UNCLASSIFIED//FOR OFFICIAL USE ONLY

Joint Military Intelligence Training Center

Counterterrorism Analysis: A Primer in the Art and Guerilla Guide for CT Analysts

UNCLASSIFIED//FOR OFFICIAL USE ONLY

COUNTERTERRORISM ANALYSIS: A PRIMER IN THE ART

and

GUERILLA GUIDE FOR CT ANALYSTS

Written by a
Senior Intelligence Analyst for Counterterrorism
Defense Intelligence Agency
Washington, DC

CONTENTS

FOREWORD BY THE AUTHOR

Consumers at all levels of the military and policymaking apparatus sometimes express dissatisfaction with the terrorism-related intelligence they receive. This is partially due to an unfamiliarity and lack of experience with the terrorism problem. The complexities of this field can be vastly underestimated both by intelligence professionals as well as decisionmakers. *Counterterrorism Analysis: A Primer in the Art* seeks to educate consumers and analysts about some of the fundamentals of terrorism analysis. Although written from the perspective of a Defense Intelligence Agency (DIA) counterterrorism analyst who has dealt with the problem since 1992, I hasten to note that it is really a collaborative effort as I have incorporated the wisdom and experience of my DIA colleagues who have collectively worked in the field for decades.

While the *Primer* seeks to communicate the challenges and limitations of counterterrorism analysis to both practitioners and consumers, *Guerilla Guide for CT Analysts* is a much more nuts-and-bolts how-to manual for counterterrorism analysts. Written specifically for new and mid-level analysts from DIA's Joint Intelligence Task Force — Combating Terrorism (JITF-CT), it suggests tips of the trade relevant to any intelligence analyst working in any organization. The *Primer* and the *Guide* are both works in progress, and I welcome any and all comments, insights, and tips-of-the-trade to enhance the usefulness of any future editions. As subsequently noted, no two analysts do their jobs exactly the same way, so as a community it is imperative we share our collective experiences.

Note: Feedback for the author of this publication can be sent to the editor (b)(3):10 USC 424 DIA. Classified questions/comments can be directed via (b)(3):10 USC 424 (b)(3):10 USC 424; (b)(6)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

COUNTERTERRORISM ANALYSIS:

A Primer in the Art

Bottom Line

No model can routinely and reliably predict the details of specific acts of terrorism. Nor can any particular sensor or technology be relied upon to unilaterally obtain details of planned attacks. Successful terrorism analysis requires a person to study data from multiple intelligence disciplines and become intimately familiar with a target terrorist group. An analyst must understand and keep abreast of several aspects of the group, including its history, personalities and ongoing activities. Only in this way will subtle nuances indicate to the careful observer that a group is preparing for a specific operation and provide the best opportunity to disrupt its activities.

Peculiarities of Terrorism Analysis

The Critical One Percent

Over ninety-nine percent of a terrorist group's time is spent tending to mundane logistical issues—resource management, recruiting & moving personnel, procuring false documents and other generic preparations for future activities. These activities are the most vulnerable to detection and exploitation by intelligence since they occur over extended periods of time. The most critical fraction of a terrorist group's overall activities is the one percent of its time spent pursuing a specific terrorist attack. This includes the target selection, pre-operational intelligence collection and the execution of the attack—the activities most diligently protected by a terrorist group. It is this tiny fraction of activity by which the success or failure of counterterrorism efforts are necessarily measured, and against which resources too often are belatedly allocated. Few people remember cells disrupted before their plots are executed or which did not approach operational maturity. For example, many Americans know of the attack on the *USS Cole* in Yemen while few will recall the August 2005 arrest in Turkey of experienced al-Qaida planner Luay Saqa for plotting against cruise ships.

While tactical warning of terrorist attacks will always remain the ultimate goal of terrorism analysis, the practical pursuit of this trophy must not be limited only to the search for obviously threatening indicators. An analyst must look at all observable aspects of the group's activities to find subtle clues about its intentions and capabilities. In this way terrorism analysis strongly parallels tried-and-true wilderness search and rescue practices. Search and rescue specialists are trained NOT to search for lost people, but to search for the *clues* of a lost person. A person walking through the wilderness unavoidably leaves behind a number of signs marking their passage, such as footprints, disturbed brush, dropped clothing and broken branches. Because there are hundreds more clues than a lost person on any given mountainside, they search for the clues and use them to direct resources towards areas with higher probabilities for detecting the ultimate clue, the lost person.

Likewise, as a terrorist group pursues its business, it also leaves behind a number of clues. If detected, these may be tracked in order to learn about a group's intentions and capabilities. Clues can be virtually anything, but obvious examples include:

- Activities and statements of key figures
- Acquisition of safe-houses
- Possession of false documents and arms
- Engaging in suspicious movements

However, while this data is valuable, an analyst must always be aware that many clues of possible attack planning may also dead-end as attacks are abandoned or altered due to unobserved factors. Other clues that may lead to one conclusion at a certain time may mislead the analyst if the entire context is not observed; this may be due to a group having to retrofit operations to meet new conditions or requirements. The net effect is that analysts must never take for granted that any single collector will publish an intelligence report explaining details of a pending terrorist operation in time to disrupt that attack.

Analysts responsible for tactical warning must locate, recognize, and incorporate bits and scraps of data from widely disparate sources as clues to determine when a terrorist group is considering a specific attack. Any warnings will almost always be issued with incomplete information because waiting to articulate a more thorough story may undermine the urgency for notification demanded by a warning problem. On one

hand, you can get the warning out fast and risk being wrong. On the other hand, you can succumb to the natural desire to publish a more accurate product by waiting and gathering more information. However, the potential consequence is failing to warn in a timely manner the likely victims of a pending attack.

