International Studies Association, 2006 ISA Annual Conference, San Diego, CA

Panel on Intelligence and Operational Issues for Counterterrorism and Counterinsurgency, 24 March 2006

Intelligence Co-production and Transaction Analysis for Counterterrorism and Counter-netwar

John P. Sullivan[1][2]

Combatting networked threats requires new approaches to producing intelligence to support a range of operations. Contemporary networked threats include terrorism and insurgency. This paper describes the need for a distributed global network for the co-production of intelligence. It introduces the concept of Intelligence Preparation for Operations (IPO) and describes a transaction analysis model suited to co-production of intelligence for counterterrorism, counterinsurgency and counter-netwar.

Networked threats dominate the horizon. This paper describes some of the emerging tools and approaches to intelligence analysis necessary to navigate this threat horizon.[1] Terrorist and insurgent networks dominate the global scene, challenging state institutions and global security. On the terrorist front the 9/11 attacks in New York and Washington, DC, the M-11 (*Em eOnce*) attacks against the Madrid Metro, and the 7/7 Attacks on the London Underground exemplify this reality. The Iraqi insurgency—or insurgencies—as well as the renewed Afghan insurgency, attacks against Nigerian oil infrastructure, together with other facets of the global Salafist jihad are further contemporary examples of netwar.[2] Within this phenomenon, also known as Fourth Generation warfare (4GW)[3], extremist organizations, exemplified by the self-proclaimed global *jihadi* movement described as al-Qaeda and its affiliates,[4] are complex non-state actors operating as transnational networks within a galaxy of like-minded networks. These entities are transnational, exploiting the seams of traditional approaches to security and intelligence.

Transnational extremists—netwarriors or Fourth Generation warriors—operate across borders and exploit the traditional boundaries between national security and criminal enforcement. These networked global insurgents mix political and religious fanaticism with criminal enterprises to exploit the seams between crime and war. Traditional intelligence and homeland security approaches are

[1] Lieutenant, Los Angeles Sheriff's Department

[2] Los Angeles Terrorism Early Warning Group, National TEW Resource Center

insufficient to address these issues without major structural overhaul and an infusion of new approaches, tools, and processes.

Traditional Approaches are Not Enough

The catastrophic terrorist attacks on the US on 9/11 were a wake up call to the citizenry, Congress and intelligence, national security, law enforcement, and public safety communities. These attacks and the subsequent anthrax attack sequence, like a modern-day Pearl Harbor, are widely viewed as intelligence failures of a large magnitude.[5] Yet as grand as this intelligence failure was, efforts to improve intelligence collection, stimulate information-sharing, and restructure bureaucracies are not enough. Largely governmental attempts at reform have included shifting bureaucracies and an emphasis on 'connecting the dots.' Yet without structural and systematic efforts to revitalize intelligence analysis, attempts to bound uncertainty and predict future terrorist activity are of limited utility. As Sundri Khalsa, drawing from prior work by Garst and Heymann, notes, "warning failures are rarely due to inadequate intelligence collection, [they] are more frequently due to weak analysis, and are often due to decision makers ignoring intelligence (Garst 2000). Decision makers, however ignore intelligence largely because analytical product is weak (Heymann 2000)."[6]

Predictive intelligence is the desired end-state for all intelligence consumers, that is decision-makers at all levels from head of state through tactical operator, investigator, firefighter or cop on the beat. Yet traditional approaches, be they military order of battle analysis for traditional combat or linear lead analysis and case support found in criminal intelligence practice, can fill the need for predicting the swarming activities of small, dispersed, diffuse non-state netwar actors. There are many barriers to achieving the all too elusive actionable intelligence. There appear to be too few good sources of data on events yet to happen, apparently too many variables, in effect a large signal-to-noise ratio, and a lack of understanding of the potential tools and methodologies available to forecast and understand future events.[7]

Captain Sundri K. Khalsa, an USAF intelligence analyst, posits three propositions for correcting this situation:

1) "Analysis, rather than collection, is the most effective way to improve warning;"
2) "Hiring smart people does not necessarily lead to good analysis;" and
3) "A systematic process is the most effective way to facilitate good analysis."[8]

These propositions are shared and validated by the LA TEW's experience in forging new approaches to counterterrorism analysis. To paraphrase Russo and Schoemaker, analysts fail when they follow a poor process in arriving at their product.[9]

The following discussion describes the systematic approaches developed by the Los Angeles Terrorism Early Warning Group (LA TEW) as part of its networked approach to intelligence fusion and intelligence support. They include the TEW concept itself, the concept of ‘co-production’ of intelligence, and a series of mutually supporting processes: Intelligence Preparation for Operations (IPO), the Transaction Analysis Model, and the Transaction Analysis Cycle.

