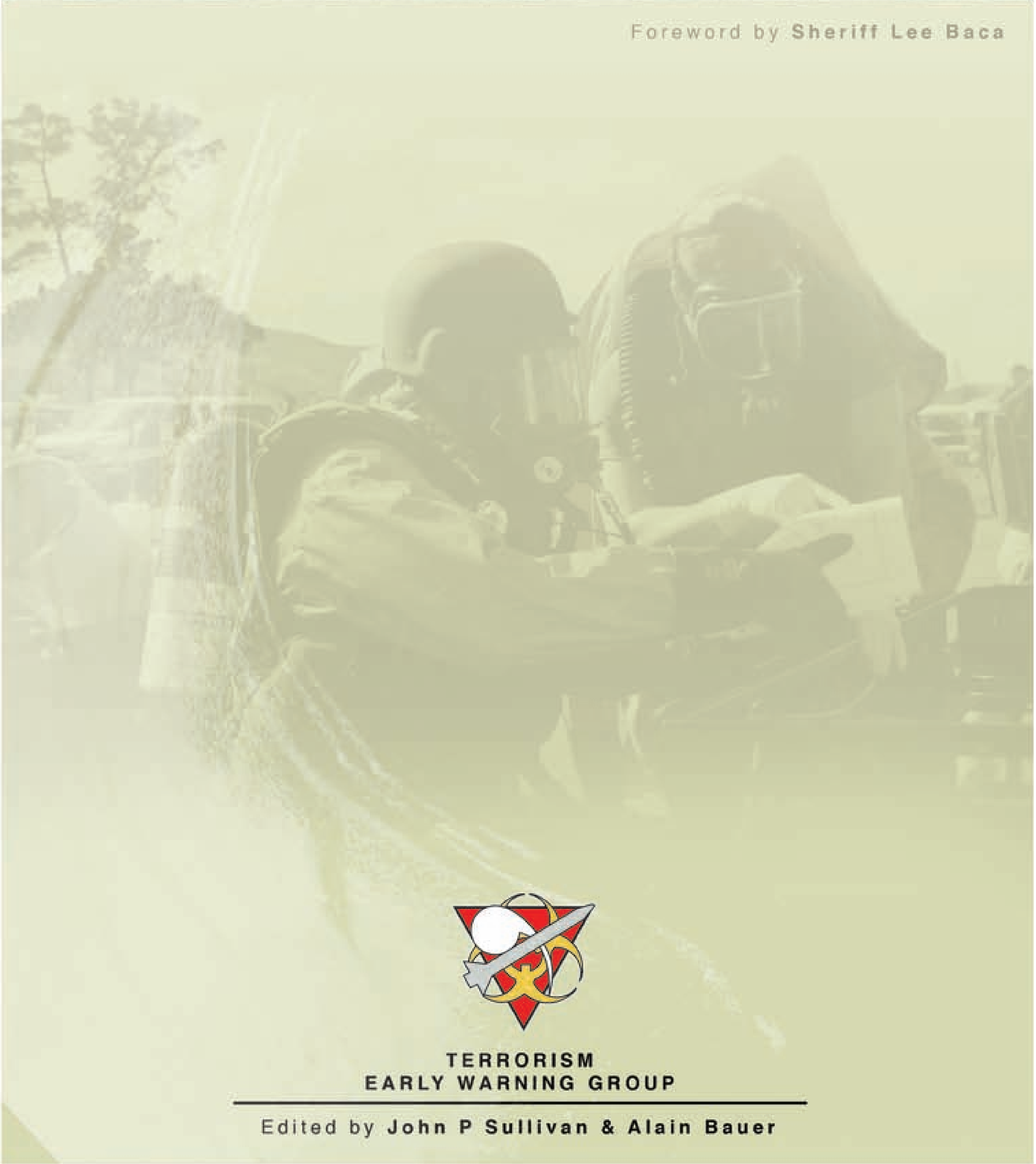
Terrorism Early Warning

10 Years of Achievement in Fighting Terrorism and Crime

TERRORISM EARLY WARNING

10 YEARS OF ACHIEVEMENT IN FIGHTING TERRORISM AND CRIME

Foreword by **Sheriff Lee Baca**



TERRORISM
EARLY WARNING GROUP

Edited by **John P Sullivan & Alain Bauer**

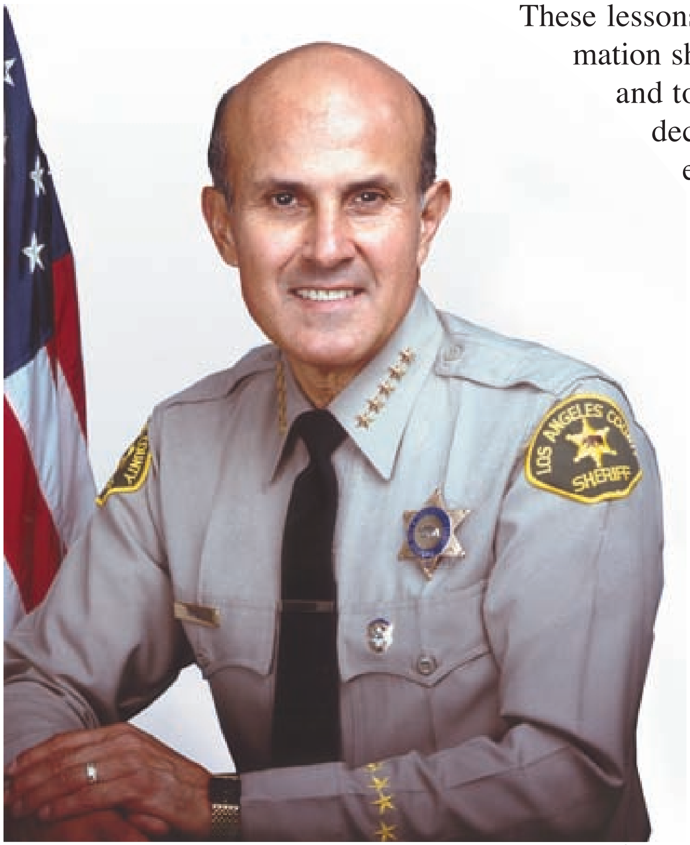
Published by the Los Angeles County Sheriff's Department, Los Angeles, California, October 2008.

Forward

Terrorism is an issue of concern to law enforcement agencies and the communities they serve. Since the 9/11 attacks, law enforcement agencies are increasingly called upon to assist in the prevention, response to, and investigation of criminal conspiracies which support extremist movements and terrorist groups. To be effective in addressing terrorism, police must work closely with their communities and among themselves. They must also learn new skills and work with new partners. This requires a great degree of understanding: of the threat, of communities, of analytical approaches and intelligence. These must be combined effectively and appropriately while nurturing and maturing public trust.

The communities served by the 19,000 sheriff's and police departments in the United States and our colleagues abroad deserve a clear and continuing trust-based relationship with their police. I call this "Public Trust Policing." This requires law enforcement agencies to foster an inclusive and open system of public participation in the public safety mission. Five principles are instrumental to this endeavor. These principles which are also applied throughout this book are: Public Participation, Core Values, Leadership, Education, and Transparency.

This book is unique. Its co-editors Alain Bauer and John P. Sullivan have assembled an important work. Together with their co-authors Xavier Raufer, Andre DeMarce, and Brian Michael Jenkins, they tell an important story. It is rigorous in scope and international in depth. It brings together academic specialists and law enforcement practitioners to capture the history and share the lessons learned by the Los Angeles Terrorism Early Warning Group (TEW). The TEW model, first developed in Los Angeles in 1996, is the forerunner of the emerging national and global network of fusion centers (like the Joint Regional Intelligence Center in Los Angeles). This book chronicles the experience and leadership of its participants from law enforcement, the fire service, public health, medical, and emergency management, and the private sector to share and develop the information necessary to craft a regional response to terrorism by local, state, and federal partners.