Five Rules of Thumb Regarding Terrorism Analysis:

1. Terrorism stems from a combination of complex political phenomenon and personal relationships between atypical personalities. These factors cannot be applied into a reliable predictive model to forecast specific terrorist attacks.

2. Only a small fraction of a terrorist group's time is allocated to preparing specific attacks.

3. Mature terrorist groups are obsessively security conscious. Obtaining precise tactical warning of specific attacks is one of the most challenging missions of the Intelligence Community.

4. Most overt terrorism threats are not credible and originate either from anonymous sources or unscrupulous persons seeking compensation for fabricated or embellished threat information.

5. An analyst must become intimately familiar with as many aspects of a terrorist group as possible to overcome the unfavorable odds for detecting and recognizing pre-operational indicators.

A Unique Analytic Problem

Terrorist groups are complex political entities that do not lend themselves well to predictive modeling, at least at a tactical level. At its core, terrorism analysis is a peculiar combination of political and social networking analysis and the "group" is its basic unit. Whether comprising one member or one thousand, whether it's a formally declared organization or an ad hoc collection of neighborhood misfits, it is the "group" that must be studied as the first level of analysis in order to understand the common motivators and goals that its members have rallied together to pursue. Many pressures affect group activities, including:

- Available resources
- Security environment

- The agendas of benefactors, including state sponsors
- Internal group dynamics

Internal dynamics, the personal relationships between members (especially leaders and operators), are major influences upon group behavior that are easily overlooked. Understanding these intangibles and their impact upon different factions within a group is vital to producing accurate terrorism analysis. However, such detailed information is often lacking.

A terrorist group's behavior often appears wildly erratic to an outside observer and it is not unusual to find yourself presented with several credible yet contradictory reports that demand attention. These discrepancies often are rooted in the fact that terrorist groups are fragile entities, dependent upon obsessive secrecy in all aspects of their daily operations in order to limit penetration and disruption from adversaries. Their vulnerabilities are compounded by necessary participation in peripheral criminal activities and, often, exposure to autocratic governments quick to suppress any perceived disturbance. Only by obsessively adhering to security procedures do terrorist groups protect and maintain their operational capabilities. This compulsive secrecy creates significant intelligence challenges for terrorism analysts, generating many more variables than some more traditional military intelligence problems such as order-of-battle analysis. In practice, terrorism analysts will be aware of only a few of the many specific pressures influencing a group. Even this understanding, however, will have limited depth for several reasons: limits of collection assets, multiple duties competing for analysts' time and attention, and competing demands upon collectors in the field.

Terrorism Analysis vs. Military Analysis

To contrast terrorism analysis with traditional military analysis, consider the summer of 1990 when Iraq threatened the Kuwaiti border. Iraq's hostile rhetoric towards Kuwait and reliable accounts of military exercises near the common border were well-documented in open sources. Concerned about a potential crisis that would affect the world's economy, decisionmakers sought to confirm the threat through other intelligence methods before committing valuable resources to counter a possibly non-existent emergency. In a matter of hours, reconnaissance aircraft and other sensors unequivocally confirmed that Iraqi military units were absent from garrisons, present in border regions or in transit between unknown locations. Such data confirmed the potential for an invasion, even if it could not confirm an invasion in progress. Decisionmakers now had a wealth of hard data to supplement intelligence assessments of Baghdad's intentions with which to make informed policy decisions regarding the crisis.

In a hypothetical terrorism scenario which frequently parallels reality, a walk-in source with no prior intelligence record approaches a U.S. Embassy with sensational threat information. He alleges to have overheard five unidentified people in a coffee shop discussing plans to attack an unspecified U.S. interest in the country. The source doesn't know when or how but wants financial compensation or assistance to obtain U.S. visas for his family in exchange for a promise to return later with more details, saying that he sometimes sees these people in his daily routines. Since this is a serious allegation, analysts would want to seek confirmation of the threat and would review other data in search of information that could corroborate elements of the report. In all likelihood this will prove impossible. There simply is no way to develop "positive intelligence" to confirm or disprove vague information from an anonymous source. This scenario actually plays out many times each year at U.S. government facilities around the world. Whenever threat information is reported it is the duty of intelligence analysts to assess the information in support of decisionmakers and people potentially at risk. An analyst will compare information provided on the threat with an existing knowledge base to attempt to determine its credibility. Often, credibility cannot be conclusively determined, particularly where few details are available.

Terrorism Analysis vs. Military Analysis (Continued)

In the end, policymakers may have to decide whether and how to react to this threat based not on facts, but on their degree of confidence in information generated by an unknown entity (the source) and assessed by an analyst whose foremost desire is to keep the policymaker well informed. One would hope that the supporting analysts will be willing to offer honest, educated opinions even at the risk of being wrong.

Tactical Warning

Tactical warning, the ultimate goal of terrorism analysis, ideally seeks to determine the following specifics about a terrorist attack before it occurs:

- Target
- Location
- Time
- Method of attack
- Group identity, hopefully including specific operatives by name and description

The absence of any of these factors creates uncertainties that impede the ability of security forces to respond effectively to a credible threat.

From a terrorist's perspective, a successful attack ultimately requires the group to match its capabilities against a perceived weakness in the target at a time when the group is motivated to risk some of its assets in an operation. This is inherently an imprecise, non-mathematical formula which may be thought of as: "Terrorist Capabilities vs Target Weaknesses" and "Motivation vs Risk Acceptance." A successful warning should, at a minimum, force a prospective terrorist to recalculate this formula by prompting unanticipated defensive measures at the target site. Frustration from setbacks in any component of the plot alters the formula and may lead to a postponement or deflection to a softer target at a later date. Mature groups dedicated to attacking a particular target may use the extra time imposed by the postponement to enhance existing capabilities and/or seek out new weaknesses in the same target rather than deflect to a new location. A delay by the group also allows,

however, more time for intelligence and counterterrorism operations to identify and negate the threat.

