2008

Terrorism early warning and counterterrorism intelligence

Sullivan, John P.; Wirtz, James J.

Sullivan, John P., and James J. Wirtz. "Terrorism early warning and counterterrorism intelligence." International journal of intelligence and counterintelligence 21.1 (2008): 13-25.

https://hdl.handle.net/10945/59141

International Journal of Intelligence and CounterIntelligence, 21: 13–25, 2008

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850600701648686

Routledge
Taylor & Francis Group

JOHN P. SULLIVAN and JAMES J. WIRTZ

Terrorism Early Warning and Counterterrorism Intelligence

Contemporary terrorist networks challenge state institutions and global security. The 11 September 2001 attacks on New York City and Washington, DC, the M-11 (*Eme Once*) attacks against the Madrid Metro, and the 7 July 2005 attacks on the London Underground highlight the threat posed by transnational terrorism. Extremist organizations, exemplified by al-Qaeda and its affiliates, are complex, nonstate actors. They undertake operations using transnational networks that draw upon a galaxy of like-minded individuals and sympathetic groups. These operations transect traditional boundaries between national security and criminal law enforcement, exploiting the legal and bureaucratic seams between crime and war. In operational terms, the difference between terrorist networks and criminal gangs is actually diminishing as terrorists turn to criminals to help finance their activities, and as criminal gangs come to see terrorists as a new and lucrative market for their goods and services.[1]

The inability of U.S. law enforcement and intelligence organizations to meet this threat is well understood and has been the subject of repeated investigations by blue-ribbon panels and congressional committees in the decade leading up to the 11 September tragedy. Seams clearly existed

John P. Sullivan, a Lieutenant with the Los Angeles Sheriff's Department, is a cofounder of the Los Angeles Terrorism Early Warning (TEW) Group. He currently serves as special projects lieutenant for counterterrorism, intelligence, and emergency operation. Dr. James J. Wirtz is Professor and past Chairman of the Department of National Security Affairs at the Naval Postgraduate School, Monterey, California. He is the editor of the Palgrave Macmillan series Initiative in Strategic Studies: Issues and Politics, and Chairman of the Intelligence Studies Section of the International Studies Association.

between domestic law enforcement and the Intelligence Community that could be exploited by transnational terrorist networks, especially if they managed to set up operational cells within the United States. True reform has been hampered by a lack of interest or commitment on the part of elected officials, bureaucratic inertia, and interagency infighting.[2] The preferred organizational response to this terrorist threat is obvious—the creation of intelligence fusion centers. Indeed, this proposed solution to the threat posed by terrorist networks—development of an ''all source'' intelligence organization among competing agencies—is not novel. The U.S. Navy, for instance, integrated information from a variety of technical sensors and human intelligence sources to monitor the whereabouts of Soviet submarines during the Cold War. Instead of linking different types of widely dispersed sensors together to develop real-time picture of submarine movements, however, all-source counter-terrorism centers would have to communicate with ''first responders'' (police officers, firefighters, public health officials, paramedics and physicians), local, state, and national government and nongovernmental agencies, private corporations, and ultimately the U.S. Intelligence Community.

Today, law enforcement officers and officials involved in the new field of homeland security are working to develop methods and organizations to meet the transnational terrorist threat, especially in major U.S. metropolitan centers. To bridge the gap between the efforts of domestic law enforcement organizations and foreign intelligence agencies to combat the terrorist threat, local officials have created their own ''all-source intelligence fusion'' centers by linking information about local events with warnings provided by the Intelligence Community, officials in the Federal Bureau of Investigation (FBI), and the Department of Homeland Security.

The Los Angeles Terrorism Early Warning (TEW) Group developed a networked approach to intelligence fusion. The TEW Group provides intelligence support to regional law enforcement, fire, and health agencies involved in the prevention of and response to terrorist acts.[3]

COPRODUCTION OF INTELLIGENCE: THE TEW MODEL

The Los Angeles, California, TEW, established in 1996, currently includes analysts from local, state, and federal agencies who produce a range of intelligence products to support a law enforcement response to terrorist and criminal activity. Finished intelligence is intended to integrate information and analysis supplied by a multidisciplinary, interagency team to provide early warning of potential threats. Finished intelligence reports are tailored to users' operational roles and requirements.

