Intelligence Preparation of the Battlespace Terrorism Analysis Process/Methodology

(Version 3.3)

CDR, INSCOM
8825 Beulah St.
Fort Belvoir, Va 22060
Attn: CW4 Beasley
Comm: (703) 706-1223
DSN: 235-1223
Email: gsbeasl@liwa.belvoir.army.mil

Table of Contents

PREFACE

"The terrorist threat is posed by those who are patient, dedicated, well financed, tenacious and resilient. The United States and the Department of Defense must confront the terrorist with the same intensity and discipline we have used in the past to defeat conventional antagonists."

USS Cole Report

The terrorist attack against the World Trade Center and the Pentagon on September 11, 2001 changed the face of Intelligence Analysis forever. Gone are the days of conventional warfare with two motorized rifle regiments forward with one tank regiment and another motorized rifle regiment following. The USS Cole Report states; "DoD intelligence needs to refocus and tailor its resources to mitigate the terrorist threat for in-transit units. At the same time, independent transiting units need to provide higher authority with requests for information to force intelligence organizations to be responsive to the transiter's requirements. To aid the Intelligence Community in the production of actionable intelligence, DoD must allocate sufficient resources for all-source intelligence collection and analysis for combating terrorism. Reprioritizing resources for the collection of human intelligence (HUMINT) and signals intelligence (SIGINT) resources and the development of language skills will support this effort. The development of clearer counterintelligence (CI) assessment standards and a corresponding increase in CI resources is also required.

The impetus for this manual was threefold. First, provide a process and methodology on the Intelligence Preparation of the Battlespace (IPB) as it applies to Counter-Terrorism (CT) analysis. Secondly, we wanted the text to be in a structure that most military analysts, whatever their background, would understand. Thirdly, this manual will provide those non-CT analysts with a place to begin their terrorism analysis. Hence the inclusion of multiple graphics to show how event, target development and named areas of interest (NAI's) templates differ from the standard IPB conventional product templates, found in FM 34-130, dated 1994.

This manual cuts across the tactical, operational, strategic operations or planning spectrum. In addition, targeteers, IMINT and SIGINT analyst's and even intelligence elements within law enforcement can use the manual.

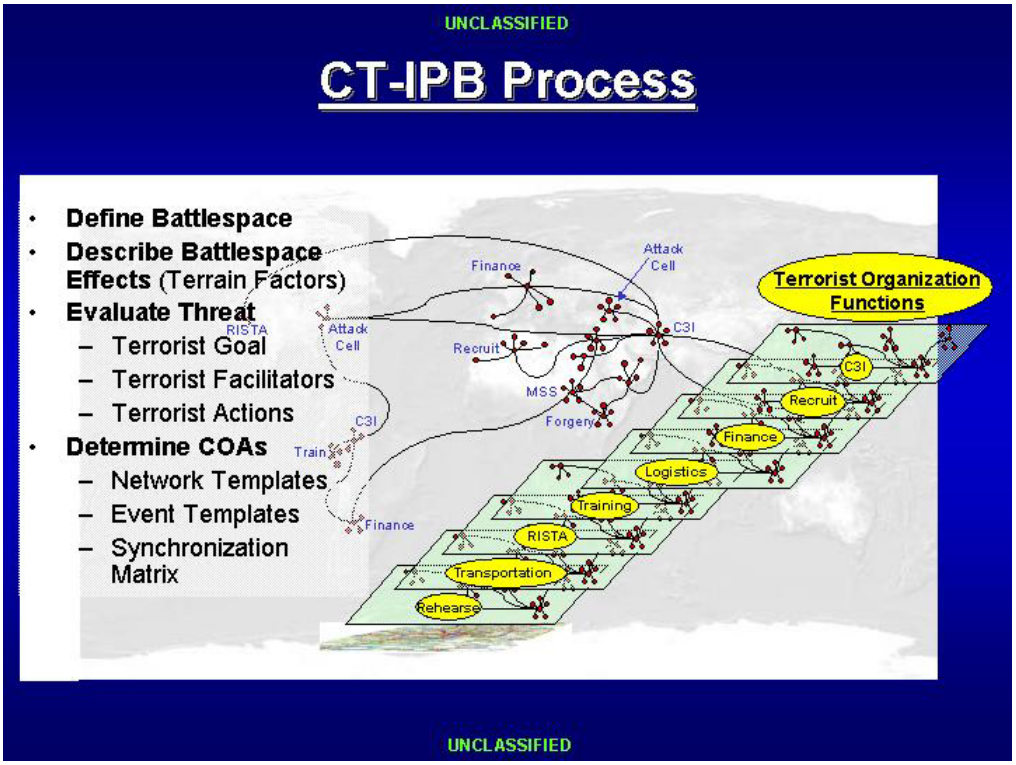
Intelligence Preparation of the Battlespace Terrorism Analysis Process/Methodology (Version 3.3)

1. **What is Terrorism**?

   - "Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience." Title 22 U.S.C. Section 265f(d)

   - "The calculated use of violence; or the threat of violence to attain goals--political, religious, or ideological in nature-by instilling fear or using intimidation or coercion." Army Regulation 525-13

2. **Four major components**: (Defining the IPB process/methodology against terrorist and Narco-terrorist groups or elements)
   A. Define the Battlespace
   B. Describe Battlespace Effects
   C. Evaluate the Threat
   D. Determine Courses of Action



Adjunct Components:

1) OCOKA-A
   a) **Observations**: Activity terrorist undertake to gather information on U.S. personnel, posts, facilities, organizations and businesses. Observations fall under reconnaissance, intelligence, surveillance, and targeting activities (RISTA).
   b) **Cover/Concealment**: Practices to protect operational personnel who are planning, leading, training, arranging for material delivery and/or coordinating transportation, and financing actions to support anti-U.S. activity. Deception measures are a component of cover and concealment. Covert and overt activity are integrated to mask true intentions and activities.
   c) **Operations**: Actions undertaken during all phases necessary to conduct a terrorist attack.
   d) **Key groups, personalities and associations**: Determine the composition, dispositions, strengths, vulnerabilities and methods of operation.
   e) **Avenues of approach and mobility corridors:** Determine the means through which the group operates, including electronic, telephonic and computer use and techniques, along with complete lists of key personnel, aliases, cover terms, contacts and associations between other terrorist organizations, elements and governments.
   f) **Activities & actions**: Integrating all knowledge on a group's procedures to know and apply understanding of normal activities. Analyzing actions of a group, cell, persons planning and potentially conducting plans to attack U.S. interests. Based on normal activities a group, cell or persons actions can become indicators, which provide warning of a terrorist attack. Review and overlaying information provided by signals, open source, human sources, and imagery can provide indicators of growing & impending actions. These overlays are situational templates of matrixes that when combined and placed over a U.S. facility may provide the terrorists courses of action (COAs).

2) Defense Mapping Overlays: (Normally performed at tactical and operational levels)
   a) Surface Configuration (Slope)
   b) Surface Drainage
   c) Vegetation
   d) Surface Materials
   e) Avenues of Approach
      [1] Lines of Communication
      [2] Mobility Corridors
      [3] Obstacles

3) Specialized Battlespace Effect overlays/matrixes: (Can be conducted from tactical to strategic levels)

   a) Region/City Infrastructures: Depicts the power grid, sewer, essential services (police/fire/rescue/governmental offices) that local authorities rely on for the region/city to function. Used to assist in defining potential targets of terrorist activity, as well as nodes necessary to assist in post attack responses.
   b) Demographics: Graphic depiction of the tribal/cultural and religious composition of an area; categorized, as an example, as a per capita figure per square km of ground for built up areas. Used to assist in defining those areas where terrorists might seek safe haven.
   c) Political affiliations: Graphic depiction of population/demographics depicting the prevalent political leaning of the populace. Helpful, in conjunction with demographic overlay, in determining areas likely sought as safe haven by certain politically motivated terrorist groups.
   d) Gangs/Tribes/Ethnic Affiliations
   e) Drug Cartels

f) Press coverage & affiliation
g) Population density
h) Environmental information
i) Atmospheric information
j) Financial networks: Graphic depiction of those trading centers and financial institutions used to support or fund terrorist operations. Assists in identifying nodes which might be of use in refining concentrations or areas in which terrorists must transit in order to financially conduct/support operations.
k) Communication nodes: Graphic depiction of the known nodes of communication used by a group. Preferably, a depiction of the physical location and density of activity. Used to compare this activity with other areas to determine areas and times the group is likely to communicate with it cadre.
l) Logistics: (Specific logistic networks): Graphic used to determine the means of delivery of those legal and illicit items the group is known to have transactions. This may involve the acquisition of illicit material, such as drugs or passports, or the areas where the group stores or caches supplies and equipment.
m) Natural resources
n) Political stability: A graphic depiction, which compares one area to another regarding the relative ability of the existing government to provide a stable, reliable institution for the populace. Areas prone to violent succession of power or lawlessness are contrasted to areas in which the existing government reduces the potential for political violence and lawlessness. The comparison is made regardless of friendliness to the USG.

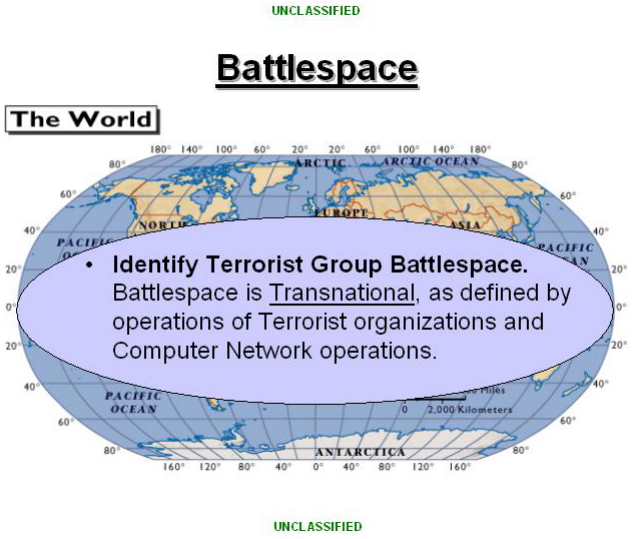
4) Weather/Meteorological Data: Depicts the effects of weather on terrain.

5) Security Environment: Estimates of the ability of local and national intelligence and law enforcement resources to deter, detect, and disrupt terrorist groups or operatives. An estimate on the relative effect of the security environment to adversely effect terrorist operation against or near US interests.

---

3. **Define the Battlespace**:

A. Identify the Friendly commanders and **Terrorist Group Battlespace**. For INSCOM and LIWA commanders, the world is their respective Battlespace. This supports IOC proposed mission of providing Army component commanders with Indicators & Warning (I&W) Force Protection notification through in-depth and integrated intelligence against Anti or Counter-Terrorism (CT), Counter-Narcotics (CN), Counter Network Operations (CNO) and Information Operations (IO).