In practice, providing tactical warning for specific terrorist attacks is one of the most challenging missions of the U.S. Intelligence Community. The most obvious avenue to attain tactical warning is to penetrate key terrorist figures with a reliable intelligence asset, but penetration of a terrorist group can never be expected or taken for granted. Attack planning by mature organizations is almost always compartmented to such an extent that few group members, including operatives, will be aware of all (or any) of the details. Recall that many of the 9/11 hijackers were unaware of the ultimate nature of the attack they were executing. Hence, collectors must not only penetrate a terrorist group, they must penetrate the relevant cliques within the group that are knowledgeable about the plot. This must be accomplished by the time the plot is being consolidated in order for intelligence to provide actionable information to consumers in time to make a difference. Even if tactical warning is attained, terrorists can simply postpone an attack if the warning impedes their plan. An important point to remember—by their very nature terrorists carry the initiative and governments are reactive. Paraphrasing an observation by the Provisional Irish Republican Army following the nearly successful murders of the British Prime Minister and Cabinet in 1984, "We must be lucky only once. You must be lucky always."

Sources

Human intelligence sources generally run the spectrum of credibility from fabricators to knowledgeable informants with established access to sensitive information. As a general rule, fabricators provide alarmist threat information seeking short-term personal gain, while credible or partially credible sources report on more routine (but no less important) aspects of terrorist group activity. Unfortunately, few sources with established credibility report on terrorism issues and even fewer sources with no established credentials pass information worthy of exploitation. Additionally, when a source with excellent access is recruited, information from his reports may become heavily redacted or restricted from dissemination from a majority of analysts in the intelligence community in order to protect that source from compromise. Most threat reports come from untested sources, many of whom are fabricators seeking compensation for allegedly imminent threat information. Fabricators rely on their creativity and government anxiety to convince officials of

their value. Critical questioning of sources usually exposes fabricators, though raw reports containing their threat information are published routinely as a matter of government policy to ensure a thorough dissemination of threat information to potentially affected parties. Another category of source includes those with legitimate access to information of limited value but who tend to exaggerate or fabricate material when they have little authentic data to report. These are harder to discredit often because they may even pass polygraphs because the kernel of info they offer is true.

Generally the number of raw reports reflecting flawed terrorism intelligence vastly outnumbers credible reports, and rarely does a single credible intelligence report portray an entire story. Consumers of intelligence should not fret excessively from alarmist reports, but should rely on their analysts as filters to alert them to credible threats. Analysts, for their part, should network with experienced and knowledgeable counterparts from around the intelligence community to compensate for any lack of depth on unfamiliar topics. Consumers may further cope with uncertainty by learning to differentiate between the different types of threat products described below.

Practical Rules of Threat Analysis

Given the diversity of terrorism intelligence requirements and the widely disparate types of reporting available from group to group, there can be no single methodology that will lead to a full understanding of information contained in intelligence reports. There are, however, some general guidelines that will help analysts place their assessments in a meaningful context. In analyzing a terrorist group or a terrorist scenario, step one is to consider the following threat assessment factors:

- Activity/History
- Anti-U.S. Intentions
- Capabilities
- Enhancing or mollifying factors evident in the Operational Environment
  - **Activity/History:** What terrorist attacks has the group conducted? How can you categorize their targets? (By nationality, religion, ethnic group, etc?) What is the group's "range" in terms of presence and operational activity? Do they confine attacks to a particular country or region? Do they have support or political elements resident in countries where they decline to conduct lethal attacks? Do they have a history of working closely with other important political entities (state sponsors, indigenous political parties, other terrorist groups)? Do they have any historic or ongoing conflicts with these or other entities?
  - **Anti-U.S. Intentions:** Can the group credibly be shown to harbor anti-U.S. sentiments? Is their degree of hostility towards the U.S. simply rhetorical or are group leaders motivated to physically attack U.S. interests? Is the group sufficiently organized to be a threat or are they too paralyzed by infighting to muster a coherent operation even if they all cheer the idea of anti-U.S. operations?
  - **Capabilities:** Provided that a group intends to attack U.S. interests, what options are available? Does the group have the resources and expertise to construct improvised explosive devices? If so, what is the scale and quality of a likely device? To what degree can a group penetrate protected facilities? Is the group limited to attacking targets of opportunity in public venues with simple small arms?
  - **Operating Environment:** Are there any factors unique to an area of operations that affect a group as it moves towards a terrorist attack? Do they enhance or impede the group's progress? Is the group known to host-nation security services? To what degree is the host nation responsive to the threat? How tolerant is the host nation? Are there other political factors that influence a group's motivation or timing with regard to preparing an attack? If a related cell was disrupted in a neighboring state, will that impede or accelerate the plans of remaining cells?

These factors are deliberately drawn from the Department of Defense's cornerstone document of terrorism analysis, DoD Directive 2000.12, which guides Defense analysts to assess a relative threat environment for anti-U.S. terrorism in every country. *(DoD Antiterrorism (AT) Program, Number 2000.12, August 18, 2003)* These criteria are not conclusive, but serve as a starting point to begin a comprehensive analysis of all available information related to a potential terrorist threat. Since the number of variables affecting terrorist groups and their actions are vast, a practical framework is needed for evaluating a potential terrorist threat when specific intelligence is unavailable. Once

the threat is broadly defined, analysts have a foundation from which to build a comprehensive analysis, focusing on the unique characteristics, capabilities and nuances of threatening groups which will eventually facilitate tactical analysis and warning.

