Canadian Association for Security and Intelligence Studies
CASIS 20th Anniversary International Conference
Montreal, Quebec, Canada

Panel 5: In Pursuit of the Analytical Holy Grail: Part 1
Innovation in Analysis, Warning and Prediction
21 October 2005

Terrorism Early Warning and Co-Production of Counterterrorism Intelligence

John P. Sullivan[*†]

Contemporary terrorism is a complex phenomenon involving a range of non-state actors linked in networked organizations. These organizations, exemplified by the global jihadi movement known as al-Qaeda, are complex non-state actors operating as transnational networks within a galaxy of like-minded networks. These entities pose security threats to nation states and the collective global security. Traditional security and intelligence approaches separated criminal and national security intelligence, as well as domestic and international security concerns. Modern terrorism exploits these seams to operate on a global scale. The Terrorism Early Warning Group (TEW) concept emerged in Los Angeles in 1996 as a way to bridge the gaps in traditional intelligence and security structures. The TEW embraces a networked approach to intelligence fusion and directs its efforts toward intelligence support to regional law enforcement, fire and health agencies involved in the prevention and response to terrorist acts.

The Los Angeles TEW 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 bridges criminal and operational intelligence to support strategic 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. Toward this end, the TEW has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and refined processes to analyze and synthesize threat data to support its client agencies. The TEW has adapted the military concept of Intelligence Preparation of the battlefield into a dynamic Intelligence Preparation for Operations (IPO) process, and has defined a framework known as the Transaction Analysis Cycle to anticipate threats and develop intelligence collection strategies. Finally, TEWs based on the Los Angeles model are emerging throughout the United States. These TEWs are forming a distributed network with the potential to co-produce intelligence to counter networked threats. This paper discusses the LA TEW model and its practices.

Contemporary terrorist networks challenge state institutions and global security. The 9/11 attacks in New York and Washington, DC, the M-11 (*Eme Once*) attacks against the Madrid Metro, and the 7/7 Attacks on the London Underground are examples of this threat. Extremist organizations, exemplified by the self-proclaimed global *jihadi* movement described as al-Qaeda and its affiliates, are complex non-state actors operating as transnational networks within a galaxy of like-minded networks. These transnational entities pose

[*] Lieutenant, Los Angeles Sheriff's Department
[†] Los Angeles Terrorism Early Warning Group, National TEW Resource Center

security threats to nation states and collective global security. Traditional approaches to security and intelligence separated criminal and national security intelligence, as well as domestic and international security concerns.

Transnational extremists operating across borders transect the traditional boundaries between national security and criminal enforcement. These networked global insurgents are blending political and religious fanaticism with criminal enterprises to challenge the rule of law and exploit the seams between crime and war. Modern terrorism exploits these seams to operate on a global scale. Contemporary intelligence and homeland security responses are influenced by these changes. This paper describes the Los Angeles Terrorism Early Warning Group's networked approach to intelligence fusion and intelligence support to regional law enforcement, fire and health agencies involved in the prevention and response to terrorist acts.[1]

Effective response to these threats demands a high degree of interoperability among all levels of responders—local, state, federal, and ultimately globally—between a variety of disciplines (law enforcement, fire service, public health and medical), between government and non-governmental agencies and private corporations, and between civil and military agencies. Intelligence is an important element of forging an interagency response. To be effective, counterterrorism intelligence must embrace network attributes and effectively fuse with networked operational forces.

Co-Production of Intelligence: The 'TEW' Model

The Los Angeles Terrorism Early Warning Group (LA TEW) was established in 1996. 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 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, this 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.

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 information fusion and the production of intelligence among cooperative nodes that are distributed among locations where terrorists operate, plan, or seek to

attack. For example, terrorists may plan their attack in Europe 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, 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 Cycle; it conducts exercises, and is forming a networked framework for node-to-node collaboration.

TEW Organization

Organizationally, the TEW is organized into six cells: the Officer-in-Charge or OIC (Command), Analysis/Synthesis, Consequence Management, Investigative Liaison, Epidemiological Intelligence (Epi-Intel) and Forensic Intelligence Support cells. The Forensic Intelligence Support cell, which includes technical means and such external resources as virtual reachback, supports the others.