B. Identify characteristics:

1) Terrain
2) Weather
3) Logistic centers, nodes and cells
4) Demographics:
   a) Ethnicity
   b) Religion
   c) Environment
   d) Atmospherics
   e) Languages
   f) Mannerisms (Folkways & Mores)
   g) Media (Printed and broadcast)
   h) Density
5) Financial Networks
   a) Banks accounts
   b) Official & Unofficial nets
   c) ATM
   d) Money transfer methods/nets
   e) Bank Correspondent agreements
6) Electronic/Communications
   a) Telephonic
   b) GSM net backbone
   c) Cellular net backbone
   d) Microwave backbone
   e) FORNSAT Sites
   f) INMARSAT
   g) Iridium net
   h) Coax cable system
   i) Fiber Optic Network
   j) Computer IP service providers
   k) Internet Chat rooms and group web sites
   l) Mail
   m) Multimedia (Distributed CD-ROMs, fliers, posters, tapes, etc.

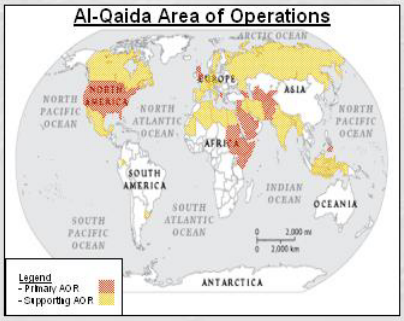
C. Estimate limits of Area of Operations (AO) and Interest

1) An Area of Operations (AO) is a geographic area from which terrorist organizations and elements coordinate operations, logistics, finance, recruitment, as well as stage, plan and execute missions. These areas, for any terrorist organization, can be thought of as either the operational or strategic areas in which the group operates and conducts the majority of its activity, as well as defining the area in which the group has the largest sympathetic base to support its organization's political goals. Development of terrorist group Area of Operations is best described as those areas the groups primarily operate. Example: Al-Qaida has primary and secondary areas of operations. The Primary AO generally includes those areas where Wahabbi school of Sunni Islam is followed. It specifically includes Afghanistan, portions of Pakistan, the areas within the Middle East and. Secondary AOs would include Africa, India to southern Philippines, the Caucuses and the Central Asian states of the former Soviet Union, England, Germany, U.S. and Canada

UNCLASSIFIED

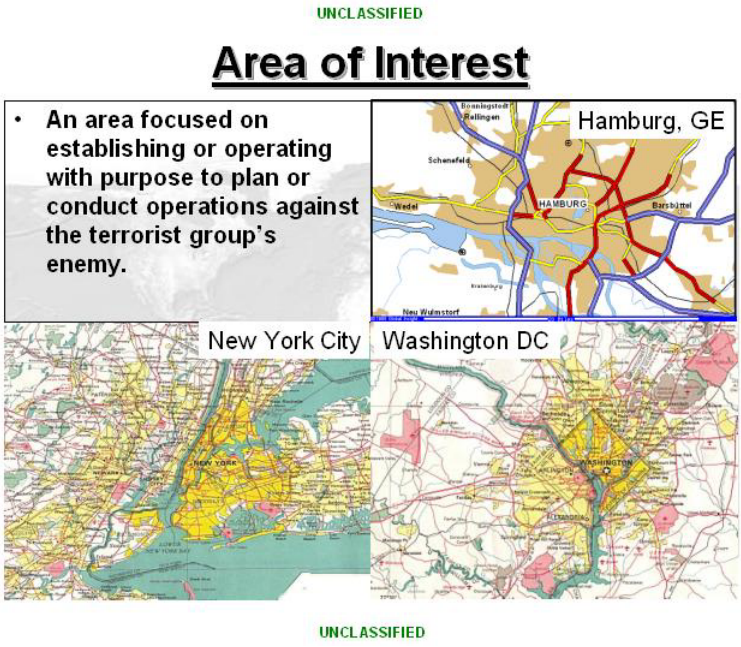
Area of Operations

- A geographic area from which terrorist organizations and elements conduct operations, logistics, finance, recruitment, stage, plan and execute missions.



UNCLASSIFIED

2) Areas of Interest (AI): Areas in which a terrorist organization plans on conducting operations against its adversary. A refined AO where terrorist groups focus operations within or against a specified target region, country, city, region or activity. An Area of Interest may fall within an Area of Operation, but certainly not in all cases for certain groups.



D. Determine initial intelligence gaps based on existent data. Note, the scope of intelligence gaps and the research required to establish a baseline set of knowledge is dependent upon the mission and composition of the force for which the AT/CT IPB process is constructed. For instance, Brigade sized (Task Force) element's intelligence requirements are much more narrowly focused and transitory than a larger element, such as ARCENT. An additional factor to consider when defining intelligence gaps is to determine the length of time the Army or Task Force element will remain in the area.

E. Establish commander's initial intelligence requirements.

1) Priority Intelligence Requirements:

a) Determine the terrorists' objectives. Understand the terrorists' immediate and long-term objectives. From these we can infer the effects they hope to achieve and identify targets that would allow them to achieve those effects.
b) Determine the terrorists' capabilities. This step involves determining the most likely methods terrorists might use to attack the target. It involves an analysis of methods used previously, but also requires imagining ways to combine methods in new ways or inferring totally original approaches.
c) Determine the terrorists' intentions. We must imagine how the terrorists are most likely to use their resources to achieve both their long- and short-term goals. Analysts must be steeped in terrorist philosophy, thinking, and culture. As threats become more defined, the PIR are changed to focus in on suspected threats and to determine both their potential targets and the means to attack them.
d) Example PIR: Just as there are no standard situation or event templates that will serve in all situations, there is no standard set of PIR. Good PIR, however, have some things in common:
[1] They ask only one question.
[2] They focus on specific facts, an event, or activity.
[3] They provide intelligence required to support an hypothesis (confirm or deny) or a decision.

2) Intelligence Requirements

3) Develop supporting Specific of Information Requirements (SIR). SIR describes the information required to answer all or part of a PIR. A complete SIR describes the information required, location where information can be collected, and time during which it can be collected. Normally, each PIR generates a set of SIR.
4) Develop and coordinate Specific Orders or Requests (SOR). The order or request generates planning and execution of a collection mission or analysis of database information. SORs sent to subordinate units are Orders. SORs sent to adjacent or higher units are Requests.

4. **Describe Battlespace Effects**

A. Identify the political objectives the terrorist groups known or suspected of operating in the same Battlespace as friendly forces. This will assist in determining whether or not the terrorist group will take action against US interests.

B. Identify effects of the area/local infrastructure for friendly and terrorist operations.

C. Identify the capabilities and limitations within the locale/area infrastructure offers for both friendly and terrorist operations. The purpose is to determine whether or not existing infrastructure and operating environment favors US or terrorist operations (or is neutral) within the battlespace.

D. Conduct assessment of geographic characteristics and man made structures and infrastructures against friendly force bases and operations and there application to support or limit terrorist operations.

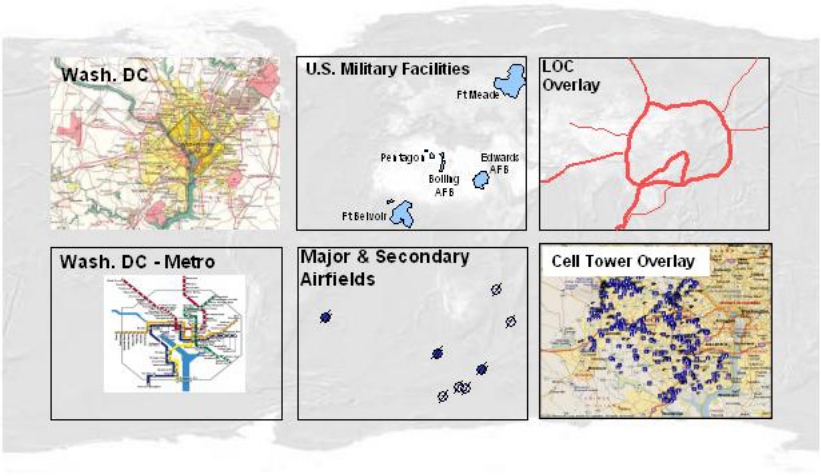
E. Describe the security environment and the ability of either US military, host nation, or local law enforcement to detect the presence and activity of known or suspected terrorists. In lieu of having an ability to detect known or suspected terrorists, describe the ability of the aforementioned to detect unusual or suspicious activity in or around US interests.

F. Type products considered Identify Terrorist Infrastructure:

1) Overlays portraying:
a) Friendly Disposition: A graphic depiction of friendly locations that the terrorists might just consider attacking.
b) Suspicious activity – A graphic depiction of suspicious activity, identified over time, relative to the position, and activity of friendly interests.
c) Demographics
d) Political affiliations
e) Religious Affiliation
f) Gangs/Tribes/Ethnic dispersal
g) Drug Cartels/Human smuggling networks or Slave trade networks
h) Press coverage & affiliation
i) Population density
j) Environmental information
k) Atmospheric information
l) Infrastructures:
[1] City functional components
[2] Airports
[3] Ports
[4] Bus schedules
[5] Trains
[6] Rental Car/Vehicle firms
[7] Police/Fire/Sanitation
[8] Cable Networks (Line diagrams)
[9] Visitor Quarters (Hotel/Motels)

[10] High/middle/low-end housing areas/regions

UNCLASSIFIED



UNCLASSIFIED

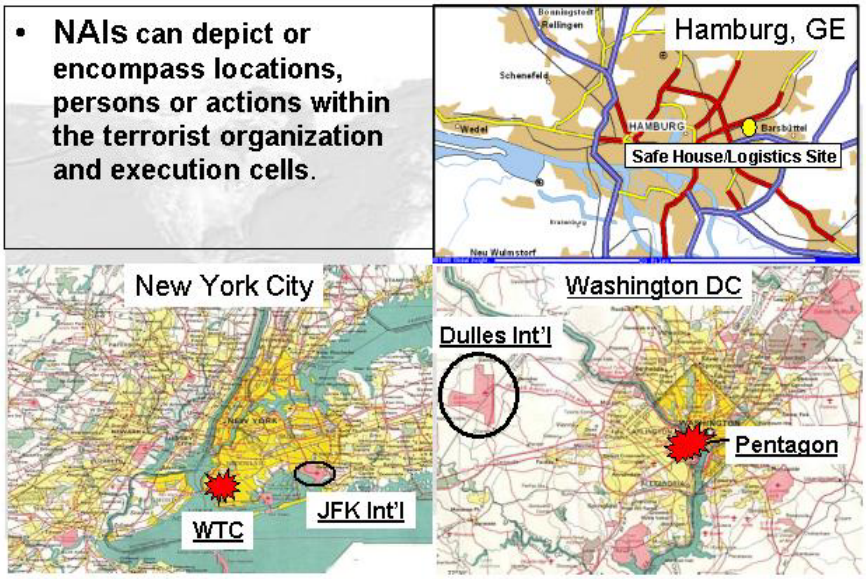
2) Modified Combined Obstacle Overlay: Reflects combination of the above overlays together or singularly. MCOO normally displays:

a) Lines of communication
   [1] Roads
   [2] Trails: Including goat, Nomadic tribe routes
   [3] Ferry sites & routes
   [4] Rail (schedules & times)
   [5] Air routes (schedules & times) Normally produced against a groups established normal movement patterns and transit points or countries.
   [6] Courier routes, waypoints, destinations and methods.
b) Communications
   [1] Cellular network/tower coverage's
   [2] GSM network & coverage areas
   [3] Country or regional established phones service. Includes layout of coax and fiber optic cables
   [4] FORNSAT coverages
   [5] INMARSAT
   [6] Iridium
   [7] Internet service provider server locations and connectivity
   [8] Internet IP and applicable URLs, chat rooms, email connections
   [9] Local/Regional landline telephone exchanges
   [10] Local television/Radio stations
   [11] Local/Regional newspaper officers/printing facilities
c) Financial Networks
d) Travel Agency Server networks (SABRE network)
e) Bottomline: MCOO supports AO & AI overlays while graphically portraying capabilities, vulnerabilities and communication methods which may be designated:
   [1] Key Terrain

[2] Named Area(s) of Interest (NAI)
[3] Target Area(s) of Interest (TAI)
[4] Decision Points (DP): The point in time and space where the commander or staff anticipates making a decision concerning a specific friendly COA. DPs are usually associated with threat force activity or associated with one or more NAIs. DPs also may be associated with the friendly force and the status of on-going operations.

