International Journal of Police Science
ISSN 2771-3377 (online); ISSN 2771-3385 (print)
https://IJPS-Journal.org
Volume 4, Issue No. 1 (2025)

International Police Science Association (IPSA)

Research Article

Terrorism Early Warning and Intelligence Fusion for Preventing and Countering Violent Extremism

John P. Sullivan

https://doi.org/10.56331/ijps.v3i2.13527

Submitted: April 2025
Accepted: April 2025
Published: April 2025

Citation: Sullivan, John; "Terrorism Early Warning and Intelligence Fusion for Preventing and Countering Violent Extremism." *International Journal of Police Science* 4, no. 1 (2025). https://doi.org/10.56331/ijps.v3i2.13527

Abstract:

Intelligence fusion centers are one approach to providing intelligence, indications and warning, and analytical support to government agencies at all levels of government, and across jurisdictional boundaries, to address a range of issues, including terrorism and violent extremism. This article provides a case study of the Los Angeles Terrorism Early Warning Group (LA TEW). The LA TEW was a pioneer in developing and providing comprehensive, all-source intelligence support to a metropolitan region. The TEW model included law enforcement (police and corrections), fire service, emergency medical services, public health, and emergency management agencies, along with a network of subject matter experts to provide insight into terrorist threats, extremism, critical infrastructure protection and emerging threats. The LA TEW also developed a range of analytical models and approaches to provide intelligence support for civil protection and counterterrorism that are reviewed in this article.

Keywords: Countering Violent Extremism, Early Warning, Fusion, Intelligence Analysis, Indications & Warning, Terrorism, Transnational Crime.

Terrorism and violent extremism in their many forms are major global concerns. These threats, along with the criminal enterprises that often enable violent attacks are fueled by radicalization, discontent, and ideological and societal fissures. Recognition of the factors that lead to these fissures, the processes of radicalization, and ultimately to significant attacks, such as the 2004 Madrid train bombings,[1] 2008 Mumbai attacks,[2] Sri Lanka's 2019 Easter Sunday massacre,[3] led to recognition by some that developing mechanisms for intelligence warning and prevention is need to address key public policy lacunas in these areas. The development of doctrine and network protocols for addressing these threats and filling those gaps is the theme of this article.

Introduction

This article provides an overview of the use of intelligence and intelligence fusion toward preventing and countering violent extremism. Specifically, the article is a case study of the Los Angeles Terrorism Early Warning (TEW) Group model and its pioneering efforts to provide comprehensive, all-source intelligence support to a metropolitan region (the Los Angeles County Operational Area). The Los Angeles County Operational Area is comprised of 88 cities, including the City of Los Angeles, covering nearly 4,800 square miles, with a population of nearly 10 million. The LA TEW was a multidisciplinary, interagency task force that provided intelligence fusion for that operational area and formed the foundation of the US National Network of Fusion Centers. The TEW model included law enforcement (police and corrections), fire service, emergency medical services, public health, and emergency management agencies, as well as a network of subject matter experts to provide insight into critical infrastructure protection.

The article provides a brief overview of the TEW's development, its interaction with other entities, such as the Federal Bureau of Investigation's Joint Terrorism Task Forces (JTTFs), and numerous operational partners, including the Royal Canadian Mounted Police (RCMP), Criminal Intelligence Service of Canada (CISC) and its Strategic Early Warning System (SEWS) for criminal intelligence, the Australian Federal Police, and a range of civil and military partners. The TEW model pioneered the development of domestic intelligence fusion, the "co-production of intelligence" among networked global and national partners, across jurisdictional and disciplinary boundaries. The TEW specialized in meta-analysis integrating criminal, national security intelligence, and the complete range of intelligence disciplines (or "INTs") into an all-source, all-phase net assessment process. This process included the use of a range of models and approaches including the "transactional analysis cycle" and "Intelligence Preparation for Operations (IPO)" resulting in "operations-intelligence fusion."

In addition, the article briefly recounts the development of analytical trade craft for providing intelligence support to law enforcement, fire and rescue (including EMS), and public health for Chemical, Biological Radiological, and Nuclear incidents, as well as traditional explosive and armed terrorist attacks. In addition, the TEW provided intelligence support and threat assessment to guide pandemic response (including differential diagnosis for suspicious outbreaks of disease), anthrax and ricin threats.

The TEW also worked on identifying radicalization within the community and in correctional facilities (prisoner radicalization) and worked to identify emerging threats. The TEW's work on emerging threats included identifying technology threats (i.e., laser strikes against aircraft, the potential use of MANPADS against civil aviation targets) and social/criminal threats such as the rise of transnational organized crime, criminal armed groups—including Mexican drug cartels and gangs—embracing quasi-terrorist tactics, employing social modification or *narcocultura*, and waging "criminal insurgency."[4]

The TEW concept embraced the complete range of intelligence from current intelligence, through early warning (indications and warning), to strategic foresight in order to address networked threats. Contemporary and future considerations building from this framework will be addressed.

Fusion Centers and Intelligence Sharing

Fusion centers are collaborative initiatives that facilitate intelligence analysis and information sharing. In the United States, they became increasingly popular after al-Qaeda's terrorist attacks on 11 September 2001, widely known as the 9/11 attacks. Indeed, fusion centers are largely a response to the "intelligence failures" that surround the buildup to those tragic events. These "failures" were viewed as a "failure of imagination"[5] an "adaptation failure,"[6] and perhaps inevitable.[7] Nevertheless, "fusion centers" are viewed as one potential means of mitigating warning failures.