At the heart of the TEW is a well-known process known as ''all-source'' fusion, whereby finished intelligence is produced by drawing on all

available sources, including classified sources of information usually drawn from federal agencies; sensitive but unclassified information provided by law enforcement agencies; and open sources that are available on the Internet and library services. The immediate precursor of an attack may be detected in the local area, elsewhere in the United States, in a foreign nation, or in cyberspace. For example, terrorists may plan their attack in Europe while obtaining logistical and financial support in South America or from Southeast Asia. This same terrorist cell could also conduct reconnaissance in their target city in North America, recruit and train operatives in Iraq, and send reports of progress back to operatives in yet another location. Identifying this type of globally distributed threat requires collaborative information fusion among analysts who are located where terrorists operate, plan, or seek to attack. As a node in a counterterrorist intelligence network, the TEW benefits from, and contributes to, this "coproduction" intelligence process. It is a place where information obtained by police patrolling neighborhoods can be integrated with the picture of global events obtained by the Intelligence Community to boost the situational awareness of local officials.

TEW Organization

The Los Angeles TEW is organized into six cells. The "Officer in Charge" serves as the Command cell, providing direction to analytical cells, setting intelligence requirements, and being responsible for interacting with fire or police officers who are in charge at the scene of local incidents. The Consequence Management cell assesses the legal, fire, and health consequences of an actual or a predicted event. The Analysis/Synthesis cell coordinates net assessments of known threats and existing security precautions, and the planned responses to various types of incidents. It also develops an iterative plan for collecting and producing finished intelligence in the form of actionable intelligence products that can be put to good use by local authorities. The Investigative Liaison cell is the critical TEW link to the counterterrorist intelligence network because it maintains the flow of information from local, state, and federal criminal investigative agencies and the national Intelligence Community. The Epidemiological Intelligence cell is responsible for real-time disease surveillance and coordination with public health officials in the event of a disease outbreak or public exposure to toxic chemicals. The Forensic Intelligence Support cell exploits a range of technical capabilities. Analysts incorporate information gathered by traditional police forensic techniques along with data provided by sensors and detectors (deployed to detect chemical, biological, or radiological events) and geo-spatial tools (including

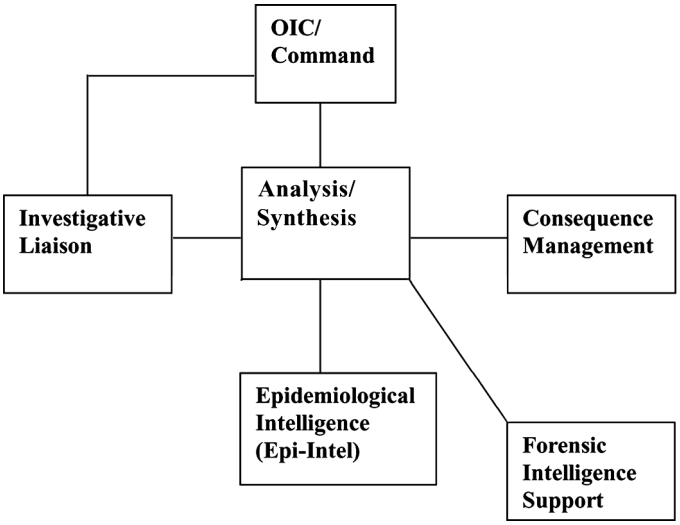

Figure 1. Foundational TEW Organization.

mapping and imagery provided by government agencies and private firms). The TEW organization is depicted in Figure 1.

The TEW has also developed a local network of Terrorism Liaison Officers at each law enforcement, fire service, and health agency in its area of responsibility. These officers are key to generating real situational awareness by providing a link to personnel who interact with the public on a daily basis. Private sector counterparts, known as Infrastructure Liaison Officers, are being established to ensure that security personnel guarding critical infrastructure, landmarks, and major public events can interact with the TEW.

Intelligence Preparation for Operations

Intelligence preparation for operations (IPO) is emerging as a civil analog to intelligence preparation of the battlefield, the military's effort to understand not only the battlefield environment, but also likely opponents.[4] The IPO is a four-step process that provides a standard toolset for situational recognition, course-of-action planning, and response rehearsal. This process bridges the gap between deliberate advance planning and crisis action planning. At the center of the IPO process is analysis, which is intended to produce actionable intelligence. This information and analysis can take the form of ''Mission Folders,'' advisories, alerts, warnings, net assessments, and other tailored intelligence products. The IPO process is depicted in Figure 2.