Co-Production of Intelligence and Terrorism Early Warning

The Los Angeles Terrorism Early Warning Group (LA TEW) was established in 1996.[10] It currently includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans- and post attack) specifically tailored to the user’s operational role and requirements. The TEW integrates criminal and operational intelligence to support strategic, operational, and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team.

Within a single TEW, process is known as “*All Source/All Phase*” fusion, where intelligence is derived from all potential sources (classified, sensitive but unclassified, and open sources or OSINT) to provide information and decision support at all phases of a threat/response. Information needed to understand an event is available from local through global sources. This process is essentially “multi-INT” fusion relying upon “meta-analysis.”

The immediate precursor for an attack may be in the local area, across the nation, in a foreign nation, in cyberspace, or in a combination of all.   Identifying global distributed threats and achieving an understanding of their impact requires more than simple information sharing. It demands collaborative data and information fusion and the production of intelligence among cooperative nodes that are distributed among locations where terrorists operate, plan, or endeavor to conduct an attack.   For example, terrorists may plan their attack in Europe and Africa while obtaining logistical and financial support in South America and the Asian Pacific. They may simultaneously conduct reconnaissance in their target city in North America, recruit and train operatives in Iraq and Europe, all the while receiving direction from another location all together.

Developing the intelligence needed to anticipate, prevent, disrupt, or mitigate the effects of an attack requires the production of intelligence in a collaborative and integrated endeavor by a number of agencies across this dispersed area. This is known as ‘co-production’ of intelligence. In essence the TEW is designed as a node in a counter-terrorist intelligence network. To achieve this local through global fusion, or co-production, the TEW has developed an organizational structure and processes, including Intelligence Preparation for Operations (IPO) and the Transaction Analysis Model including the Transaction Analysis Cycle; it conducts exercises, and is forming a networked framework for node-to-node collaboration.

Intelligence Preparation for Operations (IPO)

Intelligence Preparation for Operations (IPO) is the first set of processes used by the TEW to reduce uncertainty and produce an understanding of potential threats. IPO is a civil analog to the military intelligence preparation of the battlefield (IPB) process; it is intended to serve response information needs.[11] IPO provides a standard tool set for situational recognition, course-of-action development, and response rehearsal. This process bridges the gap between deliberate planning and crisis action planning for all facets of a unified multi-organizational response organization. Figure 1 depicts and summarizes the IPO framework.

The core of the IPO process is analysis/synthesis, or the process of breaking down information into its constituent parts, processing it into manageable components, seeking linkages with related elements, providing context, and synthesizing the results into understanding for actionable intelligence. Analysis/Synthesis drives all four steps of the IPO process by pulsing out requests for information (RFIs) to a specific step, as circumstances require.

Step 1: Define the Opspace

Step 1 involves defining the operational space (Opspace). This includes identifying named areas of interest (NAIs) that may be targeted by terrorists that will be covered by intelligence collection assets and ascertaining the critical infrastructure in the area. This process includes evaluation of local through global factors since, in our interconnected world, aspects of critical infrastructure may reside on a global scale or in several interrelated spatial domains.

Step 2: Describe Opspace Effects

Step 2 is defining the effects of various threat scenarios on the operational space (Opspace). Response Information Folders (RIFs) or target folders are developed for key venues. Population, terrain and weather, cultural features, cultural intelligence (CULTINT), including forensic theology are also assessed and analyzed. Geospatial intelligence (GEOINT) including potential infrastructural interactions, cascading impact, and the organizational dynamics of all actors (including reponse organizations) are considered. The exploitation of advanced information systems and social network analysis (defined as Cyber Intelligence or CyberINT) are an additional input. Developing an understanding of all geospatial and social dynamics influencing operations (*i.e.,* geosocial intelligence) is the goal of Step 2.

Step 3: Evaluate OPFOR (PTEs) & Threats

The third step is to identify and evaluate the opposing force (OPFOR) or potential threat elements (PTEs) and the weapons they may employ by class (*i.e.,* chemical, biological, radiological, nuclear, suicide bombing, etc.) This step is intended to identify threats which reside in a notional 'threat envelope.' The goal is achieving 'Deep Indications and Warning' (Deep I&W) driven by an assessment of a range of influences on the OPFOR and an assessment of social network structures.

Step 4: Determ ine OPFOR & Friendly COAs

The fourth step builds upon all the previous steps to develop potential OPFOR and friendly courses of action (COAs). This includes an understanding of current resource and situation status (RESTAT and SITSTAT) of all response forces actually deployed or that may be needed to address the situation. At this step completed intelligence products are disseminated. Actionable intelligence is the goal; products developed include 'Mission Folders,' advisories, alerts, warnings, net assessments and other tailored intelligence products.