These are supported by a network of Terrorism Liaison Officers (TLOs) coordinated by the TEW. The foundational TEW organization (depicted in Figure 1) is described below:

- The *OIC (Command) cell* provides direction, sets intelligence requirements, and is responsible for interacting with the incident command entities.

- The *Analysis/Synthesis cell* coordinates net assessment activities and develops an iterative collection plan (including tasking requests for information to the various net assessment elements). The Analysis/Synthesis cell is also responsible for developing the results of all the cells' analysis into actionable intelligence products.

- The *Consequence Management cell* assesses the law, fire and health (EMS-Hospital-operational medical) consequences of the event.

- The *Investigative Liaison cell* coordinates with criminal investigative entities and the traditional intelligence community.

- *The Epidemiological Intelligence (Epi-Intel) cell* is responsible for real-time disease surveillance and coordination with the disease investigation.

- The *Forensic Intelligence Support cell* exploits a range of technical means to support the TEW fusion process. These include CBRNE reconnaissance, the

use of sensors and detectors, geospatial tools (including mapping, imagery and GIS products), and cyber means.

Finally, the TEW has developed a local network of Terrorism Liaison Officers (TLOs) at each law enforcement, fire service, and health agency in its area of operations. In addition, private sector counterparts, known as infrastructure Liaison Officers (ILOs) are also being established to ensure the flow of information between the TEW and key critical infrastructure and cultural entities. TLOs and ILOs provide the outer sensing capacity for the TEW and are users of TEW products.

Intelligence Preparation for Operations (IPO)

Intelligence preparation for operations (IPO) is emerging as a civil analog to the military intelligence preparation of the battlefield (IPB) to serve response information needs.[2] 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. The IPO framework is depicted in Figure 2.

The center or core of the IPO process (as in the TEW organization) 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 actionable intelligence. This core drives IPO's four steps through the process of pulsing out requests for information (RFIs) at all steps.

Step 1: Define the Opspace

The first step is 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

The second step is defining the operational space effects. In this step target Response Information Folders (RIFs) or target folders are developed for key venues such as infrastructural or cultural locations. Population, terrain and weather, cultural features, including cultural intelligence or CULTINT are also assessed. Geospatial intelligence (GEOINT) including potential infrastructural interactions and cascading impact and the organizational dynamics of all actors are considered. Cyber Intelligence (CyberINT) or the exploitation of advanced information systems and social network analysis are then added. The goal is an understanding of all geospatial and social dynamics influencing operations (*i.e.,* geosocial intelligence).

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.

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.'

Step 4: Determine OPFOR & Friendly COAs

The fourth step builds upon all the previous 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. This is the step where 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.

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 reporting suspicious activity to community police, other human collection means, Internet scanning, signals intelligence, geospatial tools or other types of forensic intelligence support. These ultimately involve the exploitation of 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 an understanding of deception and counter-deception, of swarming and counter-swarming as tactics or approaches to conflict, as well as an understanding of the psychology of intelligence and decision dynamics, such as the need to limit group think and avoid mirror imaging. In addition, the IPO process must consider 'centers of

gravity' and 'decisive points' and be able to address both current and future operations at all steps.[3]

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. A more dynamic and practical way of viewing the event horizon is found in 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.

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.' As part of the LA TEW's on-going refinement of trade craft, 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 Chimera*, 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 pattern generator (like the TEW organization and IPO framework) centered on Analysis/Synthesis.[4] 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

The TEW model is scalable and adaptable. From its initial implementation in Los Angeles, the TEW concept and network has grown to include TEWs at various stages of development throughout California: Riverside/San Bernardino, Orange County, Sacramento, San Diego, and East Bay (Oakland, Alameda and Contra Costa counties). The TEW has also spread elsewhere in the United States: Pierce County, WA; Tulsa, OK (OK Region 7); New Orleans, LA (LA Region I); Greater Cincinnati; Albuquerque, NM (Mid-Rio Grande); and the Territory of Guam at the time of this paper, with others soon expected to come on line. These individual nodes are coalescing into a network, sharing information among TEWs, state fusion centers, and other interested entities. These expansion efforts are supported by technical assistance sponsored by the US Department of Homeland Security, Office of Domestic Preparedness. Technical assistance efforts include doctrine development and workshops to further TEW practice and analytical tradecraft at the National TEW Resource Center based at the LA TEW.