According to the US Government's Global Justice Information Sharing Initiative, a fusion center is:

> A collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.[8]

These fusion centers, collectively form the National Network of Fusion Centers According to the Factsheet on the network, these centers:

> Serve as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, and territorial (SLTT) partners. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service…, emergency response, public health, critical infrastructure protection … and private sector security personnel to lawfully gather and share threat-related information. They provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. Fusion centers conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners.[9]

Terrorism Early Warning and Counterterrorism

Fusion centers, including the TEW model were recognized as an effective mechanism toward enabling law enforcement efforts for community protection.[10] The Los Angeles Terrorism Early Warning (TEW) group was established in 1996, a full five years before the tragic 9/11 attacks. It was developed in the aftermath of the 1992 Los Angeles Riots, the 1995 Oklahoma City Bombing, and the 1995 Tokyo Sarin Attacks. During its early operational phase, the LA TEW was an ad hoc, information-sharing network that conducted monthly information-sharing and problem-solving meetings among its members from the Los Angles Sheriff's Department (LASD), the Los Angeles Police Department (LAPD), the Los Angeles Division of the Federal Bureau of Investigation (FBI), the Los Angeles City and County Fire Departments, and the Los Angeles County Department of Health (public health and emergency medical services).

From its inception, the LA TEW included representatives from academia, thinks tanks (i.e., RAND Corporation), and key critical infrastructure sectors. Over time, the groups expanded to include representatives from other local municipal police and fire agencies, emergency management organizations, and other state police agencies. It also developed liaison relationships with The Royal Canadian Mounted Police, the Australian Federal Police, and other foreign police services (especially

those with a liaison presence in the Los Angeles region.

By 1998, the LA TEW was activated to provide support to a series of anthrax hoaxes in Los Angeles. This activation was preceded by TEW analysts issuing an advisory to local public safety agencies, entitled "Responding to Potential Weapons of Mass Destruction (WMD) and Anthrax Threat Incidents."[11] The specific indications and warning sequence was described in the Gilmore Commission Report (2000):

> Anthrax hoaxes in the United States started with an incident in Wichita, Kansas on August 18, 1998, four months before the first one in Los Angeles. The media took hold of this event, and through the "copycat syndrome" other hoaxes began to slowly proliferate across the country. The significance of this proliferation of anthrax hoaxes was quickly identified by the Los Angeles TEW, which saw fit to discuss the Wichita incident during its August 27 meeting. Additional anthrax hoaxes were reported during the TEW's October, November and December meetings. By the November TEW meeting, it was felt that "anthrax hoaxes are coming to L.A."[12]

The details of the specific TEW-supported responses during 1998 are described in both Sullivan and Wirtz (2008)[13] and the Gilmore Commission Report (2000). The key takeaway as described by the Gilmore Report was:

- *Threat Analysis Needs a Cooperative Vehicle*[14]

The key contribution to intelligence fusion—at least from the author's perspective—was the development of the "TEW Model" with its emphasis on the "Co-Production of Intelligence.[15] In August 2000, the LA TEW was activated to support the 2000 Democratic National Convention, a National Special Security Event with security led by the United States Secret Service with support from the local public safety community. Sullivan and Wirtz (2008), recount the TEW's DNC activation, including on-going situation status and deploying forensic intelligence support capabilities to assess CBRN threats:

> Given that so many agencies were involved in providing security for the DNC, the TEW's greatest contribution was to improve overall situational awareness by fusing data from all sources to help officials separate the serious from the not-so-serious incidents that occurred during the convention. For example, reports began to surface that law enforcement vehicles across the city were being knocked out of action by contaminated fuel. But TEW field investigators and analysts soon determined that the vehicles had been damaged by the accidental contamination of a fuel truck. The event was neither an act of sabotage nor a precursor to a more significant attack. In another event, patrolmen in one locality noticed that protestors were apparently stockpiling bricks and other materials that could be used in violent confrontations with police. This information was quickly evaluated and disseminated by TEW analysts, especially when these preparations were linked to groups known for provoking violent street demonstrations. Additionally, TEW analysts monitored enhanced surveillance systems to detect signs that a chemical, biological, or radiological incident was unfolding.[16]

The LA TEW started to stimulate the development of similar organizations, initially in California and then nationally before the 9/11 attacks in 2001. After the 9/11 attacks that momentum accelerated with the LA TEW becoming a full-time initiative and serving as a forerunner to the National Network of Fusion Centers.[17] This initiative and its successors are still undergoing evolution as the nature of terrorist and criminal threats continues to morph. Continuing challenges include the seams between domestic and foreign intelligence, bureaucratic inertia, and bureaucratic competition. These factors

are compounded as criminal and terrorist threats intersect and exacerbated by political contention and hybrid threat actors leveraging crime, terrorism, disinformation, communal tensions, and political discord.[18] Bridging domestic and national security concerns is especially complex and problematic due to the range of issues faced when dealing with global illicit networks—especially from a domestic vantage point.[19]

Bridging Domestic and National Security (Foreign) Intelligence

Addressing violent extremism, terrorism, and transnational crime is often complicated by the existence of global illicit networks. These groups often operate as distributed, transnational networks with operational capability, leadership, intelligence, and logistical, and financial support networks that son multiple international frontiers. These national divides are exacerbated by bureaucratic divides, and organizational competition. Indeed, Aquilla and Ronfeldt[20] have commented on these networks and their use of cyber means and netwar as encompassing a new spectrum of conflict waged by terrorists, gangs, ethnic extremists, and a range of activists. In their view, "It takes networks to fight networks."[21] The LA TEW and its emergent network was one means of forging that capability and as such created a bottom up, lateral intelligence network with various nodes and multilateral participation (including links with foreign police agencies.