The I & W Envelope

Conceptually, the Indications and Warning (I&W) Envelope is depicted as surrounding Step 3, with most I&W typically occurring just prior to an actual attack at the top of the envelope. By embracing advanced social network analysis and related tools such as non-obvious relationship awareness or analysis (NORA), it is possible to achieve 'Deep I&W' by discerning terrorist potentials, and by observing the transactions and signatures associated with assembling a terrorist 'kill chain.'

Foundations of IPO's Core and Four Steps

All of the four steps, as well as the core, rely upon a foundation of intelligence knowledge, process, capabilities, and practice. First among these are a capability for acquiring or collecting information: sensors. The sensors could include a citizen's report of suspicious activity to community police, other human collection means, open source (OSINT) exploitation, internet scanning, signals intelligence, geospatial tools or other types of forensic intelligence support. This may include exploiting real-time or near real-time monitoring and/or virtual reachback from multi-sensor arrays or field reconnaissance capabilities (*e.g.,* chemical, biological or radiological sensors or detectors).

Utilizing IPO relies upon knowledge of analytical tradecraft and concepts for understanding intelligence and conflict. These include understanding of deception and counter-deception, of swarming and counter-swarming, the psychology of intelligence, and decision dynamics, including the need to limit group think and avoid mirror imaging. In addition, the IPO process must at all steps consider 'centers of gravity' and 'decisive points' and be able to address both current and future operations.[12]

Finally, all of these transactions occur along a notional 'Event Horizon' or overview of all aspects of an event or potential event. IPO appreciates three distinct focuses of intelligence production over the course of an event horizon: Trends and Potentials, Capabilities and Intentions, and ultimately conducting an Operational Net Assessment to achieve all phase, all source fusion at all phases of operations. Tools for visualizing the event horizon and making it accessible to decision-makers are found in the 'Transaction Analysis Model' and the 'Transaction Analysis Cycle.'

The Transaction Analysis Model

As noted earlier, traditional analytical techniques and approaches fall short when dealing with networked, non-state threats. Segall identifies three potential methodologies to fill this gap. These are 1) trends and patterns, 2) frequency, and 3) probability.[13] Segall notes that 'trends and patterns' of data are a traditional staple of intelligence that often are linked with the analysis of intent and capability (as specified for example in the national Security Act of 1947). Such techniques are particularly valuable in addressing armed conflict to determine OPFOR actions based upon knowledge of tactics, strategies and the disposition of forces (state and non-state) as analysts seek to discern indicators from newly emerging trends, patterns or irregularities.[14]

Frequency is often added to trends and patterns (since trends and patterns often miss catastrophic substate events). Frequency alone is not enough; it must incorporate trends and patterns to predict or forecast a terrorist event. Nevertheless, frequency is valuable in analyzing communications or other transactions to forecast terrorist activity, potential attacks, and craft interdiction and investigative activities.[15] Probability is the final traditional tool to be incorporated in Segall's trinity. For Segall, determination of the probability of a terrorist event is based upon "risk analysis of latent threat and target vulnerability."[16] Yet traditional threat-based or criminal intelligence approaches to terrorism intelligence typically ignore or segregate vulnerability and criticality (or the impact of a given attack) from their toolset. Segall quotes a private interview with an anonymous member of Her Majesty's Security Services (formerly known as MI5) to emphasize the value of integrating trends and potentials, capabilities and intentions with vulnerability and criticality:

> "The methodology of intelligence analysis of terrorism probability pertains to risk analysis of vulnerability when coupled to trends and patterns methodology determination of threat intent and capability and vulnerability assessment coupled with frequency methodology determination of the statistical analysis of prediction and forecasting of the likelihood of such threats through computerization techniques."[17]

The Transaction Analysis Model addresses these concerns. It was developed by Sullivan to illuminate and articulate the implied tasks contained in the TEW's traditional process of combining trends and potentials, and capabilities and intentions, to achieve a net operational assessment. The Transaction Analysis Model reinforces IPO, exploits IPO, and relies upon meta-analysis (that is, all phase, all source, multi-INT analysis). The Transaction Analysis Model is depicted in Figure 2.

The first stage of the transaction analysis model is determining the current threat based upon capturing transactions and signatures of OPFOR activity. Transactions can be collected as tips, leads, or reports from a variety of sources. Individual transactions or patterns of transactions can then be assigned a signature if they are consistent with specific types of activity or TTPs.