UNCLASSIFIED

Named Area of Interest



UNCLASSIFIED

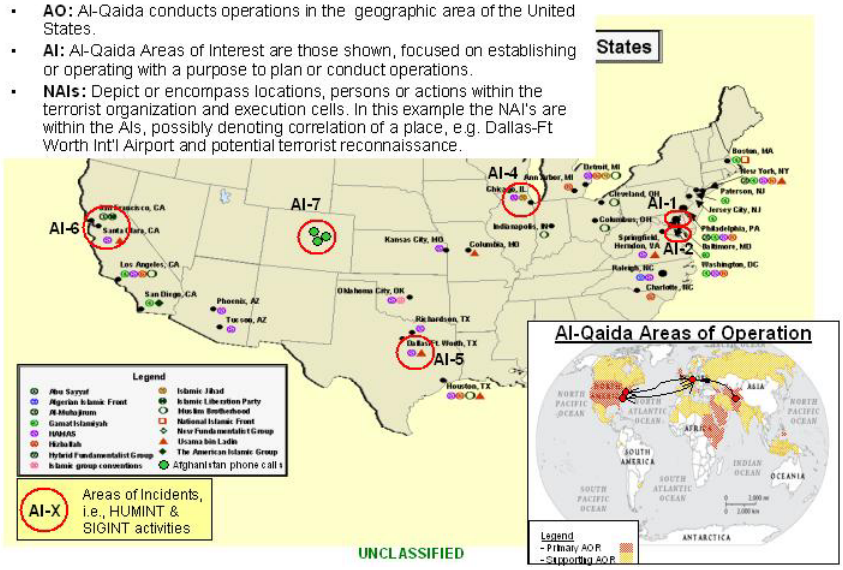
5. **Evaluate the Threat:**

UNCLASSIFIED

AO/AI/NAI

(Example)

- **AO:** Al-Qaida conducts operations in the geographic area of the United States.
- **AI:** Al-Qaida Areas of Interest are those shown, focused on establishing or operating with a purpose to plan or conduct operations.
- **NAIs:** Depict or encompass locations, persons or actions within the terrorist organization and execution cells. In this example the NAI's are within the AIs, possibly denoting correlation of a place, e.g. Dallas-Ft Worth Int'l Airport and potential terrorist reconnaissance.



UNCLASSIFIED

A. Analyze intelligence holdings to determine terrorist group's normal operating procedures, socio-political orientations, current operations, and future intentions.

B. Develop Terrorist threat models, which portray and consider established/known-operating procedures. Terrorist threat models can be based on:

1) Existing intelligence studies
2) Databases
2) Message traffic
3) Review of Friendly & Terrorist tactics, techniques & procedures.
4) Review terrorist training procedures and manuals
5) Review previous terrorist operations
6) Use Order of Battle Factors in support of establishing normal and doctrinal methods of terrorist operations. Be cognizant of adjusting previous operational patterns (doctrine) to account for new methods or modifications (Tactics, Techniques & Procedures).

a) Target Development:

[1] Determine mission objectives, e.g., physical, political, psychological, personal, profit, revenge, and possibly $2^{nd}/3^{rd}$ order effects.
[2] Acquire target
[3] Organize
[4] Conduct reconnaissance & surveillance
[5] Plan
[6] Train
[7] Rehearse/Test
[8] Execute
[9] Recover

b) Planning areas:

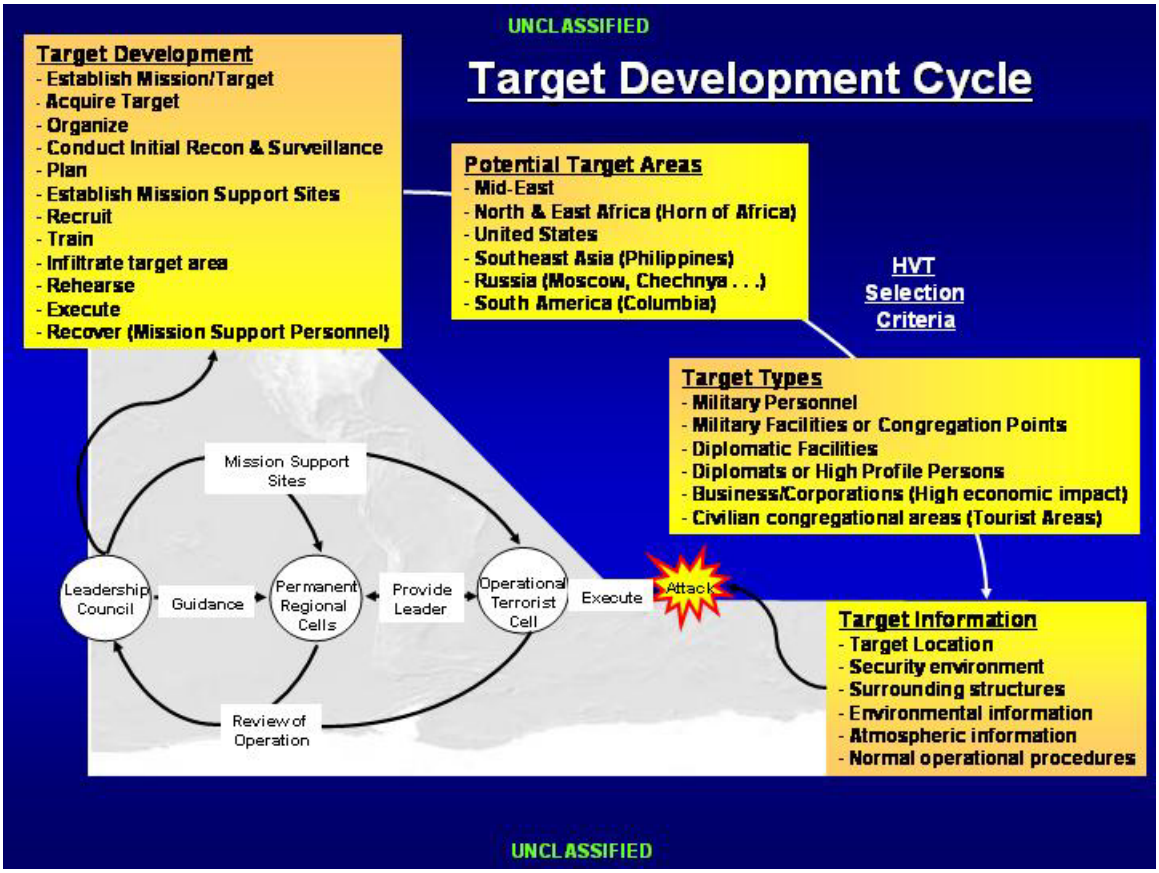
[1] Mid-East
[2] North and East Central Africa
[3] U.S.
[4] Southeast Asia (Mindanao area, Philippines)
[5] Russia
[6] Germany

c) Target types (HVT process):
[1] U.S. Military Facilities
[2] U.S. Diplomatic Facilities
[3] U.S. Diplomats/Ambassadors
[4] U.S. Businesses/Corporations
[5] U.S. Non-Government Organizations

d) Potential target folder information requirements:

[1] Target location
[2] Surrounding buildings and structures (build recognition information)
[3] Develop environmental information
[4] Develop atmospheric information, i.e., when is rush hour, how observant are people around the target, aircraft, airport, surrounding region.
[5] Security considerations, police, private security elements, alert/security procedures.

[6] Normal operations procedures observed at target and surrounding region. This also applies to terrorist travels and OPSEC procedures.



e) From a terrorist's perspective, there are generally seven steps or phases leading up to conducting an attack.

[1] Phase 1 – Initial Reconnaissance/Begin Planning. The group initiates plans to conduct a terrorist operation and assembles a limited cadre of people to formulate a plan of action. Persons not necessarily involved or affiliated with a terrorist group usually undertake initial reconnaissance of installations, facilities, or individuals. In this phase of an operation, the terrorist group is collecting a broad range of information from where it can begin its planning. *Note: Terrorists conducting reconnaissance and surveillance are vulnerable, as they must expose themselves. This exposure includes signature items, such as, cameras, notebooks, tape recorders and by conduct, e.g., loitering, repeated passes (walking or in vehicles), a long parked car with individuals, elicitation and being in the wrong place at the wrong time, i.e., being lost.* Establish Cell leaders (especially with multiple targets).

[2] Phase 2 – Possibly concurrent with Phase 1, the terrorist group establishes a cell to formulate a plan of action for accumulating additional information on potential targets, establishing sites in the target area to use as a base of operation, recruiting, evaluating, and possibly training potential operatives. This may also involve conducting supporting operations from safe havens.

[3] Phase 3 – Conduct additional reconnaissance. During this phase of the operation, additional recons of potential targets are conducted. From these observations, the list

of potential targets is reduced and general courses of action are developed concerning each potential or candidate target.

[4] Phase 4 – The terrorist group refines its information requirements concerning potential targets; and from this "short list", refined courses of actions (possibly material, financial, or personnel) and training requirements are derived.