Meta-Analysis: TEW Model and Analytical Approaches

The overall TEW Concept provides a template for developing an integrated intelligence fusion capacity for metropolitan regions, and other polities. The concept has been documented in numerous fora, including the LA TEW case study,[22] a National TEW Resource Center resource guide,[23] a detailed overview for the International Association of Law Enforcement Intelligence Analysts (IALEIA),[24] several master's theses.[25]

The LA developed and refined a networked model for developing intelligence, known as co-production, that spanned the entire range of operational phases (pre-, trans, and, post-incident. Warning[26] is at the core of the TEW approach. It as the name suggests emphasized "early warning" itself a variety of indications and warming that relies upon predictive or "estimative intelligence."[27] In many ways, this model diverges from the typical focus on current intelligence to widen the aperture to include anticipating and predicting future events, trends, and threats. It addresses, both near-term futures (early warning) and longer-range potentials (strategic foresight).

As described in the aforementioned IALEA piece:

> Achieving the predictive or estimative intelligence requires a complex set of skills and a dynamic mix of experts and generalists from a range of disciplines, knowledge of tools and processes, and an understanding of the ingredients of uncertainty. First among these ingredients is what Treverton calls recognition of the distinction between "puzzles" and "mysteries."[28] Puzzles often involve decoding secrets or gathering new data.
>
> Collecting the missing pieces of knowledge can assemble the picture emerging as a puzzle is filled in. This is commonly called "connecting the dots." Mysteries involve discerning things not known, commonly referred to as the "unknown unknown." These cannot be solved by simply collecting more data or connecting dots (they may not exist yet). Mysteries are solved through assessing multiple alternative hypotheses assessing scenarios, and ultimately time. A difficult element of some mysteries is the presence of wildcards and extreme events. This is the province of what Nassim Nicholas Taleb calls the "Black Swan."[29]

> A Black Swan is unexpected. It is an unanticipated outlier arising outside the realm of regular expectations. To solve the normal unknown of the puzzle you collect data and connect the dots. To anticipate and manage the extreme unknown of the mystery or Black Swan, you need adaptive scanning, scenarios, and flexible new tools.[30]

The new tools (or approaches) pioneered by the LA TEW include Intelligence Preparation for Operations (IPO), an adaptation of the military Intelligence Preparation of the Battlefield (IPB) methodology for the civil setting;[31] the Transaction Analysis Model, and Transaction Analysis Cycle;[32] as well as adaptive analytical red teaming.[33]

Intelligence Preparation for Operations

Intelligence Preparation for Operations (IPO) is a core TEW process. It is detailed in depth in the model TEW Concept of Operations (CONOP) which is preserved in Part Three of the LA TEW Case Stud).[34] IPO, like classic IPB, is at its heart a four-step process:

- Step 1: Define the Operational Space (OpSpace);
- Step 2: Describe the OpSpace Effects;
- Step 3: Evaluate the Opposing Force (OPFOR);
- Step 4: Determine OPFOR & Friendly Courses of Action (COAS).

The IPO process is summarized in Figure 1. The core of IPO is analysis/synthesis (A/S), which is fueled by collection management and aims at developing situational understanding. Throughout the IPO cycle, which is an iterative process, the TEW analytical staff (various types of analysts and subject matter experts) refine their understanding by soliciting various requests for information (RFIs).

- In Step 1, involves understanding the OpSpace or the area to be protected; this includes defining named areas of Interest (NAIs), such as critical infrastructure, that may be targeted and must be protected (from local to global perspectives).

- In Step 2, the effects of various threat scenarios (attacks or incidents of various type) are defined. This includes looking at "geosocial" attributes, such as population, terrain, weather, organizational dynamics, etc. and the use of geospatial information systems/geospatial intelligence and target folders (response information folders) to aide situational assessments.

- In Step 3, the various opposing forces (OPFOR) or potential threat elements (PTEs) and threats (threat vectors) are assessed (at this point AI tools like "non-obvious relationship analysis and generative AI can come to bear). Playbooks to understand the types of threats are used at this step to facilitate an understanding of various threat vectors (cyber, chemical, biological, radiological, nuclear, etc. as well as various influences. Epidemiological intelligence (epi-intel) can be employed to discern between natural disease outbreaks and intentional attacks for example, while adaptive red teaming can be employed to better understand attacks available and potential "kill chains" or attack preparation and delivery sequences. Indications and Warning (I&W) is the goal with "deep I& W" or very early recognition of threat potentials being especially desirable. The window of opportunity for threat detection ids described in this model as the "I&W envelope"

- In Step 4, the analysts anticipate and assess potential OPFOR courses of actions (COSs) while exploring the viability of various friendly COAs these are the disseminated as actionable intelligence in the form of mission folders (used by operational commanders to

develop operations and incident action planes), various warning products (advisories, alerts, and warnings), as well as threat assessments.