When aggregated, transactions and signatures may form specific trends and potentials (stage two) indicative of terrorist, insurgent or criminal activity. Absent specific indicators or information outlining a specific terrorist ‘kill chain,’ likely target locations can be identified through an assessment of vulnerability and criticality (stage three). These assessments form a hypothesis (or one of multiple competing hypotheses) about the OPFOR’s capabilities and intentions (stage four) to be tested through collection and analysis. Together all of these stages define the threat envelope.[18]

When friendly capabilities are matched with the threat, the resulting assessment of relative risk can be defined in an operational or strategic net assessment. Courses of action (COAs) to respond to and mitigate the risk as well as the posture of friendly security and public safety organizations can be calibrated to the situation described in the net assessment. This information is transmitted through a ‘mission folder,’ advisories, alerts, or warnings and described in IPO step 4. Discerning the threat components of various transactional data is achieved by combining the IPO process with the Transaction Analysis Cycle.

Transaction Analysis Cycle

Terrorist activity plays itself out over time, which can be expressed in a linear fashion as an event horizon, or in a non-linear fashion. The ‘Transaction Analysis Cycle’ developed by Sullivan is a non-linear analytical approach for discerning terrorist activity within dynamic and diffuse data sets laden with noise and masked by a fog of uncertainty. Analysts are charged with detecting and anticipating threat activity from massive amounts of societal activities or transactions. These transactions originate from a variety of sources and correspond to both legitimate and illegitimate activities. This mass of data is fraught with noise and clutter. Some of the transactions reported or observed are consistent with criminal or terrorist activity. That is, the transactions (or clusters of transactions or patterns of activity) may have signatures. Threat signatures are “structures of data that may reflect the execution of threat tasks.”[19] Some patterns or threat signatures can be related, and the connections among related signatures can facilitate hypotheses about high-level organized activities[20] or indicate trends and potentials.

The Transaction Analysis Cycle emerged as a way to teach analysts how to interpret activity in order to assess leads and other inputs while developing iterative collection plans to identify patterns and define hypotheses about a potential terrorist ‘kill chain.’ A kill chain is a pattern of transactional, linked activity that describes a structure of data consistent with threat activity. Boner describes this as a threat pattern that is characterized by a “hierarchy of tasks and subtasks that may be involved in its execution. For example, carrying out a chemical attack may involve recruiting an attack team, acquiring a nerve agent, devising a delivery method, testing, etc. Each of these tasks may in turn involve a number of subtasks.”[21] The kill chain is an analog of a decision tree and contains branches and sequels for each of its tasks and subtasks. Each of these contains transactions and signatures that can be anticipated, with the resulting patterns of data contributing hypotheses about OPFOR capabilities and intentions. Boner notes that the “data structures that are used to represent activity patterns and hypotheses are closely related."[22] Because of this, transaction analysis can help identify pattern variables such as task participants, groups, assets, locations, and other instrumental role players and entities.[23] This makes transaction analysis a valuable method for directing collections and forming investigative and analytical hypotheses.

As part of the LA TEW's on-going refinement of tradecraft, the TEW has participated in a series of exercises simulating its role in discerning indications and warning, providing net assessment, and supporting response and prevention or disruption activities. During two recent exercise series (*Operation Talavera*, a counter-radiological attack scenario in 2004, and *Operation Chim era*, a counter-biological scenario in 2005) the LA TEW exercised its ability to identify patterns of behavior that could culminate in a terrorist attack in order to refine support to prevention and deterrence activities.

The Transaction Analysis Cycle is a framework for generating patterns from large transactional datasets. It is centered (like the TEW organization and IPO framework) on Analysis/Synthesis.[24] Utilizing this framework, analysts can observe activities or transactions conducted by a range of actors looking for indicators or precursors of terrorist or criminal activity of many types. Individual transactions (such as acquiring finances, expertise, acquiring materiel, munitions or capability, recruiting members, conducting reconnaissance, mission rehearsal, conducting an attack, etc.) have signatures that identify them as terrorist or criminal acts, or consistent with the operations of a specific cell or group. These transactions and signatures (T/S) can then be observed and matched with patterns of activity that can be expressed as trends and potentials (T/P), which can ultimately be assessed in terms of a specific actor's capabilities and intentions (C/I). At any point, the analytical team can posit a hypothesis on the pattern of activity and then develop a collection plan to seek specific transaction and signatures that confirm or disprove its hypothesis.

Analysis can start at any point to support the illumination of specific terrorist trends, potentials, capabilities or intentions. Individual transactions and signatures (such as tactics, techniques and procedures [TTPs] or terrorist statements) can be assessed through a tailored collection plan to assemble a notional terrorist 'kill chain' that can be disrupted or an objective that can be protected by selection of appropriate friendly courses of action. Thus the transaction analysis cycle becomes a common framework for assessing patterns, hypotheses and social network links among a range of actors within a broad spatial and temporal context, making co-production of intelligence and situational understanding viable.