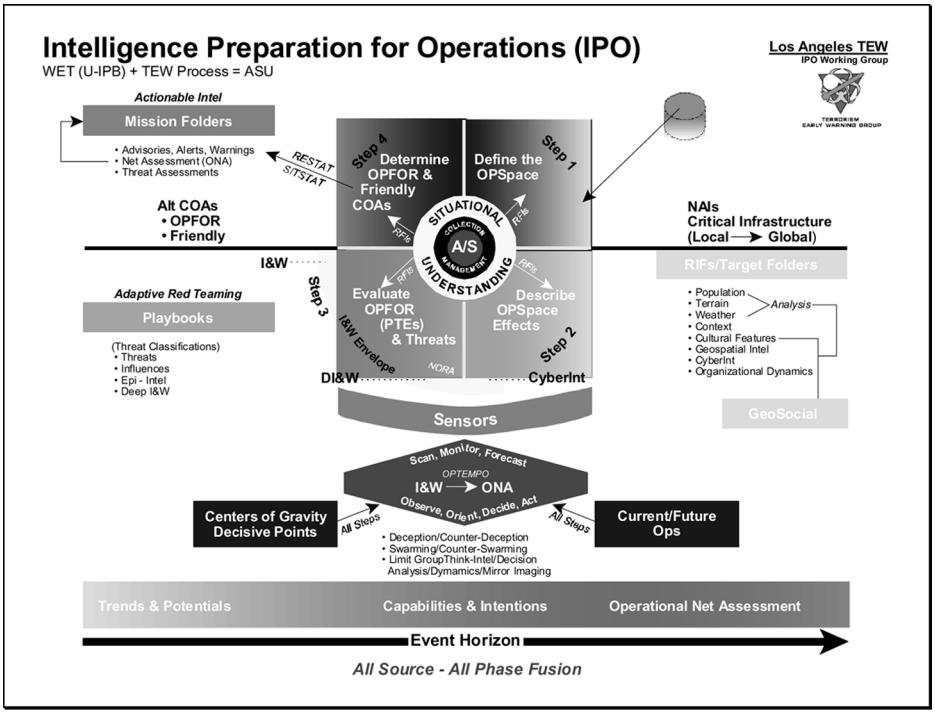

Figure 2. IPO Framework.

The first step of the IPO process is the definition of the operational space. Operational space can include planned events or "named areas of interest," that is, targets that have been identified by terrorist or criminal networks. Once the operational space has been identified, analysts have to direct intelligence collection assets towards that space and conduct further work to assess the critical infrastructure associated with the target. Because critical infrastructure and associated targets may be found not only at various locations around the United States, but in other countries, analysts often have to draw on a variety of assets to develop a realistic depiction of operational areas.

The second step in the IPO Process is to provide basic information about known operational spaces in an easy-to-use format known as Target or Response Information Folders. These folders include information about the local population, terrain, and weather, and historical information about infrastructure and cultural areas. Geo-spatial information, including potential interconnections between unrelated types of critical infrastructure, is provided to identify the potential for cascading events that might exacerbate the impact of some local incident. Social network analysis is also undertaken to understand the social dynamics that might

shape the course of an incident and the effectiveness of the response to a crisis.

The third step in the IPO Process is the identification and evaluation of threatening groups or individuals in terms of the weapons they may employ (e.g., chemical weapons, small arms, explosives, etc.) and the tactics they may adopt in their planned activities (e.g., suicide bombing, etc.). This step is intended to identify a range of threats to populate a ''notional threat envelope.'' With this threat envelope and a list of potential targets, production of an ''Indications and Warning'' protocol that matches potential threats with the factors shaping the behavior of opposing forces becomes possible. By employing advanced social network analysis and related tools, such as ''nonobvious'' relationship analysis, production of Indications and Warning indicators also becomes possible by identifying terrorist potentials, and by observing the transactions and signatures associated with assembling a ''terrorist kill chain.''

The fourth step in the IPO process develops potential courses of action for both opposing and friendly units. This can be a complicated matter, given the large number of agencies that might supply personnel in response to an incident, and the varying status of their units, based on the tempo of ongoing operations. By bringing this type of analysis to the attention to the various agencies involved in responding to a terror incident, government officials across the city of Los Angeles can begin to assess how well their training and contingency planning matches the estimates of potential threats.