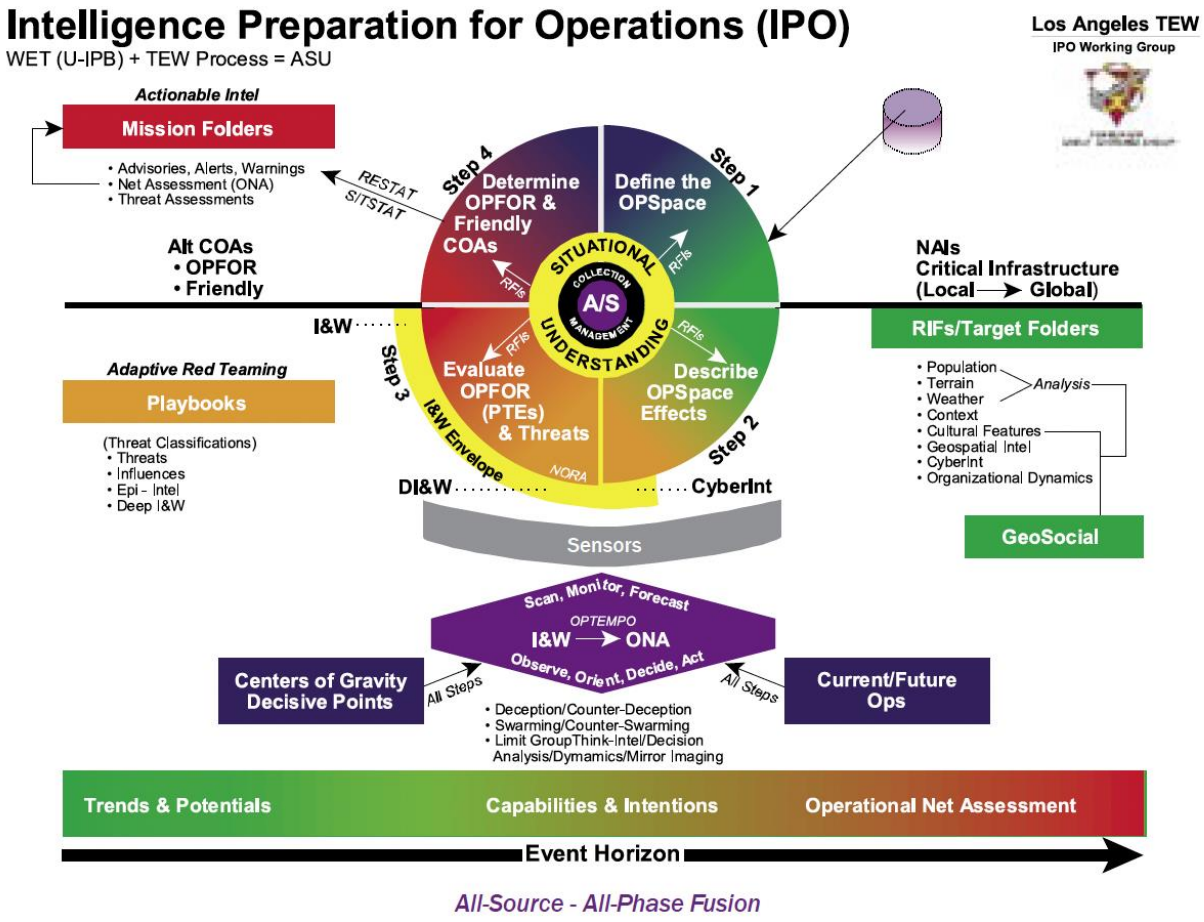

Figure 1. LA TEW IPO Process (National TEW Resource Center, 2005)

The entire TEW IPO process relied upon a series of sensors (human, machine, cyber) to detect the existence of threats and potential threats as part of its all source-all phase fusion process. It also was grounded in an on-going process of scanning the horizon, monitoring suspicious trends and activities, and forecasting potential threats. Depending upon the operational tempo and temporal horizon the processes emphasis would emphasize either I&W or operational net assessment (ONA). This is grounded in the theoretical underpinnings of Boyd's Decision Cycle or OODA Loop where Observation, Orientation, Decision, and Action are key components of achieving situational understanding;[35] analysis/synthesis was at essence the core of Boyd's Orientation phase (and later forms the core of the transaction analysis cycle as formulated by Sullivan.[36]

Deception/Counter-Deception, Swarming/Counter-Swarming, Limiting Group Think and other intelligence/decision analysis dynamics such as "mirror-imaging" were also embedded in the IPO schema. As expressed in the IPO Process the event horizon, or the foreseeable future that analysts could project was depicted in a linear fashion, ranging from discerning Trends & Potentials; assessing an OPFOR's Capabilities and Intentions; and ultimately formulating an Operational Net Assessment. This event horizon is rendered as an iterative cycle in the Transaction Analysis Cycle, which is itself can also be viewed as part of a broader Transaction Analysis Model. First, the Transaction Analysis Cycle is described.

Transaction Analysis Cycle

The transaction analysis cycle is a tool that facilitates sensing and interpreting potential threat activities. It is a non-liner, iterative approach to optimize on-going assessment of unfolding, dynamic situations. Figure 2 provides a visualization of the cycle.