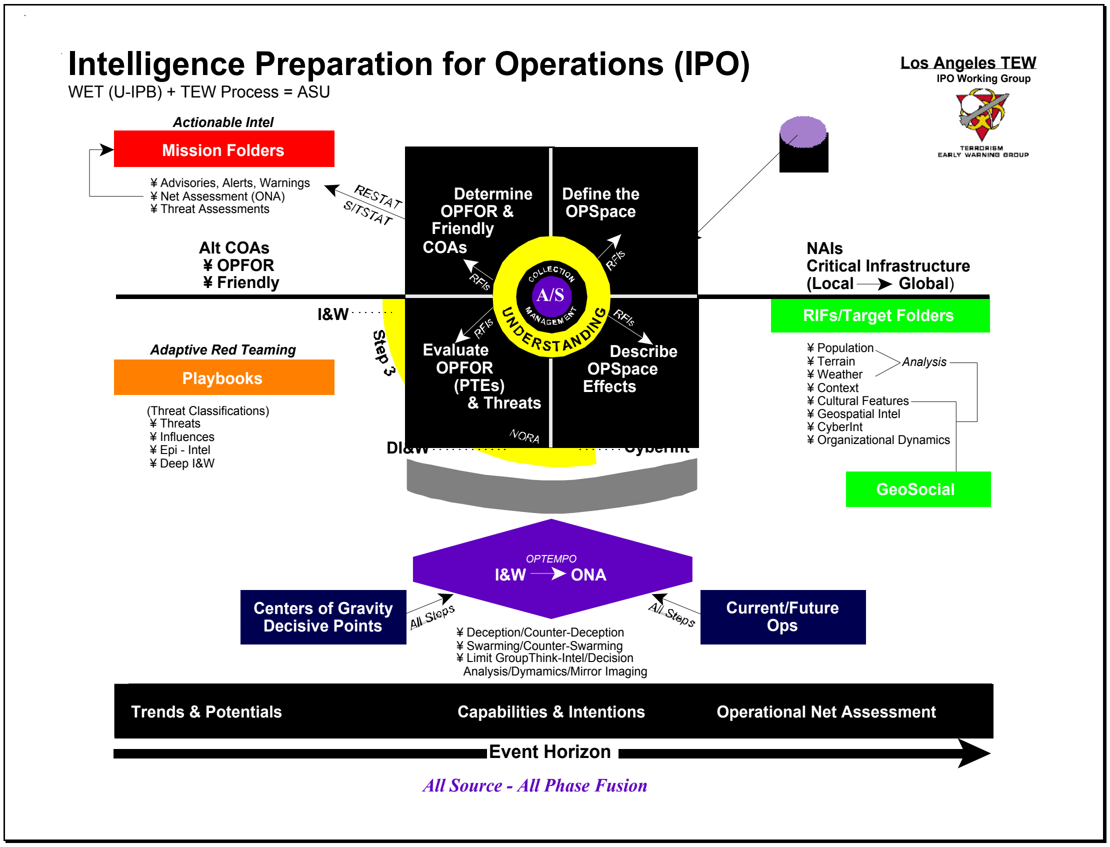
Conclusion

Co-production of intelligence to counter the evolving terrorist threat requires the development of multi-lateral structures. Much of the information necessary to understand the dynamics of a threat—indeed, even to recognize that a threat exists—is developed from the bottom-up, as well as through horizontal (as opposed to top-down) structures. Multilateral exchanges of information, including indicators of potential attacks and alliances among networked criminal actors are needed to counter networked adversaries. This requires the development of new analytical tradecraft, processes, and policy.

Intelligence Preparation for Operations (IPO) and its allied processes, the Transaction Analysis Model and Transaction Analysis Cycle, are comprehensive, systematic ways to structure analytical effort within a single analytical node (such as a single TEW) or across a distributed analytical enterprise engaged in the co-production of intelligence. These transactional approaches allow bi-directional information flow between analysis and collection (collectors feed analysts and analysts feed collection).

As a result disparate information feeds are fused to synthesize situational recognition, foster visualization of comprehensive warning intelligence, and stimulate the generation of alternative competing hypotheses which can be tested through additional refined collection. Finally, these approaches are collaborative and integrate threat (both OPFOR and criminal) intelligence with friendly vulnerability and capability to attain operational net assessment to inform response posture. These approaches have the potential to benefit the counterterrorism, counterinsurgency, and counter-netwar communities as they are institutionalized, expanded, refined, and enabled through technological and information systems support tools.