IPO requires talented analysts who possess a working knowledge of intelligence processes, capabilities, and practices. Analysts must understand deception and counter-deception, as well as an understanding of the challenges posed by the relationship between intelligence analysts and policymakers, and some common intelligence pitfalls, such as the dangers of group think and the need to avoid mirror imaging. Analysts need to search for opponents' ''centers of gravity'' and ''decisive points'' to maximize the impact of friendly operations, while minimizing the material and personnel demands involved in routine operations. IPO also requires a steady flow of raw intelligence reports from a wide variety of sources: data from remote monitors, citizens' reports of suspicious activity to community police, other types of human collection, Internet scanning, signals intelligence, and forensic intelligence support. Sometimes these sources require real-time monitoring or virtual reach back from multisensor arrays or field reconnaissance capabilities (e.g., chemical detectors and cameras placed at strategic locations).

IPO can occur at any point along a notional ''Event Horizon,'' the passage of time that occurs between the conception and execution of a terrorist activity. IPO can focus on three distinct phases of an event horizon by concentrating on Trends and Potentials, Capabilities and Intentions, and

ultimately conducting an Operational Net Assessment to evaluate contingency plans against known or even expected threats.

Transaction Analysis Cycle

Terrorist activity, which plays itself out over time, can be expressed in a linear fashion as an event horizon, or in a nonlinear fashion, as an ongoing process that may produce a variety of alternative outcomes. The "Transaction Analysis Cycle" (TAC) as developed is a nonlinear analytical approach for discerning terrorist activity using dynamic and diffuse data sets laden with noise and masked by a fog of uncertainty. The Transaction Analysis Cycle (see Figure 3) emerged as a way to teach analysts how to interpret activity to assess leads and information while developing iterative collection plans to identify patterns and define hypotheses about a potential terrorist "kill chain," a specific series of events leading up to the actual execution of a terrorist action that produces casualties or damages valuable assets.

The TAC seeks to identify patterns of activity by incorporating analysis or a synthesis of available information. Utilizing this framework, analysts can observe and assess activities or transactions conducted by a range of individuals by looking for known indicators or precursors of many types of terrorist or criminal activity. Many patterns reflect common and

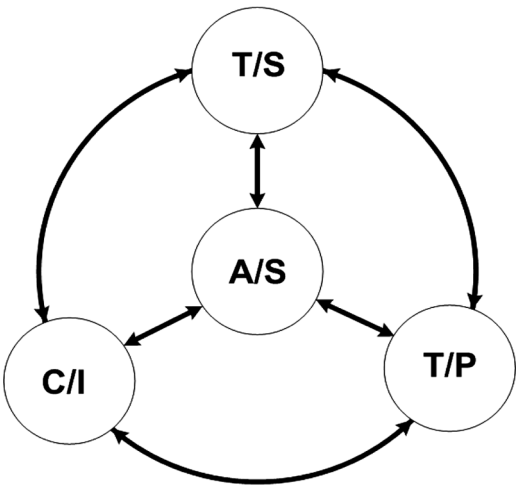

Figure 3. Transaction Analysis Cycle.

well-known criminal or terrorist modus operandi; others reflect unique types of activity adopted by specific organizations. For example, acquiring financial resources, either through nefarious or illegitimate transactions, expertise, materials, or munitions can indicate that a terrorist organization is developing a significant operational capability. Indications of more advanced preparations can include recruiting members, conducting reconnaissance, mission rehearsal, or the actual initiation of an attack. These ''transactions and signatures'' can then be observed, matched with patterns of activity that can be expressed as ''trends and potentials,'' which can ultimately be assessed in terms of specific ''capabilities and intentions.'' Once these templates have been developed, an analytical team can posit a hypothesis concerning the pattern of activity that had been observed, and then develop a collection plan to seek specific evidence that confirms or disconfirms its hypothesis.

Because terrorist or criminal gangs can be well along in some operation before they generate detectable evidence, analysts must be prepared to identify specific trends, potentials, capabilities, or intentions from just about any starting point in their opponents' planning and operational cycle. 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 appropriate courses of action. The Transaction Analysis Cycle thus 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 possible the coproduction of intelligence and the development of a common picture of the operational area.

THE TEW IN ACTION

Although most TEW operations involve highly sensitive law enforcement information or classified data provided by federal law enforcement agencies, two series of incidents have been made public that highlight how analyses produced by the TEW have increased situational awareness among police officers and first responders. In the first cluster of events, a series of hoaxes involving ''anthrax'' that occurred in the Los Angeles region in 1998, TEW analysts accurately anticipated events on the ground, but their estimates were given short shrift until they were validated by experience. In the second series of events, involving security for the Democratic National Convention held in Los Angeles in 2000, the TEW was a source of data fusion that helped police head off violent confrontations before they could get started, while helping law

enforcement officers develop situational awareness across a wide and complex series of overlapping jurisdictions.