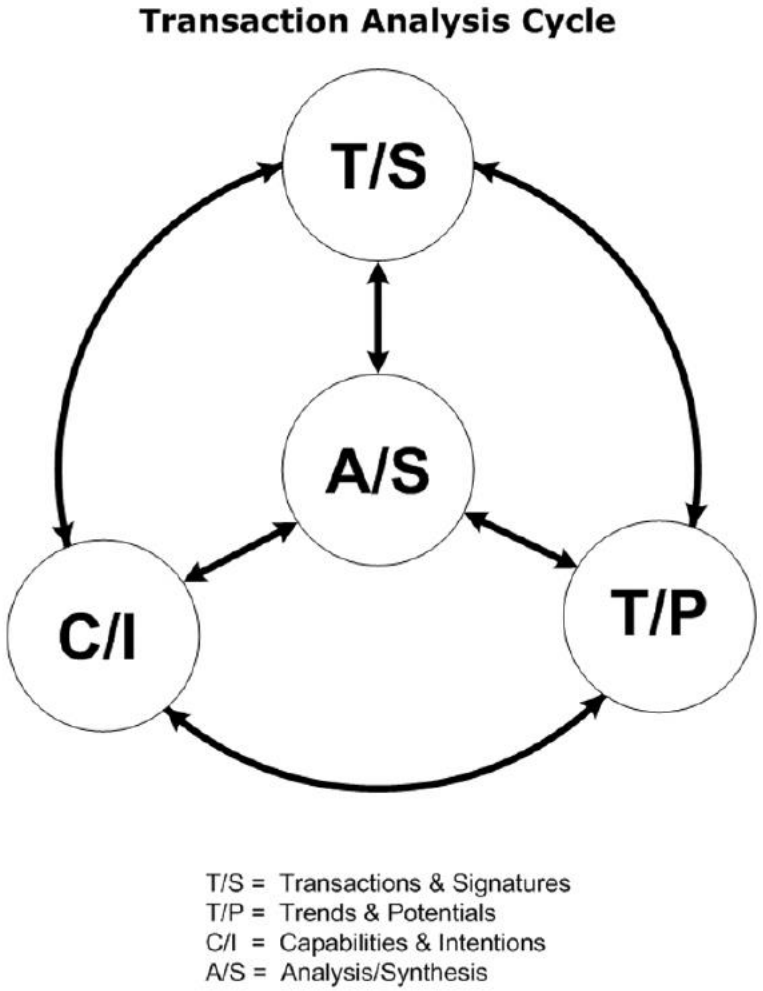

Figure 2. Transaction Analysis Cycle (Sullivan, 2005 & 2008)

The cycle has four interactive actions: 1) Observing individual Transactions & Signatures (T/S); 2) Monitoring sequences and patterns to project Trend & Potentials (T/P); that 3) can be evaluated to assess a specific actor's Capabilities & Intentions; these are all centered upon the Analysis/Synthesis (A/S) function and facilitate group assessment s by individual and distributed (networked) analytical teams enabling the co-production of intelligence. Transact ions are single, discreate acts while signatures place those acts into context. Trends & Potentials place patterns into context and help formulate hypotheses about adversary capabilities & intentions potentially allowing analysts to discern novel and emerging threats and conspiracies.

Transaction Analysis Model

Another way of viewing the TEW process is through the lens of the transaction analysis model. This model is depicted in Figure 3.

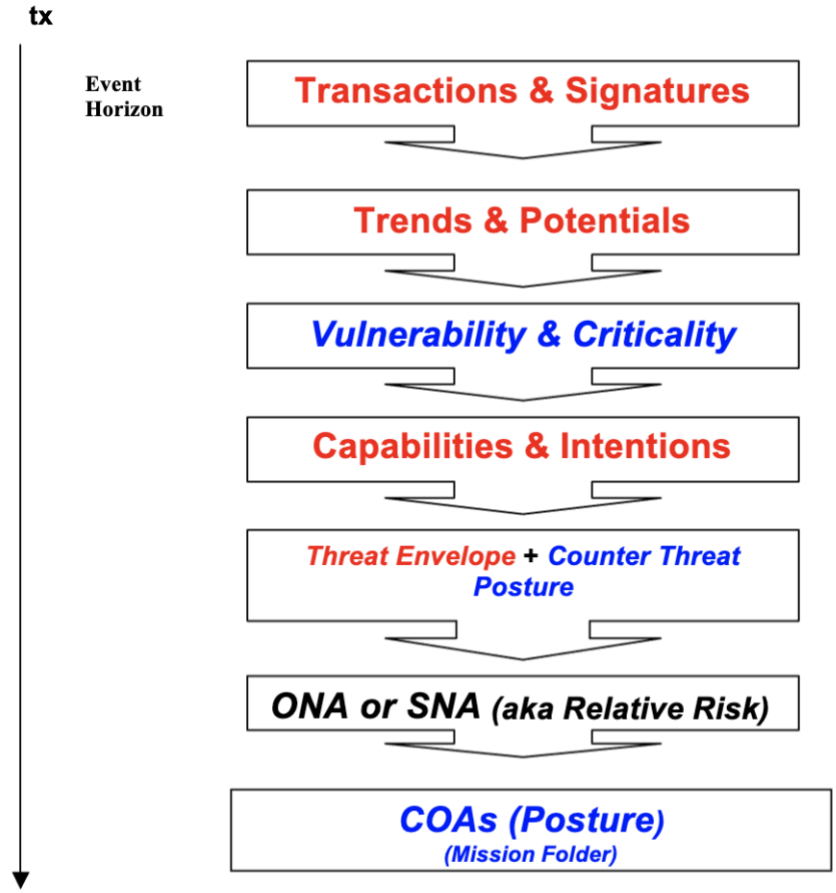

Figure 3. Transaction Analysis Model (Sullivan 2005 & 2008)

The transaction analysis model places the both the IPO Process and the transaction analysis cycle in context. Like IPO, it views time and levels of effort in a linear manner. It starts with the assessment of transactions & signatures (T/S) and trends & potentials (T/P) as the transaction analysis cycle. It then adds assessment of vulnerability of targets and the criticality of those targets if they are attacked. This interim step enables a holistic understanding of the critical infrastructure in an area of interest that may inform adversary targeting preferences. This can then be further assessed to provide current understanding of an OPFOR's capabilities and intentions. Together these illuminate the "threat envelope" or range of potential threats vectors and corresponding actors that can then be mitigated or exacerbated by the current counter-threat posture, Collectively these factors can then be used to perform and both operational or strategic net assessment (ONA or SNA respectively). These net assessments can then inform. The development of alternative course s of action (COAs) to establish a response posture based upon relative risk to a arrange of threat potentials.