An analyst's ability to provide useful warning will ultimately depend on their ability to understand and place into context myriad subtle details of a developing threat. Comprehensive Threat Analysis involves the interpretation of fragmentary, often obscure information in order to detect, recognize and understand the pre-incident indicators of an impending terrorist attack and to provide timely warning. The challenge to the analyst is to put confusing, incomplete, and superficially irrelevant information into context.

In order to put Comprehensive Threat Analysis into practice an analyst must become intimately familiar with all information available about individual terrorist groups and closely monitor the groups for new developments. The type, volume and quality of information available for study varies radically from group to group, so no two group assessments are likely to be developed the same way. An analyst's ability to develop reliable products depends upon a tremendous investment of time and effort by the Intelligence Community in order to establish appropriate collection and analytic programs from which analysts can build a knowledge base. Once a comprehensive knowledge base is established, analysts will be able to respond to a crisis quickly with the most current information, provided that the knowledge base is maintained. By contrast, the instinctive reaction of throwing untrained personnel to a terrorism problem in the aftermath of an incident tends to bog the process down in a reactive cycle. Here, the elevated operational tempo of a crisis combined with a relative lack of expertise in the workforce creates an environment where relevant but obscure intelligence is buried beneath superficially alarming but non-credible threats. The heightened collection profile and lower standards of reporting which follow high-profile terrorist incidents tend to overwhelm resources by creating more documents through which to sift, with a signal-to-noise ratio heavily weighted towards noise.

Terrorism analysis is a continuous crisis effort that defies substantial improvement with belated and temporary surges of resources in a post-incident environment. Unlike conventional political-military crises

around which intelligence task forces often are built, terrorism crises materialize and pass quickly due to the very different types of indicators available for the Indications and Warning mission. In a terrorism crisis, the documented movements of armor formations and cat-and-mouse deployments of surface-to-air missile sites are simply irrelevant. Many mature terrorist groups already have resources available to conduct an attack at a time of their choosing. Once an incident occurs, the brunt of the remaining work is investigative, supported by intelligence. Meanwhile intelligence officers must be forward-looking to make the best estimate of responsibility, re-assess the terrorists' capabilities, and attempt to anticipate their next actions. The bane of the counterterrorism analyst is that pre-incident indicators too often become apparent in hindsight through the reconstruction phase of a post-incident environment.

The only silver lining to this cold fact is that such information contributes to the knowledge base for detecting future preoperational indicators. In an ideal world, allocation of adequate resources on a routine basis will ensure the best possible knowledge base for reference following an incident. Information is then quickly available for comparison against data derived from the incident, providing timely support to investigators and other analysts whose duty is to identify for policy-makers the most likely suspects, any remaining threats to national interests, and terrorist resources which may be vulnerable to counterforce. Failure to pre-empt an incident should not be compounded by obsessing on the aftermath. Excessively diverting resources to an examination of the past dilutes the process and diverts the attention of intelligence officers from other evolving threats.

Terrorism Products

Raw or Unevaluated Intelligence Reports

Raw intelligence reports (labeled in some channels as "unevaluated") are the most common terrorism product from the IC since threats and data are reported daily and in volume in intelligence channels. Raw reporting represents data — fundamental bits of information — collected by an intelligence collector that may or may not have been "processed" or altered to conform to a specific format to facilitate the ability of analysts to read or otherwise manipulate the data. They often are misleadingly called "intelligence reports" as a term of art if they were collected through an asset owned by an intelligence organization; however it is

important to distinguish that these reports are not evaluated for the accuracy of content or other intelligence value before they are published and do not represent analytic judgments of the source agency. Such assessments would be published as "finished intelligence." This fact is easily confused by the media and others unfamiliar with the nuts and bolts machinery of routine intelligence processes.

Fortunately, the vast majority of HUMINT-based threats are fabricated. A trained, experienced analyst can usually weed-out such items. Consumers must keep in mind that raw threat reports are exactly that — raw, unevaluated reports. Terrorism watch officers know that they must learn to quickly identify and debunk non-credible threat reports to prevent overreaction from consumers. Uninformed consumers often consider a threat credible simply because it originated from within intelligence channels. As with any intelligence report, threats must be subjected to critical analysis, gauged for consistency, and evaluated against an existing body of knowledge. While this can be a lengthy process, an experienced analyst will be able within a few minutes to assess whether the report is fabricated, credible, or plausible. Credible and plausible reports warrant more thorough analysis, which will take time to process through research and collaboration with other intelligence officers. This unavoidably forces the production of finished assessments to lag behind the raw threat information, though the raw information usually is disseminated to all concerned parties simultaneously to ensure maximum awareness of the data.

History shows that intelligence reporting of pre-operational activity prior to an attack often afforded only limited insight into the operation. Such reporting usually trickles-in over time and is loaded with ambiguous references. Sometimes analysts determine that a group is involved in some type of unusual suspicious activity (as opposed to their usual suspicious activities), but the determination of targets, timing, or venues of attack may not be possible with available information at critical junctures. It is difficult to warn based on such reports, which appear vague and circumstantial, though the counterterrorism community will internally discuss these issues and apprise consumers of its thoughts and the existing body of knowledge regarding the apparent threat. The job of an analyst is to compile as much available information as possible from the raw reports and estimate its meaning.

Threat Awareness Products

This is a broad category that encompasses the bulk of finished intelligence on terrorism. Threat awareness products may include but are not limited to:

- Written assessments for specific threats
- Reference products on terrorist groups
- Assessments of potential threats in a given country
- Special reports on developing issues or trends
- Assessments of recent, individual raw reports.