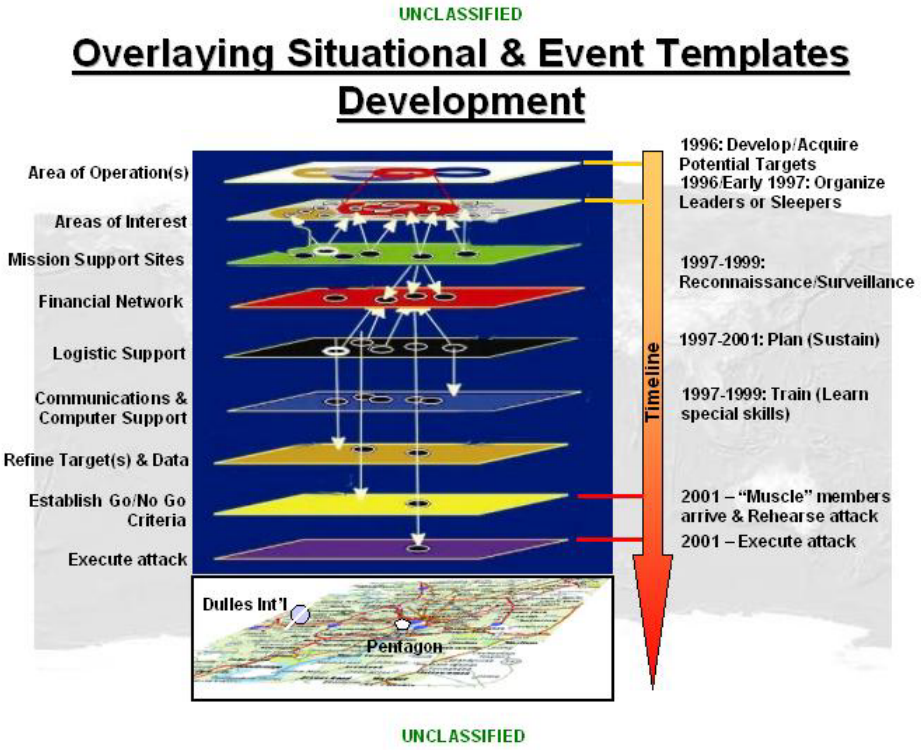
[5] Phase 5 – Rehearsal phase. At this juncture, target selection, methods of attack, and personnel issues have been determined. At this juncture, an "expert" may be sent to the operative cell to oversee final preparations for the attack or lend needed technical assistance for the attack to succeed.

[6] Phase 6 – Final reconnaissance is conducted prior to the attack. The purpose of this activity is to reconfirm previous information concerning the potential target to ensure a higher probability of success. During this phase, the outside "technical" expertise may be withdrawn to a safe haven to ensure availability for future activity. Note: It is not necessary for a "go" signal to be delivered to the potential terrorists as the decision to execute the attack will be driven by circumstances surrounding the particular target.

[7] Phase 7 – Attack phase. The actual terrorist attack occurs. This may be followed by congratulatory information or claims of responsibility, though generally such claims unless parts of a standard operation procedure for a group do not necessarily lead to culpability in all cases.

[8] NOTE: In an attempt to detect this type of activity in and around US facilities or interests, a comparison of potential hostile activity in and around US interests should be cataloged and archived. This will support long term analysis in the vicinity of fixed installations to assist in determining whether or not a US interest is possibly being surveilled for future consideration for attack.

Example: Following the attack in Dhahran, KSA in 1996, a great deal of effort was spent correlating observed activity in and around various facilities in KSA. This lead to a set of data points that allowed us to determine the mean number of unusual or suspicious activity near US manned sites. In turn, over a period of time, we were able to determine the usual number of unusual events by month. When anomalies occurred, we sought to explain them. Frequently we were able to do so, other times we were unable to. However, in those unexplained cases, they fell within the norm of unusual events, and while cognizant of them, we deduced they were the results of "normal" unexplained events, which frequently occur in this region. Similarly, a lack of reporting from a particular location was useful for us to determine potential shortcomings in our reporting apparatus or among filed reporters themselves.



7) Rank order HVTs after identification. Group identified key assets into one of eleven categories used to develop target sets.

   a) Command, control, communication and intelligence (C4I)
   b) Key personalities and job functions.
   c) Groups and associated elements, e.g., state sponsors or Al-Qaida and associated elements Egyptian Islamic Jihad, etc.
   d) Logistics personnel, locations, sites and responsibilities
   e) Finance: Personnel, locations, transfer methods (official & unofficial), server nodes, U.S. respondent banks (overseas banks with contractual ties to U.S. Banking institutions)
   f) Air Defense: (IADS structures and receipt, numbers, storage/location of MANPADS)
   g) Engineers (personnel trained in specialized assembly/handling of explosives or WMD)
   h) Reconnaissance, intelligence, surveillance and target acquisition (RISTA). Id personnel and activity/collection areas/sites.
   i) Weapons of Mass Destruction acquisition, storage, training, movement criteria.
   j) Radio, electronic, Telephonic and computers
   k) Group/element locations: Training sites, mission support centers (MSC), recruitment sites, and safe sites/houses.

Attack	Neutralization	Interdiction	Delay Ops	Operating Systems/Operating Functions	Relative Worth		
				Command & Control			
				Key Personnel			
				Logistics			
				Finance			
				Locations:			
				- Training			
				- Safe Sites			
				- Recruiting Locs			
				- Mission Support Sites			
				RISTA			
				WMD:			
				- Acquisition			
				- Development			
				- Storage			
				Electronics:			
				- Telephony			
				- Computers			

Example: High Value Targeting Matrix

C. Orders of Battle/Information data sets: Use all available intelligence agencies, National, Federal, DoD (Echelons above Corps and Theater Joint Intelligence/Analysis Centers) to collect, sustain, and refine information on terrorist groups, associations, cells, elements, gangs, tribes, etc. OB/Information data factors include but are not limited to:

1) Composition: (Leadership/Command &Control (C2))

a) Individual's name
b) Alias/A.K.A. names
c) SSN or Identification number
d) Date of Birth (DOB)
e) Position/Title
f) Physical description
g) Last known location
h) Code/cover names
i) Group affiliation
j) Group/cell/element associations
k) Associates: (Blue text represents version 2.5 addition)
   [1] Business
   [2] Friend's
   [3] Acquaintances
l) Country of origin
m) Addresses
n) Physical Description
o) Skills (Job functions)

[1] Primary skills
[2] Alternate skills

p) Phone/contact numbers:

[1] Phone
  [a] Type phone (Nokia, Iridium)
  [b] Phone feature (call waiting, voicemail)
  [c] Service Provider
[2] Contact Numbers
[3] Home (Actual home number, cellular/GSM or known phone booth, calling card associations or alternate electronic telephonic communication methods)
[4] Family
[5] Associates
[6] Financial
[7] Business
[8] Fax
[9] Call signs

q) Operational experiences

[1] Operations participated in
[2] Operations planned or led

r) Computer/Electronic:

[1] IP addresses
[2] URLs (frequented homepages, chat sites, other)
[3] IRQ, IRC, ICQ (net to phone)
[4] Software
  [a] Virus Protection
  [b] Financial (ex: Quicken)
  [c] Email (ex: Outlook)
  [d] ISP
    ((1)) Dial-up Modem
    ((2)) Wireless
    ((3)) LAN
[5] Hardware
[6] Computer Network (Diagram/Nodal Analysis)
[7] Steganography
[8] Operating System
[9] Email accounts and names
[10] PDA (Personal Digital Assistant)

s) Family:

[1] Parents (Include addresses & phone numbers)
[2] Spouses (Include addresses & phone numbers)
[3] Children (Include addresses & phone numbers)
[4] Relatives (Especially with frequent contact)

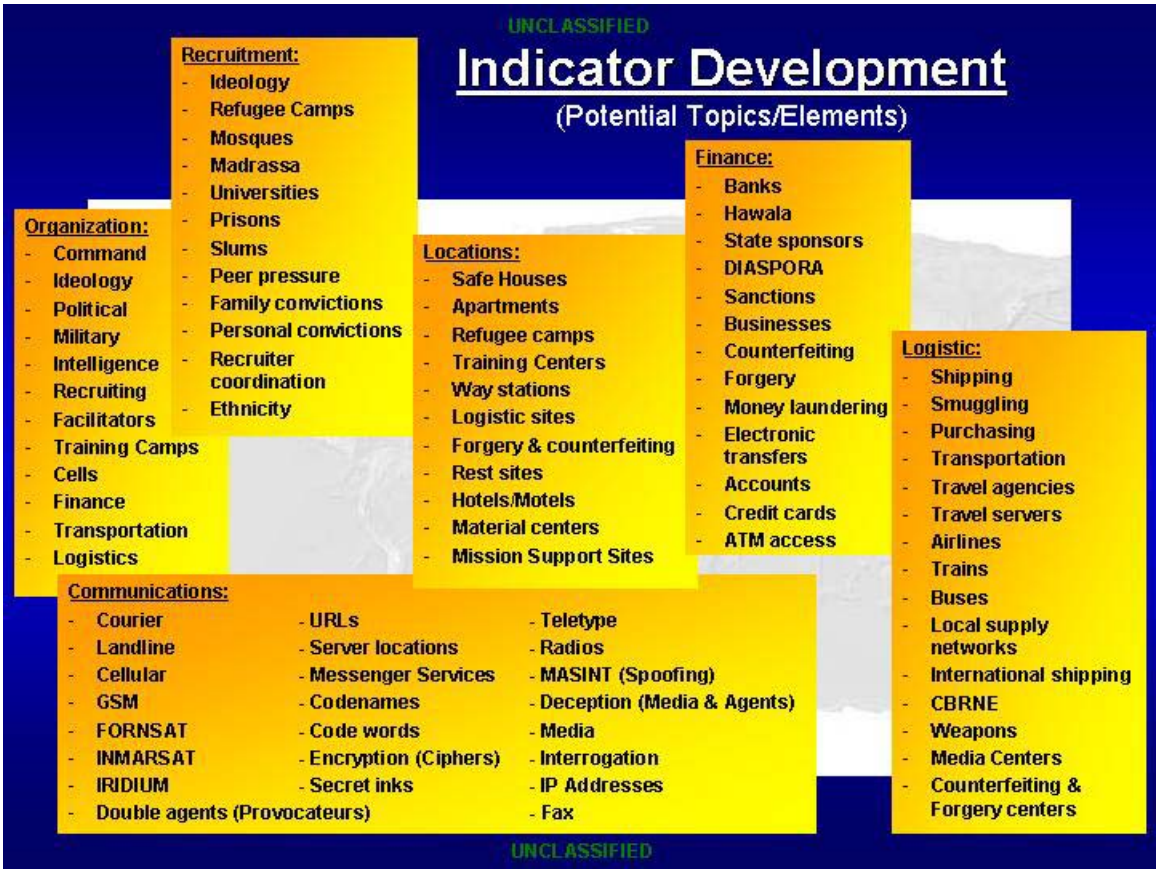
2) Disposition: (Mission Support Center)

a) Safe sites

[1] Previous locations used
[2] Specific areas/cities
b) Houses
c) Training camps/areas
d) Logistic locations
e) Forgery Sites
f) Mission Support Centers
g) Frequented hotels/motels
h) Rest/Recreation Areas
i) Areas of Interest (Frequented US cities)
j) Finance:
[1] Counterfeiting locations
[2] Bank Institutions
[3] Non-Sponsored Institutions (Hawala)
[4] State Sponsors
[5] Informal (Family)
[6] Financial Sanctions
[7] Institution Cooperation/Collaborative agreements
k) Other

3) Strength: (Manpower)
a) Numbers of personnel per cell/group/organization
b) Support (countries/other groups)
c) Methods of recruitment
d) Methods of retention
e) Recruiting:
[1] Recruitment locations
[a] Refugee camps
[b] Mosque's
[c] Madrassa's
[d] Universities
[e] Prisons
[2] Recruitment methods
[a] Family beliefs
[b] Personal characteristics
[c] Recruiter coordination
[3] Miscellaneous
[a] Languages
[b] Ethnicity
[c] Clothing

4) Methods of Operation: (Operations & Intelligence)
a) How?
b) Profile of previous operations
c) Indicators
d) Use of other individuals (cab driver, bellhops)
e) RISTA (Reconnaissance, Intelligence, Surveillance, Terrain Analysis)



5) Training:
   a) Doctrinal
   b) Military/paramilitary instruction
   c) Ideological training
      [1] Foreign
      [2] Internal
      [3] Communist:
         [a] Foreign
         [b] Internal
         [c] Communist
            ((1)) Russian
            ((2)) Che Guvera
            ((3)) Mao
   d) Special training requirements

6) Logistic operations: (Logistics/Funding)
   a) Material centers:
      [1] Smuggling
      [2] Local supply network/availability
      [3] International orders
      [4] Explosive (Components)
      [5] Weapons (Guns, knives, box cutters, etc.)
      [6] CBRNE acquisition & transfer
      [7] Media exploitation
      [8] Other
   b) Forgery centers

c) Counterfeit centers
d) Travel:
[1] Agents (Include electronic booking agencies/services)
[2] Airlines (Regional, national & international)
[3] Passports
[4] Support documents
[5] Vehicle rental operations

7) Assessments:
a) Capabilities
b) Activity (Establish norms to discern abnormal trends, patterns and actions)
[1] Activity relative to geographic location
[2] Activity relative to functional description from previous OB data set descriptions
[3] Activity related to internal/organizational matters compared to external matters.
c) Operating environment
[1] Friendly vulnerabilities: An assessment/judgment on the abilities of terrorists to exploit friendly vulnerabilities.
[2] Security environment: An assessment of the ability of organic and regional security (Host nation and local law enforcement, etc) to deter, detect and disrupt terrorist operations within the AOI.