''White Powder'' Hoaxes

The first events center on a series of hoaxes, which started in Wichita, Kansas, on 18 August 1998, involving white powders that were purported to be anthrax. In the aftermath of the media attention garnered by this incident, copycats began to emerge in Colorado Springs, Colorado (15 October), Jacksonville, Florida (3 November), Miami, Florida (20 November), and in various locations across Indiana in November 1998. These events did not go unnoticed by analysts at the TEW. In November they had reached the conclusion that anthrax hoaxes were coming to Los Angeles. This judgment was formalized in a policy advisory, ''Responding to Potential Weapons of Mass Destruction (WMD) and Anthrax Threat Incidents,'' which was disseminated across the entire Los Angeles Police Department (LAPD) on 12 December 1998.

Five days later, the first hoax occurred in Los Angeles when an employee of the Executive Parking Company received an anonymous letter stating that the employee had just been exposed to anthrax. The LAPD, Los Angeles Fire Department, Los Angeles County Hazardous Material Teams, and the FBI all responded to the report. Despite the fact that the TEW had warned of the possibility of a hoax, the on-scene commanders decided to launch a full-fledged response to the incident: hazardous materials (HAZMAT) technicians donned maximum protective gear, decontaminated 25 employees on-site (which involved stripping individuals and scrubbing them with a bleach solution), and transferred the employees to a local hospital where some of them were decontaminated for a second time. All involved were given a week's supply of antibiotics. Not until some 48 hours later was it determined that no anthrax spores were present at the site. The response to the incident cost the City of Los Angeles over a half–million dollars.

On 18 December 1998 a second incident, at the U.S. Bankruptcy Court, was reported. In response, the building was evacuated. As tests for the presence of anthrax were conducted, authorities identified 105 people who were at risk of exposure. These individuals were kept isolated for eight hours, but a growing awareness of the possibility of a hoax led officials to forego on-site decontamination. The detainees were allowed to go home, armed with prescriptions for antibiotics, and instructions to shower. The courthouse remained closed for about two days, and the total cost of the response was again over a half-million dollars.

The next hoax occurred in Van Nuys. On 21 December 1998, an anonymous caller claimed that anthrax had been released, leading to the

evacuation of the municipal and superior courthouses. Although over 1,200 individuals were evacuated, and the buildings were searched and tested over a five-hour period, no prescriptions were issued, and evacuees were given instructions on self-decontamination techniques. The courthouses were closed for 48 hours while tests were completed. When a similar event occurred at the Time-Warner corporate offices on 23 December, about 70 evacuees were isolated for six hours as the structure was searched and sampled. The building, however, was reopened following the completion of search operations.

As additional incidents occurred throughout the rest of December 1998, officials realized that the TEW estimate had become a reality. Los Angeles faced a series of ''white powder'' hoaxes that were being fed by media coverage of earlier evacuations. In response, TEW participants involved in anthrax incident response met to develop new protocols to deal with reports of contamination—responses that would prove to be less costly and intrusive and, as a result, less likely to create new copycats. Of paramount concern were the human and material costs involved in launching a full-scale response to all incidents, and the possibility that continuation of the practice could lead to real tragedy: assets responding to a hoax would not be available in the event of a real emergency. By early January 1999, TEW participants had developed a new set of indicators to assess the credibility of reports of ''anthrax'' and a new set of protocols governing the actions of emergency responders. These new, more effective, protocols were in effect when the anthrax hoaxes again broke out in Los Angeles in 2001.[5]

The 2000 Democratic National Convention

Held in Los Angeles from 7 August to 18 August 2000, the Democratic National Convention (DNC) attracted tens of thousands of delegates, members of the media, and protestors. Because the DNC was designated a National Security Special Event, the U.S. Secret Service was given responsibility for devising a security plan for the convention. Given the large number of sites housing participants and events, responsibility for handling incidents at specific locations was given to local police, fire, and first aid units. The Los Angeles County Sheriff was responsible for mutual aid and for coordinating responses to large scale incidents. As a major national event, the DNC involved personnel and resources from federal, state, county, and local law enforcement, fire, and medical agencies.

