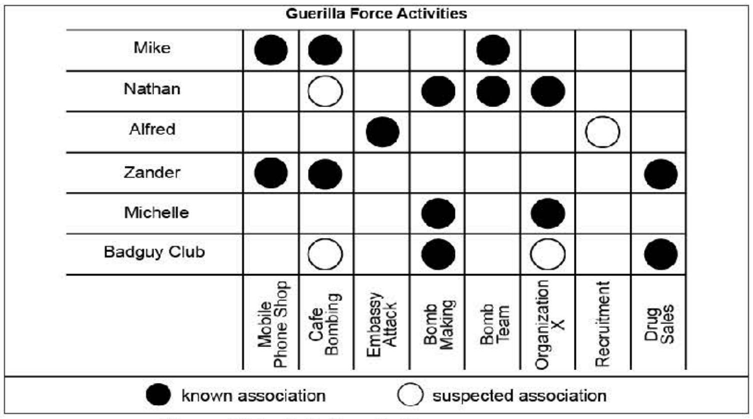
Figure C.1 Association Matrix

A matrix is a grid with as many cells as required to sort data and gain insight. A matrix can be rectangular, square, or triangular depending on the number of rows and columns required to enter the data. Three commonly used matrices.

» Threat intentions matrix efficiently analyzing information from the threat's point of view.

» Association matrix identifies the existence & type of relationships between individuals as determined by direct contact.

» Activities matrix determines connections between individuals and any organization, event,entity, address, activity, or anything other than persons.



Guerilla Force Activities

	Mobile Phone Shop	Cafe Bombing	Embassy Attack	Bomb Making	Bomb Team	Organization X	Recruitment	Drug Sales
Mike	●	●			●			
Nathan		○		●	●	●		
Alfred			●				○	
Zander	●	●						●
Michelle				●		●		
Badguy Club		○		●		○		●

● known association ○ suspected association

Figure C.2 Activities Matrix

A key feature of the matrices analytic technique is the formulation of ideas of what may occur when one element of a row interacts with the corresponding element of a column.

Link analysis is a technique used to evaluate the relationships between several types of entities such as organizations, individuals, objects, and activities. Visualization tools augment this technique by organizing & displaying data and assisting in identifying associations within complex networks. Analysts may use link analysis to focus on leaders and other prominent individuals who are critical factors in the AO.

A manual approach to link analysis is using small sticky notes of paper on a whiteboard. The analyst labels the notes to represent different entities and nodes and places them on the whiteboard.

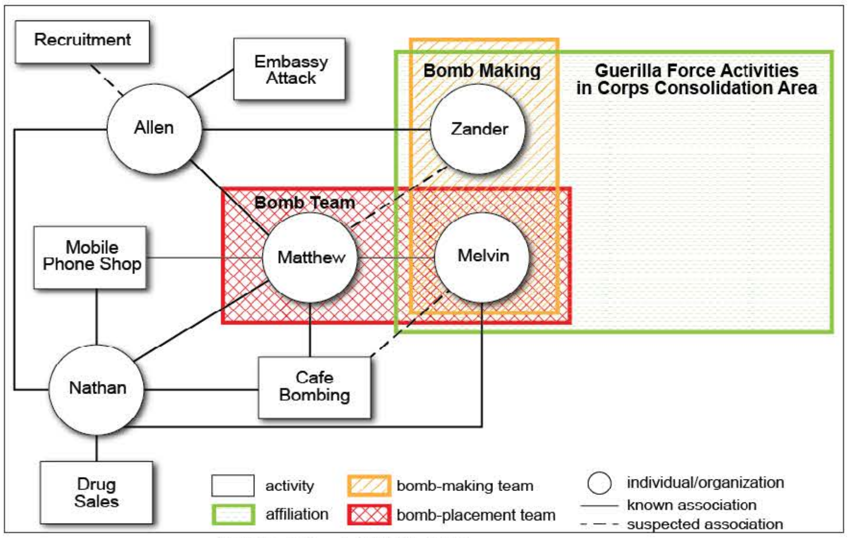


Figure C.3 Link Diagram