8) Electronic technical data:
a) Telephonic:
[1] Landline
[2] Cellular
[3] GSM
[4] INMARSAT
[5] FORNSAT
[6] Iridium
[7] Teletype/Telex
[8] Radio
b) Computers and computer network:
[1] IP addresses
[2] Service providers
[3] Server locations
[4] Frequented URLs
[5] Messenger aliases
[6] USENET/NEWSGROUPS

9) History
a) Tactics, Techniques & Procedures
b) Previous operational data:
[1] Previous areas subject to surveillance or observation, or otherwise identified as potential or actual targets.
[2] Intended but not executed targets
[3] Other operational data

D. Additional evaluation techniques/applications:

1) OB not independent – look for overarching factors.
2) Terrorist group frameworks
3) Tailor evaluation to group capabilities and intent
4) Establish and sustain picture of terrorist group, cell or elements normal operational activity and modus operandi (Who, what, when, where, why and how)
5) Brainstorm/wargame friendly vulnerabilities against terrorist capabilities.

6) Rely on subject matter experts.

6. **Determine Courses of Action**

A. Definition: The identification and development of likely COAs which terrorists, narcotics organizations, gangs or tribes plan to execute against U.S. facilities, personnel, businesses, non-governmental organizations, and key personnel/diplomatic persons.

B. Identify the full set of COAs available to:

a) Terrorist groups, cells, elements and what their possible objectives are.
b) Employ knowledge of terrorist group decision-making cycle. Example, In overview the Al-Qaida decision cycle is represented as:
c) Target Selection (Important targets are approved at highest authority level)
d) Establish Presence and communications channels
e) Initial Reconnaissance
f) Establish Mission Support Sites/mechanisms:
   [1] Financing
   [2] Logistics
   [3] Transportation
   [4] Safe sites (Potentially in another country or continent)
g) Recruit and start special training, if required
h) Refine intelligence and complete courses of action (COA)
i) Sustain Surveillance
j) Sustain Preparation and rehearse
k) Execute
l) Publicize
m) Escape/Recover (Mission Support Personnel)
n) Develop COA, which significantly influence friendly commander's decisions for force protection.
o) Think asymmetrically, e.g., a plane can be used as a bomb.
p) Develop or use indications of activity beyond normal operating procedures or parameters for terrorist personnel, cells or groups.

C. Identify those areas and activities that, when observed, will discern which target(s) the terrorist cell leader or group have chosen, develop COAs.

D. Integrate terrorist group/cell (Battlespace effects). Elements to consider:

1) Terrorist group objectives: Potential multiple targets, e.g., US Embassy's in Dar-Es-Salaam, Tanzania and Nairobi, Kenya or the near simultaneous attacks on the World Trade Centers, New York City and the Pentagon. The actual objective of al-Qaida was to demonstrate the ability to conduct large-scale, spectacular terrorist attacks. The objective was accomplished by selecting politically noteworthy, vulnerable targets.
2) Effects of environmental and atmospheric data to include normal friendly operations at and near intended targets. Environmental data for kidnapping operations would include targets daily patterns, general population movements (rush hours, lunch, school, police schedules), especially in execution window, routes and times to and from home to work, etc.
3) Friendly vulnerabilities especially security operations and movement patterns around and near selected targets.
4) Current dispositions: Known safe sites, mission support cells, hostels, associate houses/apartments, logistic centers (businesses) which are in the vicinity of U.S. facilities (Embassy's, refueling sites, bases, etc.).
5) Location of potential targets, e.g., Dar-Es-Salaam, Tanzania and Nairobi, Kenya.

6) Terrorist perception of Friendly operations. Frequently, terrorist organizations/members will modify, delay, or cancel operations based on the US force protection response to potential threat information.
7) Identification of suspicious activity in or near US interests, or areas in which US assets will transit.
8) Terrorist efforts to maintain operational and tactical surprise including (limiting) links between senior controller and target site cell leader(s), RISTA personnel, financial network/ties, and rehearsal of operations.

E. COAs must be distinct. Factors to consider:

1) Its effect on friendly mission and force protection
2) Location of single or multiple targets.

F. Additional considerations:

1) Superior understanding of a given (Terrorist or narcotic) groups operational, training and tactical procedures.

2) Feasibility of terrorist operations against DoD facilities, U.S. Diplomatic and major business corporation facilities, U.S. key personnel (OCONUS) and Non-Government sponsored organizations.

3) Acceptance of risk/casualties. Some groups are risk adverse in attempting operations, while others will carry out operations regardless of risk, e.g., LTTE. There are, however, factors which way on the amount of risk (risk being defined as the probability of concluding a successful attack, rather than the survival of the attackers.), namely the ability to approach the target area in sufficient strength or with sufficient assets to execute a successful attack.

4) Uniqueness: Applied modifications from known terrorist TTP toward target types.

5) Consistency with capabilities:

a) Based on previous operations
b) Deception practices
c) Knowledge of U.S. actions and responses.

6) Audacity. Evaluate the potential COA(s) against terrorist objectives:

a) Physical destruction
b) Political
c) Psychological
d) Personal
e) Profit
f) Revenge
g) Accomplishment of $2^{nd}/3^{rd}$ order effects.

G. Evaluate and prioritize each COA. Note, identified COAs are assumptions about terrorist plans and operations while considering U.S. facilities, businesses, and key personalities.

1) Analyze each COA to identify its strengths, weaknesses, decision points and any potential centers of gravity.
2) Evaluate how well each COA meets the criteria of suitability, feasibility, acceptability, and consistency with terrorist doctrine, previous operations and TTP.
3) Evaluate how well each COA takes advantage of the battlespace environment.

a) Terrorist group's intent or desired end state.
b) Objectives
c) Effects of friendly operations & security environment.
d) Current dispositions:

[1] Senior leadership for operation.
[2] Cell leader locations
[3] Reconnaissance and Intelligence personnel & reporting locations.
[4] Training centers
[5] Mission support centers
[6] Logistic sites & transportation methods
[7] Financial: (Banks and contacts)
[8] Execution team members

4) Compare each COA to the others and determine which presents the most likely terrorist operation.

5) Consider Terrorists capability and constraints may force or develop new methods for a COA, i.e., they choose 2nd or 3rd COA over the predicted (most likely) COA.
6) Analyze the threat's recent activity to determine if there are indications that one COA is already being adopted.

H. Develop COAs in detail or as time allows:

1) As a guideline each COA must try to answer:

a) Who:

[1] Terrorist Organization(s)
[2] Sponsor(s)
[3] Group/Cell/Gang/Cartel

b) What:

[1] Target Types
[2] Target selection
[3] Objectives

c) When:

[1] Planning criteria, TTP and/or doctrinal procedures
[2] Factors:

[a] Capability
[b] Intent
[c] History
[d] Activity
[e] Operating environment
[f] Target atmospherics & environmentals
[g] Personalities

d) Where: The terrorists groups identified or potential area of operations and areas of interests. Example, Al-Qaida:

[1] Mid-East
[2] East-central Africa
[3] United States
[4] DoD facilities:

[a] Bases
[b] Ports
[c] Airfields
[d] Transit points
[e] Other

[5] U.S. Diplomatic facilities
[6] U.S. Businesses or Corporations
[7] U.S. Diplomatic personnel
[8] U.S. Agencies, example, U.S. Aid and Information Agency

e) Why: The vision/mission of the terrorists. Note, include thoughts on potential target restrike methodology. Example:

[1] Objective

[a] Physical
[b] Political
[c] Psychological
[d] Personal
[e] Profit
[f] Revenge

[2] Decide
[3] Detect
[4] Deliver
[5] Assess:

[a] Battle damage assessment (BDA)
[b] Munitions effects (ME)

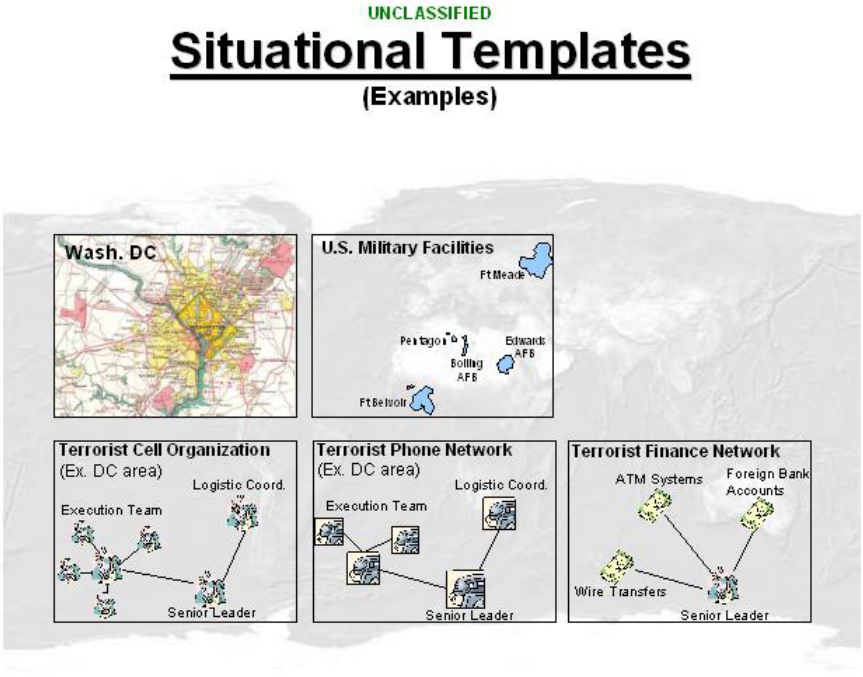
[6] Restrike nomination based on review of BDA and ME assessments. Note, assess/reassess can be applied against any phase of the planning, i.e. Objective, (assess), decide (assess), detect (assess), etc.

f) How: Methodology which the threat will employ his assets and determine time and place of the terrorist cells attack.