Adaptive Red Teaming

Analytical red teaming was one additional tool in the TEW's armamentarium. Adaptive analytical red teaming was a core element of the LA TEW's ability to anticipate and address emerging threats, It was used as an analytical tool and also as means of training the TEW's analytical team during exercises, and supporting incident commanders (unified command) and providing investigative support during operational periods. This range of activities was summarized by Sullivan[37] as:

> To develop analytical skills and explore terrorist attack (kill chain) pathways and avenues of detection and/or disruption, the TEW employed analytical red teaming (placing analysts against an active simulated adversary) to refine tradecraft for indicators and warnings (I&W) for a spectrum of scenarios ranging from current intelligence through strategic foresight. Included in these efforts were two major exercises *Operation Talavera* in 2004 and *Operation Chimera* in 2005 recounted in Sullivan (2013) and Madia (2011). These exercises reinforced the flexible, networked organizational approach described by Rust (2006) that enabled the LA TEW to effectively operate to address a range of threats.[38]

The tools described here can't see the future, since as Naveh noted when describing the role of operational art, the future is a metaphor, but they can allow organizations to consider alternative.[39] In this case alternatives for enhancing sensemaking for novel and emerging threats.[40]

Beyond Radicalization and Counterterrorism

The TEW model has calibrated for counterterrorism, and as a result also effective in recognizing the potentials for and consequences of radicalization and violent extremism =in communities. It also has application in addressing transnational organized crime, activities by criminal armed groups and within both criminal and conventional insurgencies. In the realm of serious organized crime, the TEW model both influenced and was influenced by the Criminal Intelligence Service of Canada's Strategic Early Warning Sentinel (SEWS) methodology.[41] These tools can also be used to address the crime-terror nexus.[42] Essentially, the TEW model was calibrated to address threat convergence.

Conclusion: Networked Intelligence

The LA TEW pioneered the use of all source/all phase intelligence fusion to counter terrorism, and violent extremism. The LA TEW's experience included adapting existing analytical practices developing novel analytic tools to address both emerging and novel threats. These concepts and processes as described in this paper were also used to support public order events, such as riots and disturbances, and support a range of criminal investigations including those involving transnational criminal enterprises. As mentioned earlier in this article, these threats range from the 9/11 attacks (National Commission on Terrorist Attacks upon the United States, 2004) through the *Eme Once* (M-11) Madrid train bombings—a case of criminal-terrorist nexus,[43] the Mumbai attacks,[44] and Sri Lanka's Easter Sunday Massacre.[45]

Extremist and or hybrid criminal-terrorist networks conducted all of these attacks and weak intelligence or intelligence failures contributed to their gravity, In the Sri Lanka attacks, for example, the rise of globally-connected extremist networks fueled exclusivism, extremism, and terrorism,[46] yielding a jihadi hub that ultimately conducted a series of near simultaneous attacks on Churches and hotels in Colombo and other cities in Sri Lanka. Undoubtedly failures to effectively prevent and recognize emerging threats[47] contributed to the tragedy and fueled intense political fallout. Better intelligence fusion efforts and practices may have mitigated these dire events.

Mulltilateral counter-insurgency networks are needed to address the various strains of insurgent and deviant networks that challenge nation states. These include global jihadi insurgencies[48] and criminal insurgencies[49] that alter the nature of governance and state solvency.[50] As Rust (2006) observed, the LA TEW:

> evolved from a small group of actors to a diverse, county-wide network bridging public-private, local-state-federal, and functional divides. The TEW demonstrates an example of organizational problem solving where a network facilitated collaboration in a wickedly complex and uncertain environment. The network's consensus-based innovation,

collaborative processes, and meta-leadership helped the network evolve. These factors strengthened the collaborative ethos of the network and set the stage for success as the network meets current and future challenges. The TEW's bottom-up, consensus-based network expansion contrasts sharply with top-down collaborative approaches, such as the creation of the National Counterterrorism Center and Department of Homeland Security. Lessons from the TEW's well-paced evolution provide insight into how to facilitate collaborative action and build collaborative capacity for the future.[51]

This article was crafted with the hope that future efforts to address gaps in intelligence to counter networked threats, such as extremism in its many guises, and transnational criminal and hybrid threats such as state activity to leverage organized crime, gangs, and mafias could build from these lessons and embrace and further evolve the intelligence practices and analytical processes pioneered by his early intelligence fusion effort.

Endnotes

[1] Fernando Reinares, *Al-Qaeda's Revenge: The 2004 Madrid Train Bombings* (New York: Columbia University Press, 2017).

[2] John P. Sullivan and Adam Elkus, "Postcard from Mumbai: Modern Urban Siege," *Small Wars Journal*. February 18, 2009; John P. Sullivan and Adam Elkus, "Preventing Another Mumbai," *CTC Sentinel*, 2(6), June 2009.