Because the DNC was expected to attract all types of groups and protestors, the TEW was charged with monitoring events not only within Los Angeles, but also across the United States and in other countries. TEW analysts hoped to anticipate incidents that might disrupt the

convention. The TEW was charged with developing a ''big picture'' by detecting patterns in day-to-day events. If these trends could be recognized in time, officials hoped that action could be taken to head off trouble before it started and resources could be staged in locations where they might be needed. The TEW operated as a fusion center: it monitored reports from the intelligence center maintained by the Los Angeles Police Department, law enforcement personnel operating in the field, fire units, classified reports provided by federal authorities, and open-source reports provided by local and national media. The TEW also monitored the ongoing operations undertaken by the Multi-Agency Coordination Center, the U.S. Secret Service, and the Joint Operations Center, operated by the Federal Bureau of Investigation.

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.[6] TEW helped make the DNC a safe event for everyone. According to Michael Grossman, ''Because field commanders knew what to expect from the hard-core demonstrators at the convention site, they were able to readily identify negative actions and intervene accordingly... . The public was protected and lawful citizens were able to participate in peaceful demonstrations.''[7]

A NATIONAL MOMENTUM

The TEW model is scalable and adaptable. From its initial implementation in Los Angeles, the TEW concept and network has been adopted and modified to fit local needs in various places around California. Riverside/San Bernardino, Orange County, Sacramento, San Diego, and East Bay (Oakland, Alameda, and Contra Costa counties) are in the process of creating fusion centers to provide finished intelligence, planning, and

real-time awareness of potential operational areas for local police and first-responders. State and local officials from other parts of the United States also have found the TEW concept attractive. Pierce County, Washington; Tulsa, Oklahoma; New Orleans, Louisiana; Cincinnati, Ohio; Albuquerque, New Mexico, and the Territory of Guam all have prototype or working fusion centers that link state and local officials with federal law enforcement and intelligence agencies. These individual nodes are coalescing into a national network, sharing information among TEWs, state fusion centers, and other interested entities. The creation of this national network is supported by technical assistance sponsored by the U.S. Department of Homeland Security's (DHS) Office of Domestic Preparedness. DHS help has included doctrine development and the sponsorship of state and local workshops to further TEW practice and analytical tradecraft.

Although the TEW model demonstrates that networked fusion is possible, a number of challenges remain. No matter how well conceived or operated, TEW centers often serve as a lightning rod for the resistance and hostility of existing government agencies. The response to the initial "anthrax" hoaxes in Los Angeles is a case in point: first-responders ignored accurate assessments in favor of maximum responses to what ultimately was deemed a false alarm. As networked organizations, fusion centers are inherently at odds with their traditional hierarchical predecessors. But bureaucratic inertia, combined with the protection of organizational domains and missions, slows collaboration, both within and especially across disciplines, jurisdictions, and nodes. Competition over resources and the struggles for intra-governmental primacy also complicate efforts at collaboration.

Coproduction of intelligence to meet a dynamic domestic terrorist threat requires the development of multifaceted organizations. Much of the information necessary to identify the nature of this changing threat, indeed, even to recognize that a threat exists, is often provided by operators in the field and from officials located in other jurisdictions. The multilateral exchange of information, including indicators of potential attacks and alliances among networked criminal actors, are needed to counter the networked activities of contemporary criminal and terrorist adversaries. Analysts also have to be supported by new analytical tradecraft, processes, and policy if they are going to be able to identify nefarious activity before the point of "no-return": the moment when officials can no longer put warning of an impending event to good use. Organizations have to be prepared to exploit lateral information-sharing produced by distributed intelligence processing; new technical and procedural mechanisms for sharing information among local, state, federal, and international nodes have to be developed. The TEW, though no panacea, is an important step in providing government officials and law

enforcement officers with the information they need to stop the next terrorist incident.

REFERENCES

[1] Thomas M. Sanderson, ''Transnational Terror and Organized Crime: Blurring the Lines,'' *SAIS Review*, Vol. 24, No. 1, 2004, pp. 49–61.

[2] Amy B. Zegart, ''An Empirical Analysis of Failed Intelligence Reforms Before September 11,'' *Political Science Quarterly*, Vol. 121, No 1, Spring 2006, pp. 33–60.

[3] 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; 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.

[4] 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.

[5] Second Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *II Toward A National Strategy for Combating Terrorism*, 15 December 2000, p. G 12–14.

[6] Michael Grossman, ''Perception or Fact: Measuring the Effectiveness of the Terrorism Early Warning (TEW) Group,'' M.A. thesis, Naval Postgraduate School, Monterey, CA, September 2005, pp. 45–50.

[7] Ibid., p. 50.