While the LA TEW model has demonstrated that networked fusion is possible, a number of challenges remain. First among these are organizational and bureaucratic competition. Networked forms compete with their hierarchical predecessors. Bureaucratic inertia slows moves toward collaboration both within and especially across disciplines, jurisdictions, and nodes. Fiscal competition and struggles for intergovernmental primacy are additional complicating factors.

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 trade craft, processes, and policy. Intergovernmental instruments are needed to fully exploit lateral information-sharing, along with the development of distributed intelligence processing across organizational and political seams, including the development of mechanisms for sharing information among both intra-national and international nodes. The TEW model and the processes evolving within the TEW network are the first step in pursuit of the analytical 'Holy Grail.'

Figure 1: Foundational TEW Organization

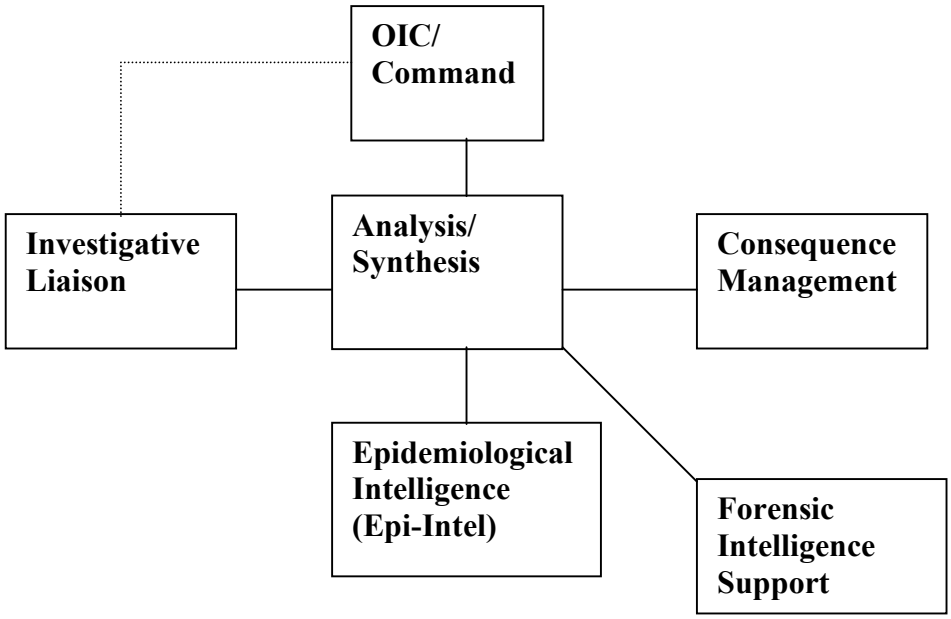


Figure 2: IPO Framework

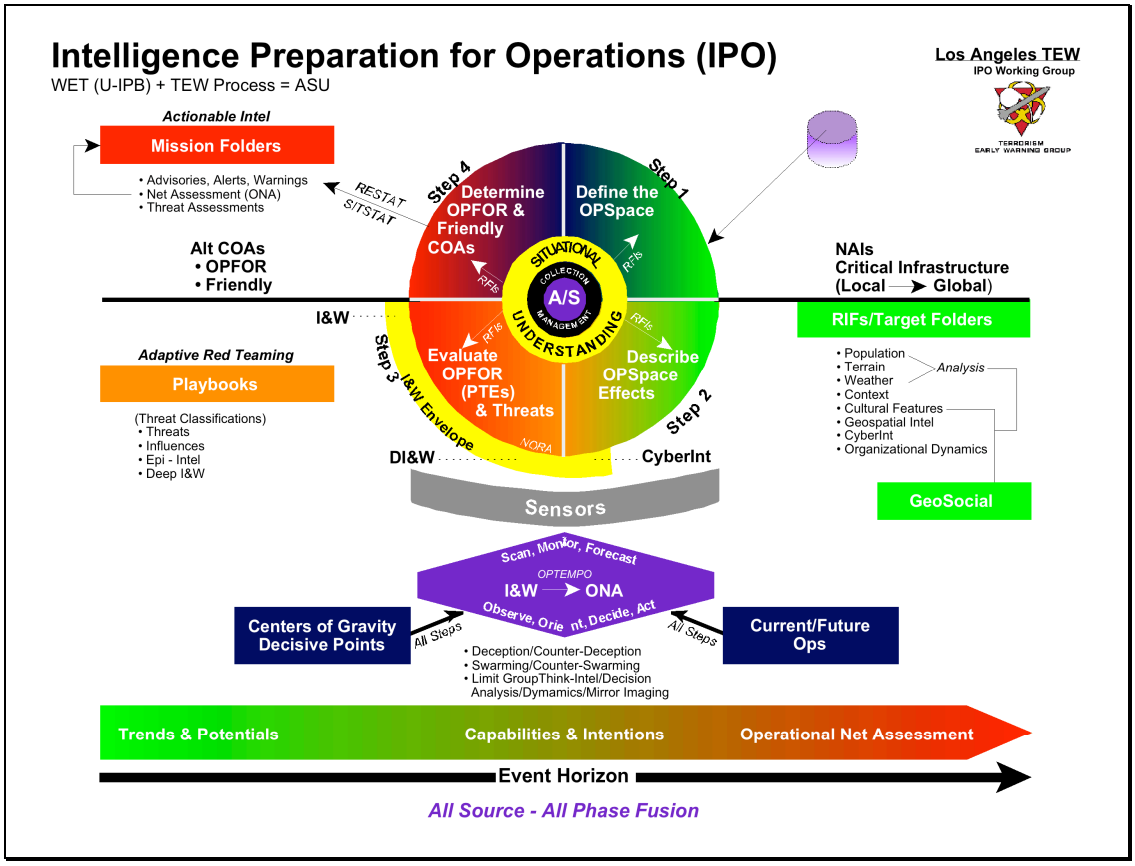
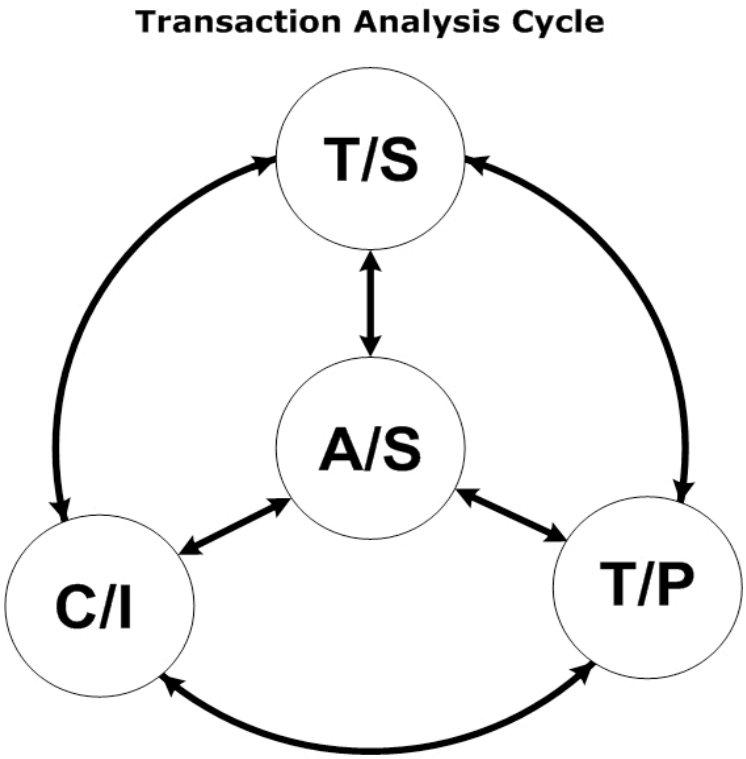


Figure 3:



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

References

[1] This paper draws from a number of previous papers and briefings presented over the nine year history of the LA TEW. These include: John P. Sullivan, "Networked Force Structure and C^{4}I," 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.

[2] 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.

[3] 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.

[4] Analyze/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.