I. Develop in detail as time allows:

1) Situation templates: Graphic overlays depicting information derived from intelligence collection processes, e.g., signals intelligence (SIGINT), etc.
2) Description of COAs and options. Description of the proposed or potential actions or activities being conducted by terrorist groups, cells and elements with intention to attack U.S. forces.
3) Develop, integrate, review, High Value Target and High Priority Target lists. Note, from terrorist perspective HVT/HPT may be U.S. Ambassadors or other key personalities.

J. Situation templates: Graphically portray intelligence information reflecting terrorist group and cell actions and activities. They are based on databased information reflecting a norm of activities in a given area or region.



K. Terrorist situation templates are normally developed from:

1) Open source information (OSINT)
2) Human derived intelligence reports (HUMINT)
3) Signals intelligence (SIGINT)
4) Imagery intelligence (IMINT)
5) Multi-spectral analysis (MASINT)
6) These templates may be applied alone or overlaid to provide common locations, personalities or activities.
7) Use analytic judgment and knowledge of the terrorists TTP, doctrine and previous operations to determine and adjust information to be modeled/displayed on the situation template or situation matrix. Account for and integrate environmental and atmospheric data.

   a) Check the situational template to ensure you have accounted for all of the terrorist group's major assets and functions.
   b) Ensure the templates reflect the potential multiple targets identified for the COA.
   c) Include as much detail on the template as time and situation warrants or allows.
   d) Next think through the COAs scheme of maneuver. Attempt to visualize how the threat will transition from collection, reconnaissance, and preparation to actual attack times and phases on the templates.

   e) Mentally wargame the scheme of activities and action required to attack each target. Identify areas, personalities and locations of commonality between SIGINT, HUMINT, and OSINT information. Follow-up by identifying how each "fits in" and supports the operation.

UNCLASSIFIED

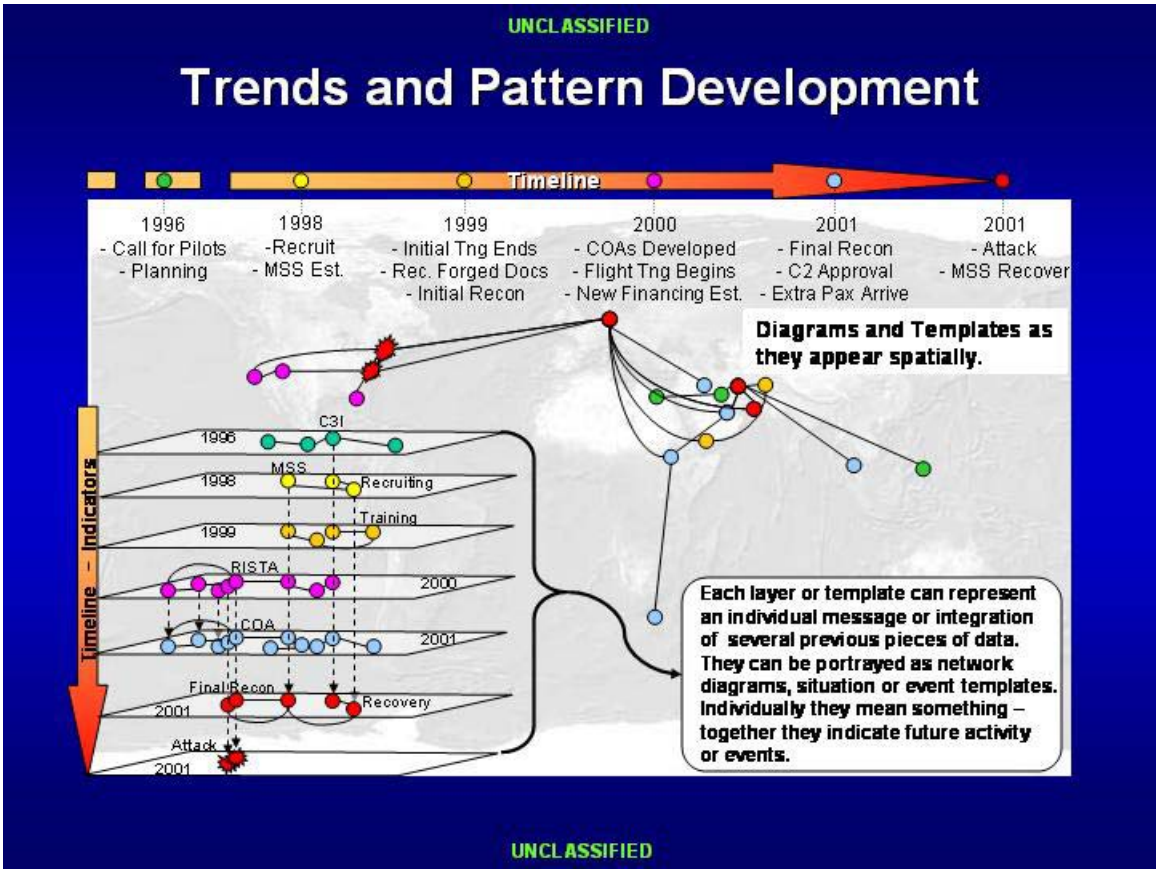
Personality Activities Matrix

(Potential: NAI, TAI, HVTs)

Name	Ldr	Log	Fin	Tng	Special Skills	Recon/ Surveil	Rehearsal	Recruit	Mission Spt Ctr	Comments
((Atta))	X		X	X		X	X		X	Computer skills, used Al-Qaida TTP doctrine
((Al-Shehhi))	X	X		X		X	X		X	
((Hanjour))	X			X		X	X			Arrived Calf, 1996
((Alhazmi))	X	X		X		X	X			In San Diego since, 1999
((al-Midhar))		X								Connected to USS Cole
((Ahmad))			X					X		UAE: Key Finance man
((Alhaznawi))								X		
((Ahmed))								X		
((Alomari))								X		
((Raissi))					X					Pilot trainer

UNCLASSIFIED

L. Evaluate time and space factors to develop timelines of activities. Timelines are established from observations of previous terrorist actions. Example, Al-Qaida attack operations against the U.S. embassies in Dar-Es-Salaam and Nairobi, began in 1993. Between 1993 to 1995 reconnaissance and surveillance intelligence collection was conducted. Starting in 1995 logistics sites were activated in both locations and in Khartoum, Sudan. During the 1995 to actual attack date in 1998, senior leaders in Afghanistan spoke or met with cell leaders and supported continued planning, training and movement of materials and personnel.



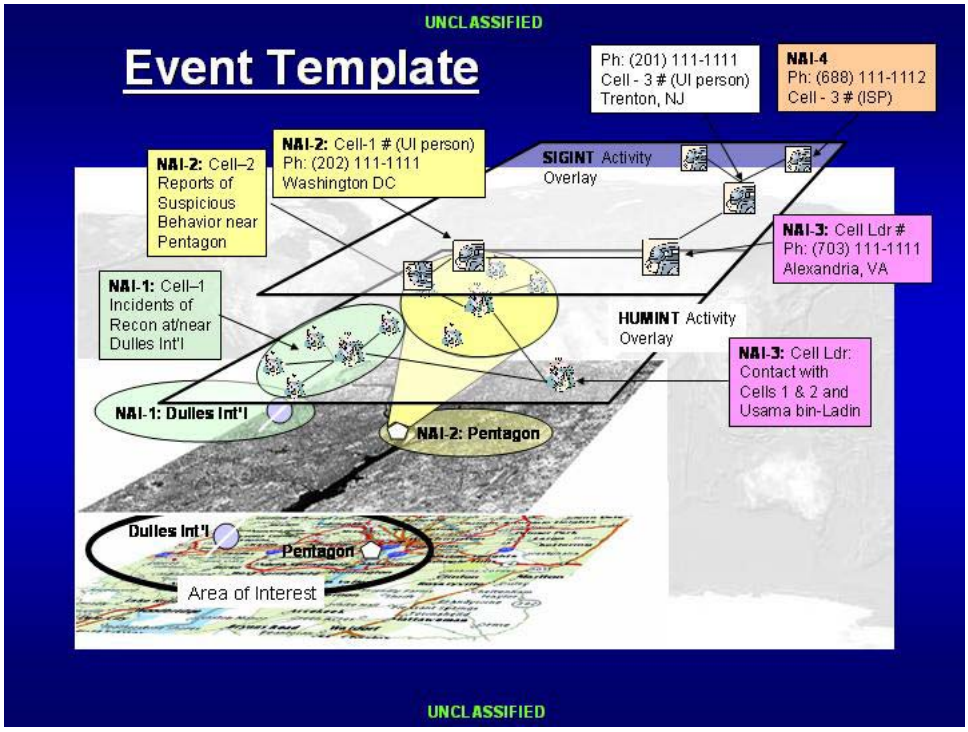
M. Overlay as many as necessary situational templates against the U.S. facility, place or person's activities. Synchronize the templates against potential/established terrorist decision cycles and timelines to friendly actions and activities. Once overlaid staff wargaming should determine possible indicators and warning of any impending terrorist actions, activities or attacks.

N. The combination of situational templates against friendly posts, facilities and actions forms a/or several potential terrorist COAs. Note, the overlay depicting friendly movements and posts is the event template. The combination of situational and event templates is a COA which supports collection planning requirements.

O. Identify initial collection requirements: The art of identifying initial collection requirements revolves around depicting specific areas and activities, which when observed, reveal terrorist intentions and possible COAs. Identifying terrorist actions and activities lead to indicators. These identified indicators occurring near or around U.S. facilities or personnel become information requirements and support development of a collection plan. Based on indicators and synchronizing situational templates with an event (U.S. person, facility, post, etc) PIR and IR, NAIs, TAIs, Decision Points (DP), and HVT/HPT lists are derived. The combination of these derivatives also supports the collection plan as well as guiding the RISTA plan.