Current assessments — those published newspaper-style on a daily basis — are the most important products for consumers responsible for assets potentially at risk for terrorism, since they document current terrorism trends and provide credibility assessments for routine threat reports. Baseline reference products are invaluable for helping customers acquire a detailed understanding of important issues or trends and placing into context current intelligence assessments that are necessarily more limited in scope.

Threat level assessments for specific countries are maintained by the Departments of State and Defense. However, the State and Defense systems are separate and distinct, focusing on different criteria for different audiences. The State Department's system is administered by the Bureau of Diplomatic Security's Office of Intelligence and Threat Analysis (DS/DSS/ITA) in the form of the Biannual Security Environment Threat List (SETL). The SETL has six threat categories spanning a wider range of potential threats to U.S. interests than just terrorism. Of the six categories, three directly relate to different aspects of the terrorism problem in a country. State Department assessments are assigned to specific diplomatic facilities, leading in some cases to multiple threat levels within a given country if there are multiple posts.

The Department of Defense system, by contrast, is mandated by DoD Directive 2000.12, and focuses exclusively on terrorism, assigning a single threat level to each country. The purpose of the DoD methodology is to offer a short, clear description of the relative threat to U.S. military interests in a given country by terrorists in that particular environment in support of the vast number of military personnel and assets

that travel, often unexpectedly and on short notice, to unfamiliar countries. The DoD threat system authorizes only the Defense Intelligence Agency (DIA) to establish country threat levels.

Threat Warning Products

Three warning systems co-exist in the terrorism community, one representing the voice of the Intelligence Community, another maintained by the Department of Defense and a third maintained by the Department of Homeland Security. The Intelligence Community system is managed by the Interagency Intelligence Committee on Terrorism (IICT) within the National Counterterrorism Center (NCTC) and offers two warning products, Terrorism Threat Alerts and Terrorist Threat Advisories. The only warning product of the Defense warning system is the Defense Terrorism Warning Report (DTWR) which may be issued unilaterally by DIA and/or any Combatant Command. Every effort is made in these cases to issue one report co-authored by DIA and all affected commands, though this is not a requirement. Defense Terrorism Threat Awareness Messages (DTAM) are also part of the DoD system and serve to call attention to important terrorism trends that may affect force protection.

Products issued by a Defense author will reflect only the opinion of that agency or command on a particular issue and can be published within hours of the receipt of threat information. Products published by the IICT reflect the coordinated opinion of CIA, DIA, NSA, State Department, DHS, FBI, and the NCTC (known colloquially as the Warn Seven). All warning products aim to alert consumers at multiple levels of government to the likelihood of near-term terrorism, along with a description of its expected characteristics.

Consumers must be careful to note the origin and substance of any warning product they receive and determine its value as it pertains to their own mission or area of interest. It is not unusual for national-level agencies to disagree on the need for a warning product or for some agencies to lag in the warning process. Warning is considered a serious issue requiring a deliberate process and not all agencies achieve confidence in threat information at the same time, if at all.

Beyond Analysis—Perspectives on Related Terrorism Issues

The Paradox of Warning

What if a warning report is issued and a terrorist attack doesn't occur? Does this mean that reaction to the warning (enhanced security, proactive arrests, etc.) disrupted the threat? Or does it mean that the threat information was inaccurate? This is the "paradox of warning." Warning reports are not issued whimsically in the Intelligence Community and history clearly shows that the failure of an attack to materialize does not necessarily mean that the threat didn't exist. Terrorists plotting to conduct attacks are vigilant and may have altered their planning as a result of the target's increased security awareness, hopefully oblivious to the compromise of their operation. Other times, terrorists will not meet their own timetables and thus be forced into a delay. There are also times when warnings will be issued based upon inaccurate or even unevaluated intelligence. These incidents are regrettable but inevitable in this business of predicting the future with no time to spare.

Limits of Counterforce

Policymakers will often consider options for combating a terrorism enemy or resolving a crisis through the use of deadly force, either through police/security actions or military engagements. Many factors will weigh in their calculation of this option that analysts should be aware of and be prepared to address in the course of supporting that executive. Broadly, policymakers must weigh, on a case-by-case basis, the expected material and political benefits of a counterforce option against the potential costs before authorizing any use of force.

Counterforce falls into two categories: Reflexive and Elective. Reflexive counterforce addresses attempts to resolve current, ongoing emergencies, such as a hijacking. Elective counterforce applies to pre-emptive or retaliatory attacks against terrorist personalities or infrastructure where the decision-maker has the luxury of time to thoroughly consider policy options. Reflexive counterforce always has merit as an option for ending an emergency situation. However, the issue of elective operations is far more complicated, especially outside of established war zones like Iraq and Afghanistan, and any benefits will depend upon factors unique to a given situation. For example, unilaterally striking

suspected al-Qaida targets in Europe, Russia or Egypt would each carry unique consequences that are far more significant than striking similar targets in Afghanistan or on the open ocean. Terrorist facilities such as training sites and headquarters are attractive targets because, once located, they are stationary and accessible over time from the perspective of a targeteer. Tracking individuals, by contrast, is far more valuable but much more difficult and presents more complicated political questions for policymakers.

The overarching problem with targeting any terrorist group for counterforce is that it rarely can be done comprehensively. There is precedent for small groups to be defeated by sweeping arrests, such as the Combatant Communist Cells in Belgium or the Red Brigades in Italy, but large, mature organizations have learned from experience to diversify and disperse their resources in order to be resilient. Infrastructure can include front companies, political offices and cells in various countries, private homes, safehouses, and even government buildings. Destroying an office or a training site may kill a handful of prospective terrorists, deny the use of infrastructure and destroy some materials, but the overall organization remains intact. Facilities are easily reacquired, usually with an increased appreciation for security awareness. Their physical location in sovereign states presents another limiting factor. The deaths of key leaders can hinder an organization, though larger groups reconstitute quickly unless continuously attrited or unless high value people are lost. Targeting exposed terrorist infrastructure may seem logical in a campaign of attacks against the whole organization, but token retaliations may merely sting a group, producing few lasting material effects. On the other hand, striking a small subset of terrorist operatives may pay huge dividends if the action disrupts or delays the planning or execution of a terrorist attack. Another paradox of counterforce is that striking often makes the group more difficult to monitor for the purposes of Indications and Warning as security consciousness increases.