[3] Rohan Gunaratna, *Sri Lanka's Easter Sunday Massacre: Lessons for the International Community (*Singapore: Penguin Random House SEA, 2023).

[4] John P. Sullivan, "From Drug Wars to Criminal Insurgency: Mexican Cartels, Criminal Enclaves and Criminal Insurgency in Mexico and Central America. Implications for Global Security," Working Paper, Nº9, Fondation maison des sciences de l'homme, April 2012, https://shs.hal.science/halshs-00694083.

[5] *The 9/11 Commission report. Executive summary.* National Commission on Terrorist Attacks upon the United States. Washington, DC: National Commission on Terrorist Attacks upon the United States, pp. 9–10, August 21, 2004, https://9-11commission.gov/report/.

[6] Amy Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies," *International Security* 29(4), pp. 78-111, Spring 2005, http://www.jstor.org/stable/4137498.

[7] James J. Wirtz, "Are Intelligence Failures Still Inevitable?" *International Journal of Intelligence and CounterIntelligence*, 37(1), 2023, pp. 307-330. https://doi.org/10.1080/08850607.2023.2214328.

[8] Global Justice Information Sharing Initiative, "Baseline Capabilities for State and Major Urban Area Fusion Centers." Washington, DC: United States Department of Justice, September 2008, p.47.

[9] "National Network of Fusion Centers Factsheet," United States Department of Homeland Security, January 2023, https://www.dhs.gov/national-network-fusion-centers-fact-sheet#:~:text=%22A%20fusion%20center%20is%20a,to%20criminal%20and%20terrorist%20activity.%22.

[10] Stephan A. Loyka, Donald A. Faggiani, Clifford Karchmer, Maureen Baginski, Daniel Bibel, Melvin Carraway, Stuart Kirby, Ritchie A. Martinez, Steve Sellersand John P. Sullivan, *Protecting Your Community from Terrorism: The Strategies for Local Law Enforcement Series, Vol. 4: The Production and Sharing of Intelligence* (Washington, DC: Police Executive Research Forum, February 2005), https://www.policeforum.org/assets/docs/Free_Online_Documents/Terrorism/community%20policing%20and%20terrorism%20vol.%204%202004.pdf.

[11] John P. Sullivan and James J. Wirtz., "Global Metropolitan Policing: An Emerging Trend in Intelligence Sharing." *Homeland Security Affairs* 5(2), May 2009, https://www.hsaj.org/resources/uploads/2022/05/5.2.4.pdf; Gilmore Commission, "Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction. II. Toward a National Strategy for Combating Terrorism." Appendix G—Los Angeles Case Study. Santa Monica: RAND Corporation, December 15, 2000.

[12] Gilmore Commission, p. G-12.

[13] John P. Sullivan and James J. Wirtz, “Terrorism Early Warning and Counterterrorism Intelligence,” *International Journal of Intelligence and CounterIntelligence*, 21(1), 2008, pp. 13–25. https://doi.org/10.1080/08850600701648686.

[14] Gilmore Commission, p. G-18.

[15] Sullivan and Wirtz 2008; John P. Sullivan and Alain Bauer, eds., *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime*, Los Angeles: Los Angeles County Sheriff’s Department, October 2008, http://shq.lasdnews.net/Content/uoa/SHB/publications/TerrorismEarlyWarning.pdf; John P. Sullivan, “Terrorism Early Warning and Co-Production of Counterterrorism Intelligence,” 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, October 21, 2005.

[16] Sullivan and Wirtz, 2008, p. 23.

[17] Sullivan and Wirtz, 2008, pp. 23–24; Lois Pilant, “Strategic Modeling: Los Angeles County's Counter-Terrorism Program is Being Duplicated Nationwide,” *Police: The Law Enforcement Magazine*, 28(5), pp.34–38, May 2004.

[18] Partnership for Peace Consortium (PfPC), *Hybrid Threats and Hybrid Warfare: Reference Curriculum*. NATO Headquarters Brussels, June 2024.

[19] Genevieve Lester and John P. Sullivan, “Calibrating Domestic Intelligence at the 20-Year Mark,” *Homeland Security Today*, November 15, 2021, https://www.hstoday.us/featured/calibrating-domestic-intelligence-at-the-20-year-mark/; John P. Sullivan and Genevieve Lester, “Revisiting Domestic Intelligence,” *Journal of Strategic Security*, 15(1), 2022, pp. 75-105 March, https://doi.org/10.5038/1944-0472.15.1.1976.

[20] John Arquilla and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror Crime, and Militancy* (Santa Monica: RAND Corporation, 2001).

[21] Arquilla and Ronfeldt, p. 15.

[22] Sullivan and Bauer, 2008.

[23] *Resource Guide, Book One: TEW Concept and Overview*. National TEW Resource Center, January 2005.

[24] John P. Sullivan, “The Terrorism Early Warning (TEW) Model for Sensing Novel and Emerging Threats,” *Journal of Intelligence & Analysis*, 22(2), April 2015, Special Edition: Intelligence Canaries: Applications in Strategic Early Warning, pp. 103–117, https://www.researchgate.net/profile/Richard-Cincotta/publication/276920174_Demography_as_Early_Warning_Gauging_Future_Political_Transitions_in_the_Age-structural_Time_Domain/links/59d95cffa6fdcc2aad0d9223/Demography-as-Early-Warning-Gauging-Future-Political-Transitions-in-the-Age-structural-Time-Domain.pdf.