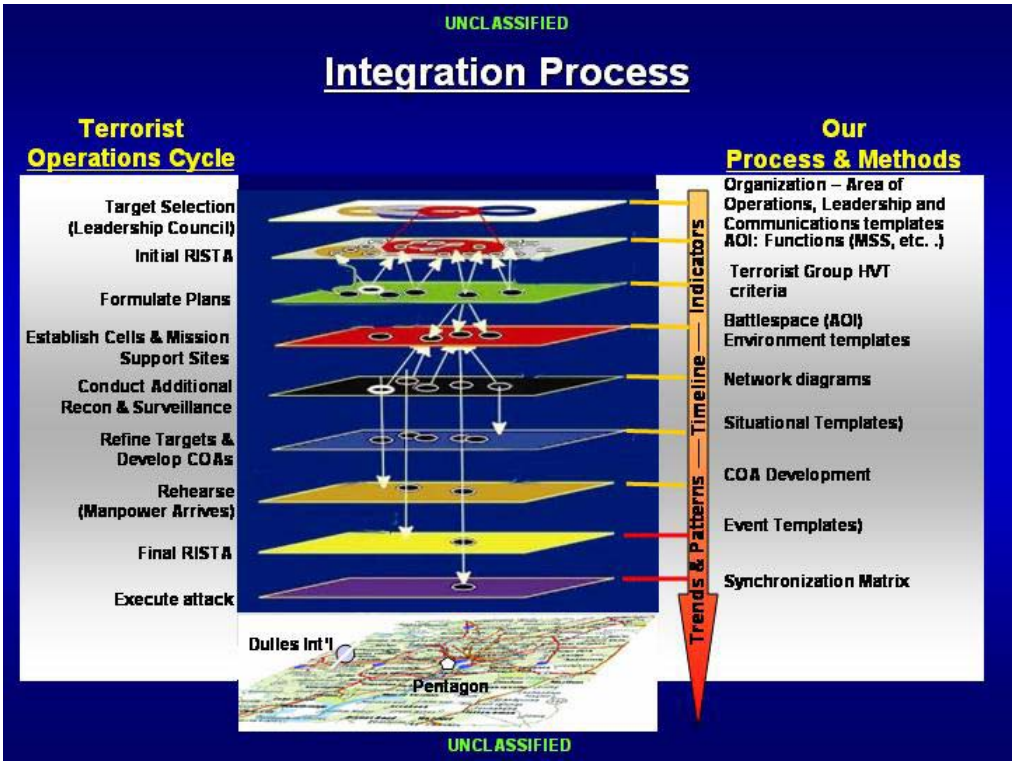
1) Evaluate each COA to identify its associated NAIs, TAIs, and DP.

2) The Event Matrix/Template: Is a graphical depiction of the terrorist's target. Overlaying situational templates helps determine locations, logistic sites, personnel, financial support chains and other functions necessary for their (terrorist) attack, these become NAIs.



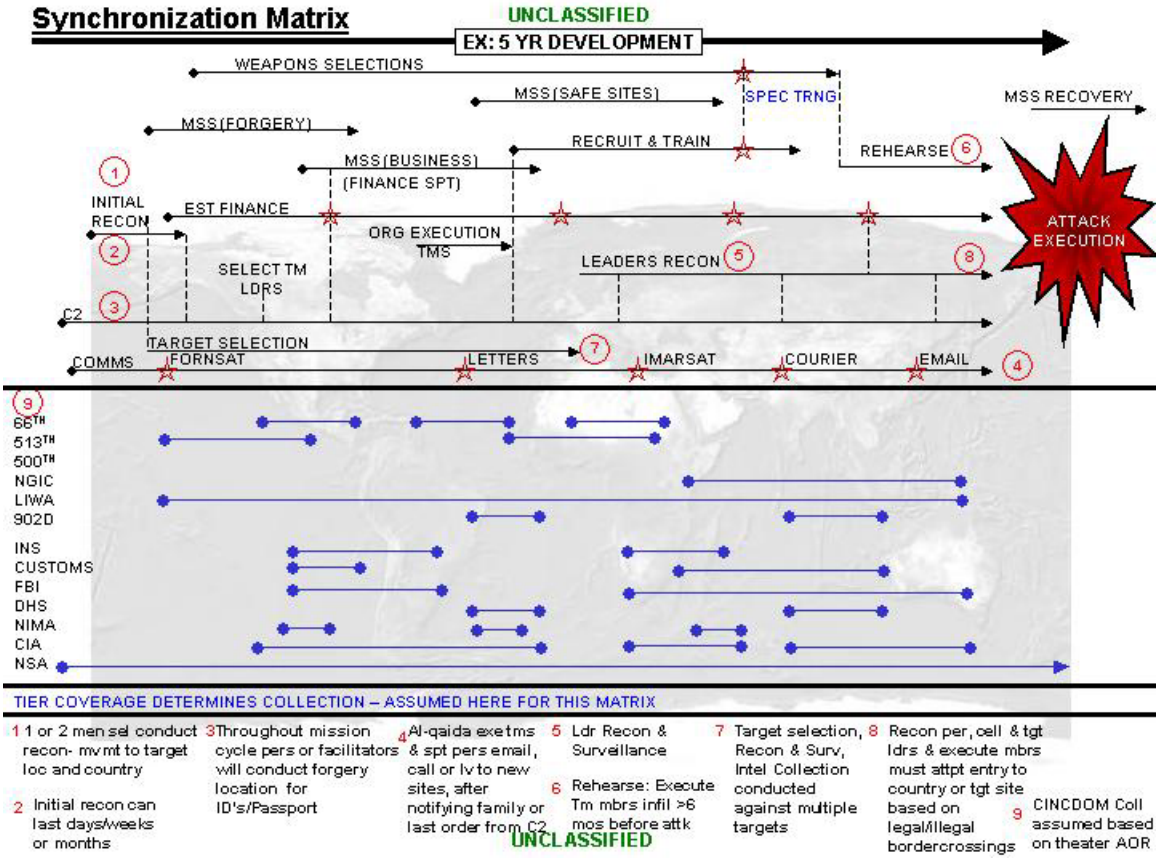
3) NAIs can depict or encompass locations, persons or actions within the terrorist organization and execution cells, i.e., NAIs for terrorism can also include the connections between personnel (phone calls), transportation and shipping methods, funding/money transfers and banking sites, recruit and training centers, associations with governments, etc.

4) Additional considerations:



a) NAIs also support indicator development. Indicators may include or reflect what phase the terrorists are in their normal planning to execution timeline. Determining the potential phase of a terrorist group or cell operations provides friendly forces with capability to interdict within the terrorists decision cycle.
b) Remember that terrorist groups can be transnational, i.e., they operate without borders or government limitations.
c) An NAI may need to encompass a terrorists travel plans, actions and flights, e.g., follow a key terrorist from departing Afghanistan to Pakistan and all subsequent movements and methods (airline or vehicle travel).
d) Staff wargaming incorporates NAIs to establish a decision support template (DST), which is used by the commander, and staff to track high priority targets (HPTs).

5) The event template and matrix, once complete, form the basis for planning collection strategies, synchronizing intelligence with friendly operations and preparing the collection plan.



7. **Abbreviated Anti/Counter-Terrorism IPB:**

A. Define the Battlespace Environment:

1) Determine locations of U.S. presence
2) Know terrorist group and activities.
3) Group and state sponsor affiliations.
4) International and National supporters:

a) Moral supporters
b) Financial support
c) Physical/logistic support

5) Identify terrorist capability and intent.

B. Describe Battlespace Effects.

1) Demographics:

a) Ethnicity
b) Religion
c) Environment
d) Atmospherics

2) Targets and routes:

e) Identify susceptibility
f) Identify infiltration routes and transportation modes.

C. Evaluate the Threat:

1) Identify AO
2) Identify AI
3) Identify cell, composition and jobs skills
4) Conduct Order of Battle analysis

a) Composition:

[1] Organization
[2] Cellular structure
[3] Links/associations

b) Internal discipline:

[1] Recruiting
[2] Training
[3] Security
[4] Special selection for projects
[5] Continued political indoctrination

c) Goals:

[1] Short term
[2] Long term

d) Dedication
e) Religious, Political and Ethnic affiliation.
f) Identify:

[1] Leaders
[2] Trainers
[3] Opportunists
[4] Idealists
[5] Group skills

[6] Specialties
[7] Training
[8] Sniping
[9] Demolition
[10] WMD:

[a] Chemical background
[b] Biologic
[c] Nuclear
[d] Hardened Deeply Buried Engineering skills

g) Surveillance/Reconnaissance
h) Electronic:

[1] Computer background
[2] Telephonic expertise

i) Tactics:

[1] Previous operational experiences & TTP
[2] Methods
[3] Requirements
[4] Supporting documents

j) Describe or template demonstrated terrorist activity to include over time.

D. Determine Threat Courses of Action

1) Id potential targets
2) Template terrorist actions/objectives
3) Template terrorist actions/indicators near target.
4) Template terrorist escape routes.
5) Template or describe support functions.

a) C4I
b) Locations of facilities
c) Logistic support
d) Financial support
e) Training centers and specific job functions.

E. Minimum essentials:

1) Know your terrorists
2) Know how they've conducted previous attacks.

GLOSSARY

Area of interest – Areas in which a terrorist organization plans on conducting operations against its adversary. An area within the area of operation, which terrorist groups focus operations against a specified target region, country, city, region or activity. An Area of Interest may fall within an Area of Operation, but certainly not in all cases for certain groups.

Area of operations - a geographic area from which terrorist organizations and elements coordinate operations, logistics, finance, recruitment, as well as stage, plan and execute missions. These areas, for any terrorist organization, can be thought of as either the operational or strategic areas in which the group operates and conducts the majority of its activity, as well as defining the area in which the group has the largest sympathetic base to support its organization's political goals. Development of terrorist group Area of Operations is best described as those areas the groups primarily operate.

Assumptions - Information used to replace missing facts necessary for command and staff planning, estimating, and decision-making. Assumptions may also be required for facts that change due to the time difference between receipt of the mission and the time of execution, such as threat dispositions. Assumptions should be confirmed or denied by intelligence collection whenever practical.

Avenue of approach - Determine the means through which the group operates, including electronic, telephonic and computer use and techniques, along with complete lists of key personnel, aliases, cover terms, contacts and associations between other terrorist organizations, elements and governments.

Battle damage assessment - The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against an objective or target.

Battlefield Operating System - The major functions performed by the force on the battlefield to successfully execute Army operations in order to accomplish military objectives. BOS forms a framework for examining complex operations in
terms of functional operating systems. The systems include maneuver, fire support, air defense, command and control, intelligence, mobility and survivability, and CSS.

Battle space - Components determined by the maximum capabilities of a unit to acquire and dominate the enemy; includes areas beyond the AO; it varies over time according to how the commander positions his assets. It depends on the command's ability to both acquire and engage targets using its own assets or those of other commands on its behalf.

Capability - The ability to successfully perform an operation or accomplish an objective. The evaluation of capabilities includes an assessment of a force's current situation as well as its organization, doctrine, and normal TTPs. Capabilities are stated in terms of broad COAs and supporting operations. Generally, only capabilities that will influence accomplishment of the friendly command's mission are addressed.

Chemical, Biologic, Radioactive, Nuclear and /or Explosive - Used to denote weapons or operations, which depend on NBC warheads, dispersal devices or agents for their casualty-producing effects; or which protect or defend against, or react to, their use.

Confirmed intelligence - Information or intelligence reported by three independent sources. The test for independence is certainty that the information report of one source was not derived from either of the two other sources, usually resulting in reliance on original reporting. Analytical judgment counts as one source. Ensure that no more than one source is based solely on analytical judgment.

Doctrinal template – ***NOTE***: *Terrorist actions and activities, as of the printing of this document, do not have a recognized or rigid pattern, i.e., there are no known "Doctrinal terrorist templates." This definition is included to show difference between conventional FM 34-130 methodology and that for counter-terrorism.* A model based on postulated threat doctrine. Doctrinal templates illustrate the disposition and

activity of threat forces and assets (HVTs) conducting a particular operation unconstrained by the effects of the battlefield environment. They represent the application of threat doctrine under ideal conditions. Ideally, doctrinal templates depict the threat's normal organization for combat, frontages, depths, boundaries and other control measures, assets available from other commands, objective depths, engagement areas, battle positions, and so forth. Doctrinal templates are usually scaled to allow ready use on a map background. They are one part of a threat model.