Counterforce often has merit, but it is not a panacea. No terrorist group has yet been intimidated into submission by a counterforce threat. In many circumstances, benefits will be political, not material. Success in material terms is often temporary and should be measured with a realistic estimate of the time the group will take to recover. Success may also be measured in expertise or other limited resources that are suddenly denied to the group. Some groups, such as al-Qaida and its

affiliates, are effectively on a war footing; they aggressively pursue attacks and are willing to receive heavy casualties in the process. These groups leave their opponents little choice but to respond with counterforce whenever circumstances permit. Other groups represent serious, but dormant threats which may be addressed more effectively thorough means other than counterforce. The threat of military force may be most effective against state-sponsors of terrorism rather than against terrorist groups, since states have many more valued resources to protect than do groups. Libyan support for international terrorism plummeted following the imposition of political and economic sanctions by the United Nations in 1991 in reaction to Libya's involvement in the bombings of Pan Am Flight 103 in 1988 and UTA 772 in 1989. By contrast, U.S. airstrikes in 1986 prompted by Libyan-sponsored anti-U.S. attacks failed to intimidate Libya from bombing these airliners. These very different reactions by the Libyan government to different policy measures demonstrate that any state may react uniquely and unpredictably to terrorism policy measures, particularly counterforce.

Conclusion

Terrorist groups represent unique and complex threats to our society. The demands upon those committed to understanding and undermining these groups are equally complex. Analysts must become intimately familiar with a multitude of political, environmental and personal factors in support of customers potentially at risk and policymakers responsible for countering the threat. Thorough, sustained intelligence efforts are needed in order to develop this information, communicate it to customers and create for ourselves the best possible opportunities to counter terrorist threats. A customer base knowledgeable about both the intelligence community and the nature of our terrorist enemies is equally important to maintaining the flexibility, agility and effectiveness of our government. Hopefully this guide will serve to advance many of these ideals and serve as a basis to invite additional constructive discussion among and between intelligence customers and our community of professional intelligence officers.

GUERILLA GUIDE FOR CT ANALYSTS

At some point after arriving at your new job as a terrorism analyst, you'll notice a flurry of inexplicable activities by analysts around you and probably think, "Just what am I supposed to be doing here? What does a terrorism analyst do?" This guide should help you get started.

There's no way to get around the fact that terrorism analysis is a difficult vocation with a steep learning curve. Frustration is part of the territory, especially early in your career. Worse, no two analysts will do their jobs exactly the same way so you can't precisely model another analyst and expect the same degree of success. This guide should help you focus on your goals and provide a framework to attack that learning curve.

Mission

The core of your job is to:

- Learn about terrorist threats to U.S. interests
- Communicate that threat to customers

Other activities (training, liaison, directing collection, etc.) should either contribute to those missions or enhance your skills relative to those missions.

Additionally, from an organizational perspective, as a new analyst you'll be learning:

- The Intelligence Community (IC) and intelligence processes
- DIA/JITF-CT's role in the national-level Intelligence Community
- DIA's role in the military community
- The substance of your specific terrorism "accounts"

This text will only directly discuss how to approach the last bullet in detail. The others will be addressed academically in the Counterterrorism Analyst Course (CAC), the Advanced Counterterrorism Analyst Course (ACAC), and the many general analyst courses provided by DIA. Coursework aside, pay attention to events that will occur around

you, such as coordination of Community assessments and discussions about analytic topics such as warning. Observe the processes and ask questions.

Learning the Threat

At some point after you arrive, you will be given one or more "accounts" to follow. These typically consist of countries and/or terrorist groups, usually with a logical overlap.

Most of your mechanical duties are to:

- Maintain and create database records relevant to your accounts, including:
  - country profiles
  - group profiles
  - biographies
  - event profiles
- Draft original assessments of varying lengths such as Response Memos, J2 desknotes, CJCS briefing slides and JITF-CT's flagship product, the Defense Analysis Report-Terrorism (DART).
- Draft and present briefings to a variety of specialized target audiences ranging from Cabinet Secretaries to military police units.

However, your *foremost goal as a terrorism analyst* is to develop the ability to detect and recognize (two distinct processes) when your terrorist groups are preparing for an attack, communicate that information to affected parties and do so in enough detail that protective measures may be enacted to disrupt the attack in a timely manner. This process is called Indications and Warning and it is the single most important duty of every terrorism analyst.

Your ability to detect a warning condition is derived directly from your ability to learn everything you can about the terrorist groups you follow. Similarly, your customers' ability to react appropriately to a warning will be enhanced by your efforts to educate them through various types of intelligence products. Even for a small terrorist group, this is a great challenge, so you must prioritize. Your senior analyst can

provide specific guidance but the following general guidelines can give you a head start:

- List your assigned terrorist groups and those present in your countries
- Identify (with your peers) groups that are operationally active, logistically active, dormant, and defunct
- Determine which active groups have anti-U.S. intentions or have the obvious potential to adopt an anti-U.S. posture
- Prioritize operationally active anti-U.S. groups over all others, followed by operationally active groups that have the potential to adopt an anti-U.S. posture; dormant groups rank last

After prioritizing, learn the following basics for each group:

- Ideology and goals
- Operational history (study the attacks they have conducted)
- Group structure (political and operational architecture, cell locations & activities, other wings, factions, etc.)
- Leadership structure (overall leader, councils, officers, etc.)
- Capabilities (can they build bombs, operate transnationally, etc.)