[25] Sunchlar M. Rust, “Collaborative Network Evolution: The Los Angeles Terrorism Early Warning Group.” Master’s Thesis, Monterey: Naval Postgraduate School, 2006, http://www.au.af.mil/au/awc/awcgate/nps/rust_collab_network.pdf; Michael Grossman, "Perception or Fact: Measuring the Effectiveness of the Terrorism Early Warning (TEW) Group." Master's Thesis, Monterrey: Naval Postgraduate School, September 2005, https://apps.dtic.mil/sti/tr/pdf/ADA439375.pdf; William A. Forsyth, "State and Local Intelligence Fusion Centers: An Evaluative Approach in Modeling a State Fusion Center." Master's Thesis, Monterey: Naval Postgraduate School, September 2005, https://apps.dtic.mil/sti/pdfs/ADA439535.pdf.

[26] Gregory O’Hayon and Daniel R. Morris, “Warning in the age of WMD terrorism,” in Peter Katona, Michael Intriligator, and John P. Sullivan, eds.*, Countering Terrorism and WMD: Creating a global counter-terrorism network* (New York: Routledge, 2006).

[27] Sherman Kent, “Words of estimative probability,” *Studies in intelligence*, 8(4), 1964, pp. 49-65.

[28] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge: Cambridge University Press, 2003).

[29] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

[30] Sullivan, IALEIA, 2019, p. 106.

[31] John P. Sullivan, Hal Kempfer, and Jamison J. Medby, “Understanding Consequences in Urban Operations: Intelligence Preparation for Operations*” INTSUM Magazine*, Marine Corps intelligence Association, XV(5), Summer 2005.

[32] Sullivan, 2005; John P. Sullivan, "Analytical Approaches for Sensing Novel and Emerging Threats," Paper at Panel on Novel Risks, Future Threats: The Emerging Global Security Landscape, International Studies Association, *49th Annual ISA Convention*, San Francisco, March 29, 2008.

[33] John P. Sullivan and Adam Elkus, "Adaptive Red Teaming: Protecting Across the Spectrum," *Red Team Journal Occasional Paper* 01, July 2010; John P. Sullivan and Adam Elkus, "Red Teaming Criminal Insurgency," *Red Team Journal*, January 30, 2009; John P. Sullivan, "Analytical Red Team Exercises for Irregular Conflict," *Red Team Journal,* September 13, 2013.

[34] Sullivan and Bauer, 2008.

[35] Chet Richards, "Boyd's OODA Loop" from John Boyd, "The Essence of Winning and Losing." July 28, 1995, https://web.archive.org/web/20110324054054/http://www.danford.net/boyd/essence.htm.

[36] Sullivan, 2005; Sullivan 2008.

[37] John P. Sullivan, "The Terrorism Early Warning (TEW) Model for Sensing Novel and Emerging Threats," *Journal of Intelligence & Analysis (JIA), Special Edition: Intelligence Canaries: Applications in Strategic Early Warning*, 22(2), pp. 103-117, April 2015.

[38] James D. Madia,"Homeland Security Organizations: Design Contingencies in Complex Environments." Master's Thesis, Monterey: Naval Postgraduate School, September 2011, http://hdl.handle.net/10945/5559; Rust, 2006; Sullivan, 2015, p. 114.

[39] Shimon Naveh, in Matt Matthews, "Interview with BG (Ret.) Shimon Naveh," *Operational Leadership Experiences*, Fort Leavenworth, Kansas: Combat Studies Institute. November 1, 2007.

[40] Sullivan IALEIA, 2015, p. 114.

[41] *Strategic Early Warning for Criminal Intelligence: Theoretical Framework and Sentinel Methodology* (Ottawa: Criminal Intelligence Service of Canada [CISC], 2007), http://www.cisc.gc.ca/products_services/sentinel/document/early_warning_methodology_e.pdf.

[4242] John P. Sullivan, "Criminal-Terrorist Convergence: Intelligence Co-production for Transnational Threats," *International Journal on Criminology*, 3(2) Fall, 2015 https://doi.org/10.18278/ijc.3.2.7; John P. Sullivan and Nathan P. Jones, "Intelligence and Analytical Approaches for the Crime-Gang-Terrorism Nexus," *International Journal on Criminology*, 10(1), 2022/2023, Fall, https://doi.org/10.18278/ijc.10.1.8.

[43] Reinares, 2017.

[44] John P. Sullivan and Adam Elkus, "Postcard from Mumbai: Modern Urban Siege," *Small Wars Journal*. February 18, 2009; John P. Sullivan and Adam Elkus, "Preventing Another Mumbai," *CTC Sentinel*, 2(6), June 2009.

[45] Gunaratna, 2023.

[46] Gunaratna, 2023, p. 60.

[47] Gunaratna, 2023, p. 210.

[48] John P. Sullivan and Robert J. Bunker, "Multilateral Counter-Insurgency Networks," *Low Intensity Conflict & Law Enforcement* 11 (2/3), winter 2002, pp. 353-388, https://doi.org/10.1080/0966284042000279081.

[49] John P. Sullivan, "Crime wars: Operational perspectives on criminal armed groups in Mexico and Brazil," *International Review of the Red Cross,*105 (923), August 2023, pp. 849-875 http://dx.doi.org/10.1017/S1816383122000558.

[50] John P. Sullivan, "The Information Age: Transnational Organized Crime, Networks, and Illicit Markets," *Journal of Strategic Security*, 16(1), 2023, pp. 51-71, https://doi.org/10.5038/1944-0472.16.1.2049.

[51] Rust, 2006, abstract.