Event matrix - A description of the indicators and activity expected to occur in each NAI. It normally cross-references each NAI and indicator with the times they are expected to occur and the COAs they will confirm or deny. There is no prescribed format.

Event template - A guide for collection planning. The event template depicts the NAIs where activity (or its lack) will indicate which COA the threat has adopted.

High-payoff target - Target whose loss contributes to the success of the terrorist COA.

High-value target – Targets, which terrorist organizations select based on their capabilities, intentions and selection criteria. High Value Targets (HVT) for terrorist organizations account for stated goals or objectives and there physical, political, psychological, personal, profit or revenge motives. Example: Al-Qaida selects HVTs based on their stated objective while concentrating selection in the Mid-East, North and East Africa, the United States, Southeast Asia and Russia. Actual target selection is then refined by conducting reconnaissance and surveillance for vulnerabilities at, near or against U.S. Military Facilities (Khobar towers, USS Cole), U.S. Diplomatic facilities (Nairobi and Dar-Es-Salaam embassy bombings, circa 1998), U.S. Diplomats, U.S. businesses and potentially Non-government organizations (NGO).

Indicators - Positive or negative evidence of terrorist activity or any characteristic of the Area of Interest or Named Area of Interest which points toward threat vulnerabilities or the adoption or rejection by the terrorist or organization of a particular mission, or which may influence their selection of a COA. Indicators may result from previous actions or from terrorist failure to take action.

Infiltration lane - A route used by terrorists to infiltrate through or into an Area of Operation, Area of Interest, Named Area of Interest, territory, or country . Movement is usually conducted either individually or more normally in small groups. Terrorists utilize commercial transportation, pay or conduct legal or illegal border crossing operations. Dependent upon operational time line terrorists may attempt legal infiltration, e.g., visas or seek citizen ship to the target AI. Normal infiltration is conducted with forged identification and support documents. Normally, infiltration tactics seek to avoid law enforcement profiling techniques.

Information requirement - An intelligence requirement of lower priority than the PIR of lowest priority.

Intelligence preparation of the battlespace – The systematic, continuous process of analyzing terrorist intentions, capabilities, target criteria and actions in a specific geographic area or on a trans-national basis. IPB is designed to support the staff estimate and military decision-making process. Most intelligence requirements are generated as a result of the IPB process and its interrelation with the decision making process.

Intelligence requirement - A requirement for intelligence to fill a gap in the command's knowledge and understanding of the battlespace or terrorist organizations or individuals. Intelligence requirements are designed to reduce the uncertainties associated with a developing or potential terrorist COA; a change in the COA usually leads to a change in intelligence requirements. Intelligence requirements that support decisions which affect the overall mission accomplishment or terrorist development of targeting intelligence or support activities are designated by the commander as PIR. Less important intelligence requirements are designated as IR.

Last time information of value - The time by which information must be delivered to the requestor in order to provide decision makers with requestor in order to provide decision makers with expected time of a decision anticipated during staff wargaming and planning. If someone other than the decision maker must first process the information, the LTIOV is earlier than the time associated with the decision point. The time difference accounts for delays in processing and communicating the final intelligence to the decision maker.

Lines of communication - All the routes (land, water, and air) that connect an terrorist individual, cell, element or organization with one or more safe sites, mission support centers or sites and along which terrorists move or transfer information, by courier, electronic or telephonic communication, including finances.

Mission, enemy, terrain, troops, and time available - to describe the factors that must be considered during the planning or execution of a tactical operation. Since these factors vary in any given situation, the term "METT-T dependent" is a common way of denoting that the proper approach to a problem in any situation depends on these factors and their interrelationship in that specific situation.

Mobility corridor – Normally a refined avenue of approach or specific line of communication used by a terrorist or execution cell, example, reconnoitering airline flight schedules, times, and either local, trans-continental or oceanic flights, potentially to hijack aircraft. Modern mobility corridors can also include terrorist or narcotic organizations use of specific world wide web, URLs, internet protocols (IP), encryption methods or methods to move large sums of money.

Modified combined obstacle overlay - A product used to depict the battlefield's effects on military operations. It is normally based on a product depicting all obstacles to mobility, modified to also depict the following, which are neither prescriptive nor inclusive.

- Cross-country mobility classifications
- Objectives. or
- AAs and mobility corridors.
- Likely engagement areas or sites (HVT/HPT).
- Key terrain.

Named area of interest – A specific location or area encompassing individual terrorists, cells, or organization mission support centers/sites (example, safe houses), area of activities or targets. NAI are normally developed through fusion of intelligence information, which relates to the terrorists intent to do bodily or physical damage. The primary development of NAI is accomplished during the Courses of Action and Event template/Matrix process.

OCOKA-A

- **Observations**: Activity terrorist undertake to gather information on U.S. personnel, posts, facilities, organizations and businesses. Observations fall under reconnaissance, intelligence, surveillance, and targeting activities (RISTA).
- **Cover/Concealment**: Practices to protect operational personnel who are planning, leading, training, arranging for material delivery and/or coordinating transportation, and financing actions to support anti-U.S. activity. Deception measures are a component of cover and concealment. Covert and overt activity are integrated to mask true intentions and activities.
- **Operations**: Actions undertaken during all phases necessary to conduct a terrorist attack.
- **Key groups, personalities and associations**: Determine the composition, dispositions, strengths, vulnerabilities and methods of operation.
- **Avenues of approach and mobility corridors:** Determine the means through which the group operates, including electronic, telephonic and computer use and techniques, along with complete lists of key personnel, aliases, cover terms, contacts and associations between other terrorist organizations, elements and governments.

- **Activities & actions**: Integrating all knowledge on a group's procedures to know and apply understanding of normal activities. Analyzing actions of a group, cell, persons planning and potentially conducting plans to attack U.S. interests. Based on normal activities a group, cell or persons actions can become indicators, which provide warning of a terrorist attack. Review and overlaying information provided by signals, open source, human sources, and imagery can provide indicators of growing & impending actions. These overlays are situational templates of matrixes that when combined and placed over a U.S. facility may provide the terrorists courses of action (COAs).

Order of battle - Intelligence pertaining to identification, strength, command structure, and disposition of personnel, units, and equipment of terrorists or narcotic individuals, organizations or cartels. The OB factors form the any terrorist or Narco-terrorist force. The OB factors form the framework for analyzing their capabilities, building threat models, and hence developing COA models.

Pattern analysis - Deducing the actions and activities, tactics, techniques and procedures (TTP) of an individual terrorist or organization, through careful observation and evaluation of information and trends it potentially portrays. Pattern analysis leads to the development of threat models and hence to COA. Identified patterns of threat activity can be used as indicators of threat COAs.

Possible - Information or intelligence reported by only one independent source is classified as ***possibly*** true. The test for independence is certainty that the information report of a source was not derived from some other source, usually resulting in reliance on original reporting. A classification of possibly true cannot be based on analytical judgment alone. Analysts commonly refer to a "possibility" as information or event, which is $\leq$ 50 percent chance of truth or potential to occur.

Priority intelligence requirement - An intelligence requirement associated with a potential terrorist or Narco-terrorist action or activity, which affects force protection and friendly commander's capabilities to delay, disrupt, capture, or eliminate a threat. PIR are a subset of intelligence requirements of a higher priority than information requirements. PIR are prioritized among themselves and may change in priority over the course of the operation's conduct. Only the commander designates PIR.

Probable - Information or intelligence reported by two or more independent sources is classified as ***probably*** true. The test for independence is certainty that the information report of one source was not derived from the other source, usually resulting in reliance on original reporting. Analytical judgment counts as one source. Ensure that no more than one source is based solely on analytical judgment. Analysts commonly refer to a "probable" as information or event, which is $\geq$ 51 percent chance of truth or potential to occur.

Reconnaissance - A mission undertaken to obtain information by visual observation, or other detection methods, about the activities and resources of an U.S. national, U.S. military, diplomatic, business or other potential site for terrorist actions. Terrorists normally conduct reconnaissance, intelligence, surveillance and target acquisition to build information on vulnerabilities to personnel or facilities. This information includes collection of regional environmental and atmospheric data around, near and at the potential target location.

Situation template - Depictions of terrorist dispositions, actions and activities based on their TTP and previous operations, and the effects of the battlespace, if terrorists seek to adopt particular COAs. In effect, they are templates depicting a particular operation modified to account for the effects of the battlespace, area of operation, area of interest, environment and the terrorist's current situation (training and experience levels, logistics, finances and dispositions). Normally, the situation template depicts suspected communications, logistic mission support sites, finance data, individuals and cells. Situation templates are one part of a COA model. Models may contain more than one situation template.

Sources of information:

- Open source information (OSINT) – normally, written or visual print media material.

- Human derived intelligence reports (HUMINT) – Information derived from persons or persons who voluntarily provide or surreptitiously gain and pass information to the United States.
- Imagery intelligence (IMINT)
- Measurements and Signatures Intelligence (MASINT)
- Signals intelligence (SIGINT)
- Communications intelligence (COMINT)
- Non-traditional intelligence (NTI) – information gained from live televised information from unmanned aerial vehicles or combat systems, example, AH-64 (Apache) helicopters.

Specific information requirement – Specific information requirements describe the information required to answer all or part of an intelligence requirement. A complete SIR describes the information required, the location where the required information can be collected, and the time during which it can be collected. Generally, each intelligence requirement generates sets of SIRS.

Specific order or request - The order or request that generates planning and execution of a collection mission or analysis of data base information. **SORs sent to subordinate commands are *orders.* SORs sent to other commands are *requests.*** SORs often use system-specific message formats but also include standard military OPORDs and FRAGOs.

Surveillance - The systematic observation of an location or surrounding area by visual, aural, photographic, or other means. Surveillance differs from reconnaissance primarily in duration of the mission.

Synchronization – Normally a matrix depicting terrorist function actions or activities, over time, in relation to friendly collection plans and use of collection systems and capabilities.

Target area of interest - The geographical area where HVTs can be acquired and engaged by friendly forces. Not all TAIs will form part of the friendly COA; only TAIs associated with HPTs are of interest to the staff. These are identified during staff planning and wargaming. Engagement areas plan for the use of all available weapons; a single weapon might engage TAIs.

Terrorist course of action model - A model of one COA available to the threat. It consists of a **graphic depiction** (situation template); a **description** (narrative or matrix); and a **listing of assets** important to the success of the COA (HVTs). The degree of detail in the model depends on available time. Ideally, threat COA models address all terrorist or Narco-terrorist functions. At a minimum, threat COA models address the five standard elements of a COA, i.e., who, what, when, where, why and how.

Threat model - A model of the terrorist/Narco-terrorist organization training, operational experiences and TTP for the conduct of a particular operation. Threat models are based on a study of all available information, structured by the OB factors, of the particular terrorist individual, cell or group under consideration. Ideally, threat models consider all terrorist organizational functions, in detail.

INDEX