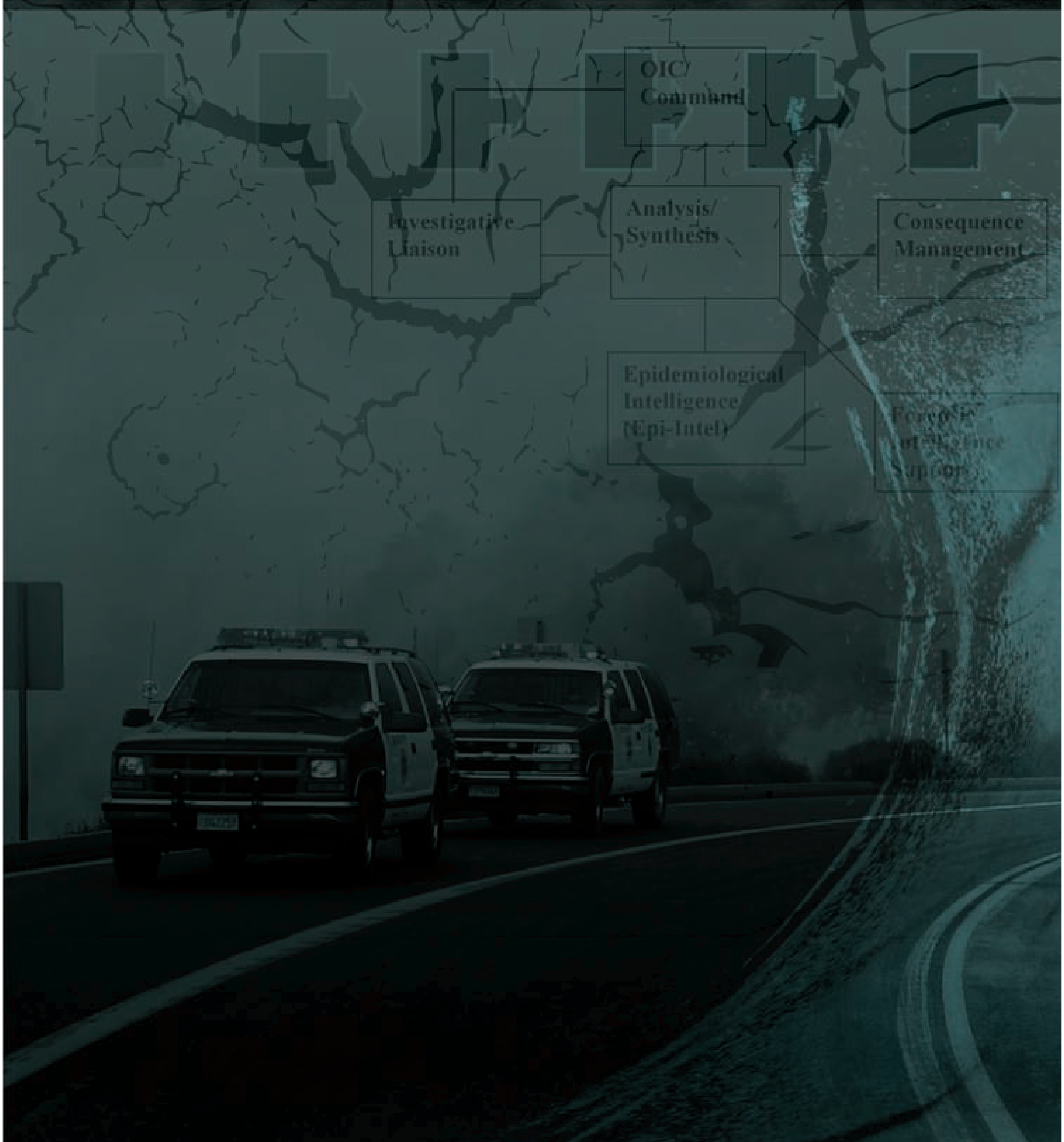
These lessons learned demonstrate a need for more than information sharing. They point to the need to apply both skills and tools to develop the knowledge needed to support decision-making at all levels. This book places these experiences in context and provides a foundation for educating future analysts and decision-makers, and sharing this practice across organizations. Finally, it makes these arcane and complicated processes available to the public, ensuring the transparency necessary for maintaining the public trust necessary to counter terrorism and serious crime. I am proud to share this book with our law enforcement and community partners worldwide.

Leroy D. Baca, Sheriff

TABLE OF CONTENTS

PART ONE:

INTRODUCTION/STRATEGIC CONTEXT



I. Introduction: The Los Angeles Terrorism Early Warning Experience

Alain Bauer and John P. Sullivan

We live in an era marked by the impact of virulent forms of crime, organized and transnational crime, but also imported and homegrown terrorism, and insurgency. In this environment, accurate intelligence and emergency management procedures are more important than ever. National intelligence and response systems need to evolve and cope with the threats.