Figure 1: IPO Framework



Intelligence Preparation for Operations (IPO)

WET (U-IPB) + TEW Process = ASU

Los Angeles TEW

IPO Working Group

TERRORISM EARLY WARNING GROUP

Actionable Intel

Mission Folders

- ¥ Advisories, Alerts, Warnings
- ¥ Net Assessment (ONA)
- ¥ Threat Assessments

Alt COAs
¥ OPFOR
¥ Friendly

Adaptive Red Teaming

Playbooks

(Threat Classifications)
- ¥ Threats
- ¥ Influences
- ¥ Epi - Intel
- ¥ Deep I&W

Determine OPFOR & Friendly COAs

Define the OPSpace

Evaluate OPFOR (PTEs) & Threats

Describe OPSpace Effects

NAIs
Critical Infrastructure
(Local → Global)

RIFs/Target Folders

- ¥ Population
- ¥ Terrain
- ¥ Weather
- ¥ Context
- ¥ Cultural Features
- ¥ Geospatial Intel
- ¥ CyberInt
- ¥ Organizational Dynamics

Analysis

GeoSocial

OPTEMPO
I&W → ONA

Centers of Gravity Decisive Points

Current/Future Ops

- ¥ Deception/Counter-Deception
- ¥ Swarming/Counter-Swarming
- ¥ Limit GroupThink-Intel/Decision Analysis/Dymamics/Mirror Imaging

Trends & Potentials

Capabilities & Intentions

Operational Net Assessment

Event Horizon

All Source - All Phase Fusion

Figure 2: Transaction Analysis Model

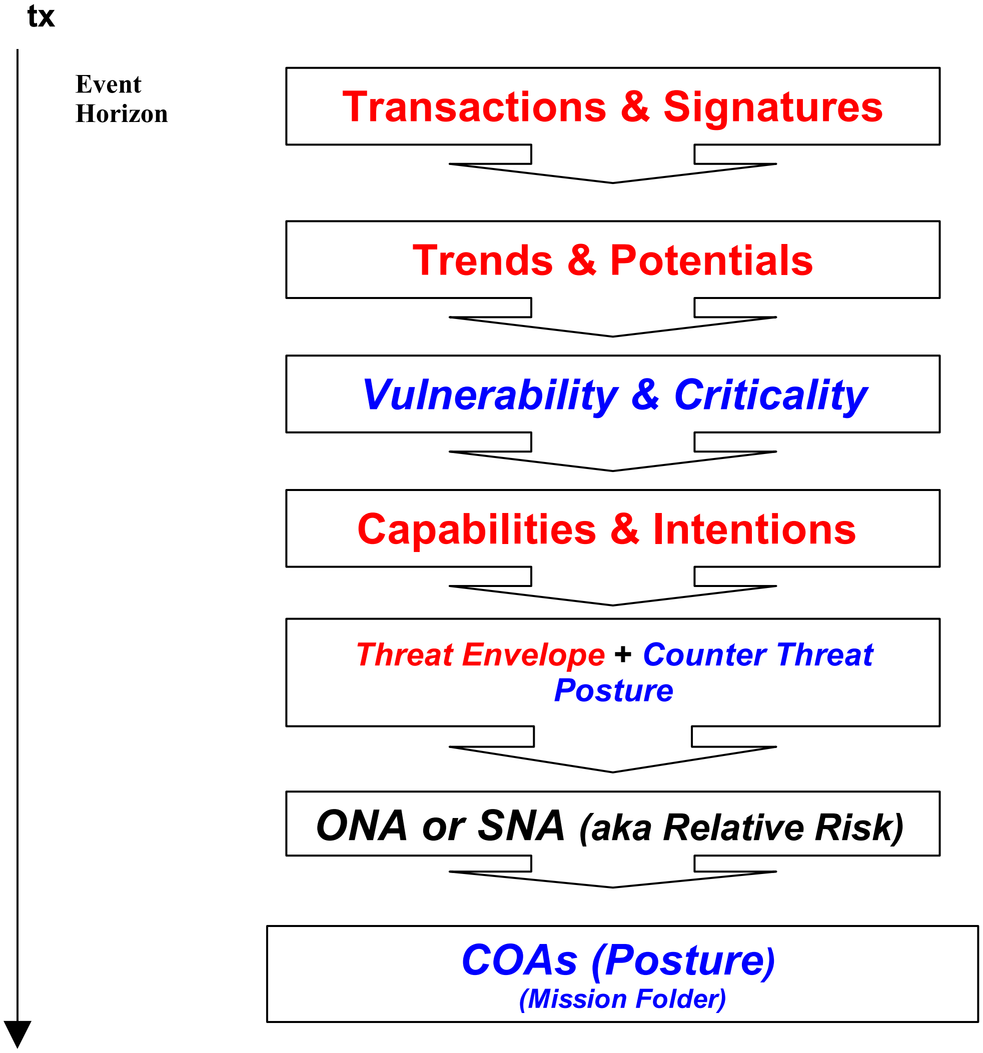
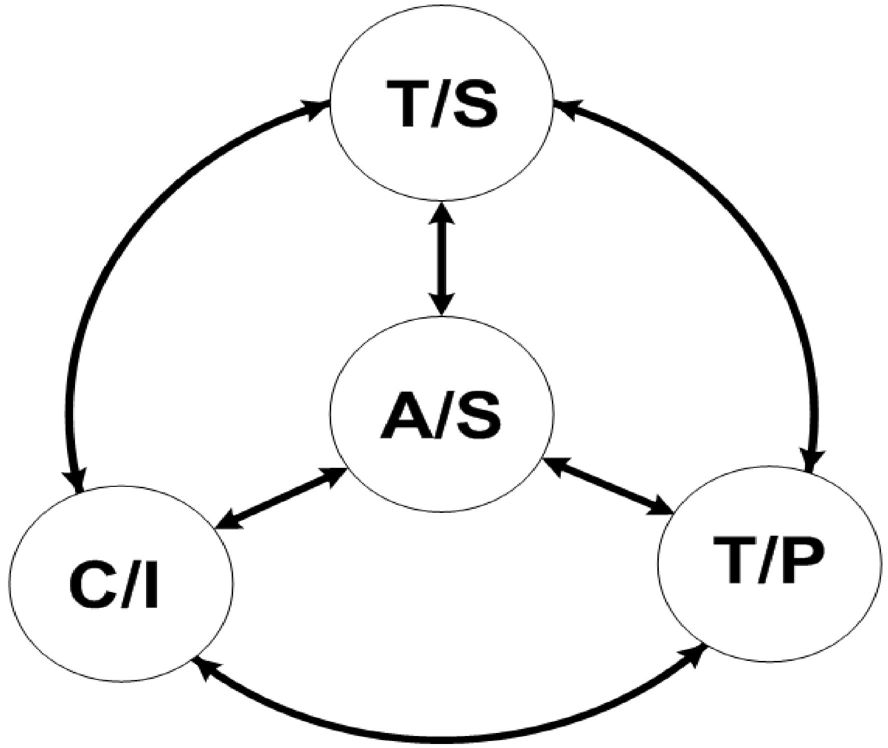