Most of this information will be easy to obtain but may take a while to digest. In the end it will give you a basic roadmap to understanding relevant terrorist groups. Much of this information is already available in the database files you're now responsible for maintaining and in previously published assessments. However, you also need to conduct original research using your classified message handler (eg, WISE). Doing so will allow you to become familiar with the range and varying types of information that are available about these groups and get you started in following them from a current, operational perspective. Ultimately, you will likely tune in to the personalities and social dynamics of the membership of a terrorist group to stay on top of current developments—social network analysis. All terrorist groups, including state sponsors, plan and execute their activities through people who must make and act upon a long chain of decisions before an activity occurs.

Once your highest priority groups are identified and understood on a casual level, you'll gradually subject them to greater degrees of scrutiny in order to obtain a 'high-resolution' understanding of your targets.

Here you'll try to learn about and document as much (relevant) detailed information as possible on your groups. There's no limit to the types of data this may include, for every group is different in terms of the body of information available for explication. Types of data valuable for understanding one group may be meaningless or unavailable with regard to understanding others. Aided by your senior analysts, you'll have to determine which data are worth digging into and which ones are "white noise."

Regardless of the group you study the single most revealing aspect of any terrorist group are the personalities of individual members, particularly leaders. If you can accurately track a group on this level you will be well-positioned to perform any intelligence activity related to that group from writing assessments to directing collection and detecting pre-operational activities. After identifying the people worth monitoring, a representative list of requirements would be to determine for each significant figure:

- Character/personality (to include ideological beliefs)
- Personal data (birth date, passport number, distinguishing characteristics, etc.)
- Addresses
- Phone numbers
- Feuds, antagonisms, and personal enemies
- Leadership qualities
- Identities of family members
- Identities of close advisors/associates
- Formative experiences (i.e. previous experience fighting in Bosnia, living in Europe, etc.)

Developing and maintaining a depth of knowledge at this microscopic level will yield huge rewards. The reason is simple, but not obvious: Terrorist groups are complex organizations subject to a variety of pressures and influences. They also are obsessive about operational security, severely limiting the information that will be available to intelligence officers seeking to counter their activities. Ultimately, any terrorists' "go/no-go" decision whether to pursue an attack will be determined by the actions, reactions and decisions of a handful of individuals who may not behave according to a superficially recognizable logic. Only by

becoming intimately familiar with all observable aspects of a terrorist group will an analyst have a reasonable chance to detect and recognize indications of pre-operational activity in time to issue a meaningful warning, or to recognize new trends worthy of documentation in other intelligence products. Understanding your group's personalities will yield the bulk of this capability.

Terrorism Analysis: Building an Analytic Argument

1. **Establish a baseline assessment:** What do we know is going on, what do we think is going on, and what don't we know that we need to figure out?

2. **Vet new information for consistency with the baseline.** Is it in the ballpark of the baseline? Does it say the same thing or does it reveal new developments? Does it add new details about something we already know? Does it say something outlandish or contradictory to reports from more reliable sources?

3. **Revise your baseline as necessary to accommodate new information.** If there's contradictory reporting of equally good quality, acknowledge this and explore ways it might be reconciled. If there are no good sources or reports with which to establish a reliable baseline, acknowledge the weakness of the reporting and make your best estimate.

4. **Follow-up information gaps as they become apparent.** Learn about and task your collection resources as appropriate across the IC to generate new information. Work closely with collectors whenever possible to help them help you. Never forget that collectors work for YOU, the analyst, but they rarely will have your depth of knowledge on the target.

Analytic Rigor

Critical Evaluation is the process of:

- Intensively studying raw intelligence reports, taking into consideration the source and substance of the reporting
- Weighing the information against other bodies of information (concrete, alleged and provisional)
- Assigning to this reporting an assessment of its intelligence value.

If aspects are sufficiently credible or are of high visibility, standing

assessments may need to be updated to address the new information.

Source Considerations include its access to sensitive information (claimed & real) and the frequency and means through which this information changed hands before being "collected" by an intelligence mechanism. The name of the source, in the case of human intelligence (HUMINT), often is less critical than details about their placement unless it is a person whose roles and relationships are influential to the issues being reported upon. Analysts may ask:

- Is the source a HUMINT or SIGINT asset?
- If HUMINT, does he claim first-hand access to the information?
- Did he learn through intermediaries (2nd & 3rd hand access)?
- Who were the intermediaries and why should they be considered authoritative?
- Is the source a witting asset who knows the U.S. government is the recipient?
- Does the source have an obvious motivation to 'spin' the reporting to their own benefit?
- If SIGINT, exactly who are the parties that are communicating?
- Why are they important?
- What is the relationship between the parties communicating?
- Do they, or should they, have authentic access to the information being reported?
- Is one party trying to influence another?

Substance Considerations:

- How does this information fit with established facts, established assessments and reporting you consider unreliable but are nevertheless maintaining an awareness of?
- Is there contradictory reporting from a source with more authentic access and assessed veracity?
- Is there a chance that dramatic information legitimately represents a sudden shift deserving of immediate attention from policymakers and intelligence collectors?
- Should such a shift be observable via another mechanism?
- Is the information so far removed from established fact that the source is discredited without needing any further knowledge of its particulars?

- In the reporting, does the source distinguish between information he has observed, obtained circuitously, obtained through cultural/ common knowledge, and judgments based on its personal evaluations?