As counter-terrorist expert John Robb argues in his book *Brave New War*, the key to survival is developing local procedures for civil defense. To advance Robb's point further, cities do not just need Emergency Management Teams, bomb squad techs, tactical units, and other emergency responders. They need to be able to collect, process, analyze, and disseminate intelligence on possible sources of civil disorder and use such information to shape the operating space. To do so requires a new method of thinking about intelligence and emergency responses, one that borrows from the best of law enforcement and military practices yet draws on the experience and insight from the medical and scientific communities, academia, and the private sector.

The purpose of this book is to highlight one successful effort to forge this new mode of defense: the Terrorism Early Warning Group (TEW). Contained within is a wealth of information on the new operating environment for military and law enforcement professionals, an overview of the theories behind TEW intelligence, a concept of operations (CONOPS) for TEW operations, and a list of relevant resources for further reading.

Alain Bauer and Xavier Raufer start off in Part One, Chapter II with an essay chronicling the history and development of the hybrid form of terrorism, crime, and global insurgency that has developed in the wake of the Cold War.

Part Two, Chapter I features a succinct history of the TEW's operations and a brief overview of its functions.

Part Two, Chapter II contains several essays by the TEW's co-founder, Lieutenant John P. Sullivan outlining the theory and practice of TEW operations. Also included in Part Three is a case study outlining the procedures for TEW intelligence co-production and emergency response to terrorist incidents, as well as a glossary of TEW terminology and bibliography of recommended writings on terrorism, urban operations, transnational crime, and intelligence. Part Four is an assessment of the TEW's contribution by Brian M. Jenkins.

Part Five contains an annotated bibliography of writings by Lieutenant Sullivan and many other figures on the TEW process, as well as other issues associated with law enforcement intelligence fusion. It also features a comprehensive list of individuals who have briefed before the TEW, and includes an annotated guide to large-scale TEW conferences.

We hope that this text can serve as a guide to the construction of a new mode of American intelligence and defense, one that eschews large Soviet-style bureaucracies in favor of a network of smaller units that can collaborate and thrive in today's new operating environment. To quote the late United States Air Force fighter pilot John Boyd, the TEW model is a formula for continued "vitality and growth" in a rapidly changing world.

II. NEW CRIMINAL AND TERRORIST THREATS: NEWS FROM THE GROUND

Alain Bauer and Xavier Raufer

In November 1989, a historical parenthesis opened. It closed in September 2001.

In the interim, the developed world felt the disorder and violence of the world but was saved from any major conflict. For the most part, the developed countries were at peace. Thus, during the turning point, the population of these countries showed little interest for the global chaos. It thought its tranquility was durable and definitive. No one really listened to the warnings: *"Peacetime is superficial, since public order seems assured, one turns to society's problems; leaders are judges on the basis of the media presence rather than on their public performance. Such periods never last very long."*[1]

Here is the chaotic world now. And now that the dust raised by the fall of the Berlin Wall has settled, now that the historic parenthesis is closed, we discover that the crucial issue in terms of global security is henceforth that of terrorist and/or criminal war, now on a strategic scale.

In conventional international law, the State is the only subject of history. It holds the monopoly for legitimate violence and as a result only inter-state wars are "real" wars. But the inter-state wars are a disappearing breed:

- Nuclear dissuasion has made them too dangerous, notably between major powers;
- The democracies (more numerous than before) avoid fighting each other; and
- The development of the economy and technologies since the middle of the 20th century makes the acquisition of territory by military means less important than in the past.

Until the end of the Cold War, the extreme limit of the inter-state war game was the indirect strategy, all the maneuvers allowing the enemy's battle formation to be split apart. At the dawn of the 21st century, the logic of the indirect strategy is outdated, inapplicable in a world where yesterday's clear distinctions between attack and defense, State and civil society, public and private domain, civilian and military, war and peace, police and army, legal and illegal have been erased a little more. New forms of confrontation have emerged and the determining factor is no longer ideology or the nation but race, tribe, greed or religious fanaticism.