tx
Event Horizon
Transactions & Signatures
Trends & Potentials
Vulnerability & Criticality
Capabilities & Intentions
Threat Envelope + Counter Threat Posture
ONA or SNA (aka Relative Risk)
COAs (Posture)
(Mission Folder)

Figure 3:

Transaction Analysis Cycle



T/S = Transactions & Signatures
T/P = Trends & Potentials
C/I = Capabilities & Intentions
A/S = Analysis/Synthesis

References

[1] This paper expands upon an earlier paper, John P. Sullivan, Terrorism Early Warning and Co-Production of Counterterrorism Intelligence, presented to the Canadian Association for Security and Intelligence Studies, *CASIS 20th Anniversary International Conference,* Montreal, Quebec, Canada, 21 October 2005. That paper can be downloaded at: http://www.terrorism.com/modules.php?op=modload&name=Documents&file=get&download=432.

[2] Netwar is a theory developed by John Arquilla and David Ronfeldt to describe networked conflict in the Information Age. Perhaps the best text outlining Netwar and its attributes can be found in John Arquilla and David Ronfeldt (Eds*.), Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica: RAND, 2001.

[3] Fourth Generation warfare (4GW) was first articulated in William Lind, K. Schmitt, J. Sutton, and G.I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, October 1989, pp. 22-26. A comprehensive overview can be found in Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century*, St. Paul, MN: Zenith Press, 2004. The intelligence challenges incumbent in addressing 4GW are discussed in G.I. Wilson, John P. Sullivan, and Hal Kempfer, "Fourth-Generation Warfare: It's Here, And We Need New Intelligence-Gathering Techniques for Dealing with It*," Armed Forces Journal International*, October 2002, pp. 56-62.

[4] See for example Jonathan Schanzer, *Al-Qaeda's Armies: Middle East Affiliate Groups & the Next Generation of Terror*, New York: Specialist Press International, 2005 for a description of the range of al-Qaeda affiliates.

[5] See *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition, New York: W.W. Norton & Co., N.D. for a detailed discussion of the events and disconnects leading up to the 9/11 events.