Projected Outcomes:

- The information is demonstrably false
- It's too shaky to be trusted
- Contains elements of truth but aspects are suspect
- Contains elements of truth and aspects are uncertain
- Contains elements of truth and aspects seem likely
- Authentic—source clearly has access to data

Question to Self: To what extent will I risk my credibility by embracing this report? Analysts may feel pressure to balance two risks, neither of which serves our customers:

- Being too willing to accept reports at face value; "Chicken Little" syndrome that disaster is always about to strike;
- Being too cautious to recognize and report on a changing situation; being reactive vs predictive

Resolution: Critical evaluation of data and precise descriptions to self and to customers eliminates 90% of this dilemma.

How Good is Good Enough? It likely will be impossible to convince all customers of any given assessment. Even when presented with an overwhelming body of credible data that is consistent with itself on several levels, some people will refuse to be convinced for various reasons. Always consider thoughtful feedback, but remember that you are responsible for the quality of your product, not any of your customers. The nature of our job often puts us in the position of delivering unwelcome news and we must not flinch from that responsibility.

Evaluating an Intelligence Report

1. Scan the report: Does this report say something interesting, sensational or irresponsible that invites attention?

2. Check out the source: Is there reason to suspect he may be credible/non-credible? Might he have access to the sensitive data reported?

3. Read the details: Does the report still warrant scrutiny? If true, could it warrant a change to a baseline assessment?

4. Go deep: Carefully scrutinize all relevant aspects of the report. Find out details about the source and his previous reporting; research and fact-check key elements of the report looking for authoritatively corroborating or refuting information. Brainstorm the implications if the information is true.

5. Consider for finished production. For credible reports, update baseline data via published intelligence products. Tweak collection informally and via IIR evals, etc. For non-credible reports, place allegations into context compared with assessments built upon more reliable data.

Communicating the Threat

The most elegant analysis is useless unless the right details are passed to the right people in time to make a difference. At DIA your customer base will vary widely. You will write papers read by the National Security Council, brief Ambassadors, answer pointed questions from frustrated and deeply-concerned General Officers, and dialog with soldiers responsible for protecting deployed personnel and overseas installations.

Serving such a wide variety of specialized audiences places special demands on you as an analyst since you'll have to learn to communicate at different levels. For example, senior executives require briefs that go directly to the point and address the "so what" factor without hedging. Products written for other analysts tend to fall on the other extreme, requiring well-constructed, logical arguments that are also well-documented. Consumers at other levels may not know exactly what they want other than having all available information addressed, with an emphasis on "all." Most audiences fall somewhere in the middle.

Finding the balance for each product and audience is an ongoing process which you'll learn by trial-and-error as guidance is provided by

your management and peers. Pride of authorship is a non-existent luxury in the intelligence world. Learn to expect massive revisions of your drafts and understand that every analyst, no matter how senior, always coordinates their products with other relevant analysts and offices, usually improving the product in the process.

Peer Review

As important as it is to coordinate your finished products and seek the opinions of your peers, there will be many times when parties sharply disagree. This is fairly common so you'll need to develop a thick skin, an ability to tactfully discuss differences of opinion with others and a sense of when such disputes are truly important. Analysts tend to debate the meaning of inconclusive data, sometimes with strong opinions that may not necessarily be relevant to the overall bottom line of an assessment. Don't get lost arguing about minor points, keep your focus on the bigger picture. Also, keep an open mind- your colleagues may actually have a point. Your senior analyst will guide you through those occasions, though in general, they should reflect a healthy atmosphere of critical thinking and debate. As much as possible, keep the discussion about the specific language used in a draft assessment or about concepts the language is attempting to describe. In the debate, avoid personally loaded terms such as, "You say here that..." or "I don't agree with you that...". Rather, use phrases addressing wording or concepts such as, "I'm concerned that this language is misleading due to..." or "I'm not convinced of the concept that..." Try to think in precise, even scientific terms about draft assessments, to reduce as much as possible the potential for unrecognized biases between parties to create false differences in understanding of draft language.

In the vast majority of disagreements, careful compromises in wording will usually allow you to carry your point while satisfying the concerns of opposing viewpoints. There may be times, however, when you are confident of language in a particular assessment but find few colleagues to endorse your conclusions. It then will be the job of senior analysts in your chain of command to study the issue, weigh the importance and potential impact of proposed language and establish an office position. Remember, your products reflect not only your individual opinion but also that of the Agency. DIA's credibility suffers whenever individual analysts take a publicized fall. Ultimately, the Senior Defense

Intelligence Analyst for Combating Terrorism will resolve any serious disputes and decide the JITF-CT position.

With these cautions in mind, do not let the process intimidate you when your thoroughly researched and well-articulated assessments place you in conflict with colleagues from DIA or other agencies. Outstanding analysts are not content to simply repeat information fed by intelligence reports in their assessments. Rather they will gauge each report by its content and the credibility of each source, then weave the entire body (sometimes dozens of reports of varying quality) into a coherent, meaningful assessment. Remember that few of your peers will share your comprehensive understanding of your target. Ultimately you may have to decide whether you want to "go out on that analytic limb" over a controversial topic or temper strong language in an assessment to ease coordination. There's no universally correct answer to this scenario but in the field of terrorism analysis you should expect that you will occasionally make controversial conclusions and be fully justified in standing behind the quality of your assessments if you have followed a rigorous analytic process and precisely described the quality of the reporting upon which it is based. It can be very tempting to publish unilateral assessments at times, but you should also understand that customers tend to pay more attention to assessments that have a broader endorsement from within one agency or across multiple agencies—a "community consensus." Therefore you may have to consider whether it's better to be 90-100% correct and stand with one voice or whether to be 75% correct with a community consensus. The more senior your customer, the more likely they will demand a single voice from the Intelligence Community in important topics.