[6] Sundri K. Khalsa, "Forecasting Terrorism: Indicators and Proven Analytic Techniques," *Proceedings of the 2005 International Conference on Intelligence Analysis*, Mitre Corporation and Office of the Assistant Director of Central Intelligence for Analysis and Production, 2-4 May 2005, McLean, VA found at https://analysis.mitre.org//proceedings/Final_Papers_Files/106_camera_Ready_Paper.pdf; Ronald D. Garst, "Fundamentals of Intelligence Analysis," *Intelligence Analysis ANA 630*, No. 1 Joint Military Intelligence College (Ed.), Washington: DC: Joint Military Intelligence College, 2000, pp. 5-7; and Hans Heymann, Jr., "The Intelligence-Policy Relationship," *Intelligence Analysis ANA 630*, No. 1 Joint Military Intelligence College (Ed.), Washington: DC: Joint Military Intelligence College, 2000, pp. 53-62.

[7] See Glen M. Segell, "Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004," *International Journal of Intelligence and CounterIntelligence,* Vol. 18, No. 2, Summer 2005, pp. 221-238 and David T. Resch, "Predictive Analysis: The Gap Between Academia and Practitioners," *Military Intelligence*, Vol. 21, No. 2, April-June 1995, pp. 26-29.

[8] Sundri K. Khalsa, op sit, see note 6 above.

[9] Khalsa, ibid., quotes Russo and Schoemaker: "frequently groups of smart, well-motivated people…agree…on the wrong solution… They didn't fail because they were stupid. They failed because *they followed a poor process in arriving at their decisions*." (Khalsa's emphasis.) As cited by Khalsa, Edward J. Russo and Paul J.H. Schoemaker, *Decision Traps: The Ten Barriers to Brilliant Decision-Making and How to Overcome Them*, New York: Rockefeller Center, 1989.

[10] Additional details on the Los Angeles Terrorism Early Warning Group, its approach, and the emerging TEW network can be found in John P. Sullivan, "Terrorism Early Warning Groups: Regional Intelligence to Combat Terrorism," in Russell Howard, James Forest, and Joanne Moore (Eds.), *Homeland Security and Terrorism: Readings and Interpretations*, New York: McGraw-Hill, 2006, pp. 235-245; John P. Sullivan, "Networked Force Structure and C^4I," in Robert J. Bunker (Ed*.), Non-State Threats and Future Wars*, London: Frank Cass, 2003, pp. 144-155; John P. Sullivan, "Networked All-Source Fusion For Intelligence and law Enforcement Counter-terrorism Response," paper presented to Intelligence Studies Section of the International Studies Association (ISA), *2004 ISA Annual Convention*, Montreal Quebec, Canada, 18 March 2004; and John P. Sullivan and Robert J. Bunker, "Multilateral Counter-Insurgency Networks," in Robert J. Bunker (ED.), *Networks,Terrorism and Global Insurgency*, London: Routledge, 2005,pp.183-198.

[11] See John P. Sullivan, Hal Kempfer, and Jamison Jo Medby, “Understanding Consequences in Urban Operations: Intelligence Preparation for Operations,” *INTSUM Magazine*, Marine Corps intelligence Association, Vol. XV, Issue 5, Summer 2005, pp. 11-19 for an in depth discussion of IPO.

[12] A center of gravity is that key aspect of the OPFOR, whether it is a location, leader, bond or relationship, or other part of their operational matrix that is determined to be critical if removed or neutralized by our forces. A Decisive Point is a subordinate component of a center of gravity, such as a location, event, time or other identifiable node or action that enables the center of gravity.

[13] Glen M. Segall, op sit, at p. 221.

[14] Ibid. pp.224-225.

[15] Ibid. p. 228.

[16] Ibid. pp. 229-230.

[17] Ibid. p. 231. Segall cites an unnamed member of MI5 to describe ideal forecasting capability for terrorist events.

[18] The threat envelope corresponds roughly to the Indication and warning (I&W) envelope in IPO, since the indicators tracked in the I&W envelope manifest the visible or potentially visible activities which can be discerned through collection and analysis.

[19] Christopher M. Boner, “Novel, Complementary Technologies for Detecting Threat Activities within Massive Amounts of Transactional Data,” , *Proceedings of the 2005 International Conference on Intelligence Analysis*, Mitre Corporation and Office of the Assistant Director of Central Intelligence for Analysis and Production, 2-4 May 2005, McLean, VA found at https://analysis.mitre.org//proceedings/Final_Papers_Files/318_camera_Ready_Paper.pdf;

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Analysis/Synthesis is the core of the ‘Orientation’ phase of Col. John Boyd’s Decision Cycle or OODA (Observe-Orient-Decide-Act) Loop. The TEW model draws much of its theoretical grounding from the interaction between the OODA Loop of parties to networked conflict.