Chaotic Wars, Terrorists and Criminals Emerge

At the beginning of a new era, the major difficulty consists in seeing who the enemy will be, what the battlefield will be, and what the rules of war will be (if there are any) early enough.

In June 1962, at the military academy of West Point, President John F. Kennedy gave a good example of this foresight by defining the guerilla warfare as follows: *"it is a new form of war, new in its scale but whose origin is old…conducted by guerillas, subversives, rebels, assassins: a war of ambush and not battle, of infiltration and not aggression, where one wants to win by exhausting the enemy not attacking it. To confront this form of warfare, we need a new strategy, totally different forces and, as a result, an awareness of the phenomenon and entirely new and original training."*

[1] Robert D. Kaplan, "Kissinger, Metternich and Realism", *The Atlantic Monthly*, June 1999.

In today's chaotic world, war is no longer conducted by one State against another and as a result, it becomes increasingly ferocious: those we face fight most often for what man considers to be the most essential, most sacred, his blood (life, bloodline, family, clan) and soil (house, territory).

The chaotic war is also polluted, penetrated by crime, tribalism, and terrorism. Even more, the adversary is a hybrid, part "ordinary law" and part "political." A warlord, clan chief, or a fundamentalist, fanatical religious dignitary whose militia or terrorist network is financed by racketeering, trafficking in human beings, weapons, drugs, rare or protected species and toxic waste. (An example is the infernal spiral in which a number of sub-Saharan African countries find themselves in: "stranding" of the nation-states; multiplication of armed gangs, non-ideological guerrillas, and the subsequent "gang wars," escalation of organized crime, tribalism, reign of the warlords, culture of impunity, etc.).

"Civil war becomes one with the most abject criminality" states Oswaldo de Rivero, a high official of the United Nation, in the "Monde Diplomatique" of April 1999. For him, the *"national non-viability of many developing countries"* is causing the nation-state to implode into *"ungovernable chaotic entities,"* where the *"alliance of general anarchy and diverse delinquency reign."*

Characteristics of the Chaotic Wars:

- Abolition of the marked-out geo-strategic space in which the national defense of major countries evolved.
- Drastic decrease in the number of States that respect the current international rules in effect. As a result, the non-recognition of States or borders by at least one of the two parties to a conflict, due to the weakening of the concept of the nation-state with continuous and controlled borders on three continents.
- End of the distinction between military and civilian, front and rear; rarefaction of militias that still wear the semblance of a uniform.
- Complex human environment: necessity of confronting a dispersed adversary, lost in the population, often mixed in with friendly forces.
- Absence of conventional battles in an empty countryside, but constant with massacres, bloody vendettas (Albania, Algeria, Chechnya, former Yugoslavia), and a succession of terrorist episodes.
- Use of armed forces of developed countries, more for police action, aid and assistance missions and other "stabilization operations" than for military combat.

All of this occuring in the middle of a criminal whirl where trafficking in drugs, nuclear substances, individuals (whole, illegal immigrants; or in parts, sale of organs), "sensitive" electronic components, precious gems ("war diamonds") and weapons intermingle with the confrontation of religious, ethnic or tribal fanaticisms, civil war or famine, maritime or aerial piracy.

A New Terror, Now Unclear and Sudden

During the historical parenthesis of 1989-2001, the nature and pace of terror changed. Before, the threat was heavy, slow, foreseeable and explainable. Let us take for example the Revolutionary Council-Fatah of Abou Nidal: everyone knew the host country and which weapons and explosives it used. It was child's play to "break the code'' of the signature it used to claim credit for its actions. Today, however, terror is brutal and sudden, short-lived, and often irrational, for instance the case of al-Qaeda, the Aum sect or the Algerian Armed Islamic Group (GIA).

On the basis of these premises, three questions arise which we will try to answer one by one: Where will we fight? Which are the truly dangerous entities of world chaos? Finally, how will we fight?

1) Where are we already fighting, where will we fight? "Urban Jungle" and "Concrete Forests"

"Urban areas form a terrain that is particularly complex for combat…The losses in urban areas are higher than in open terrain. Even if the military prefers to avoid the subject, it must be dealt with in the end since it is most likely one of the preferred terrains of our future opponents. A way for the future enemy to counterbalance the technological and numerical superiority [of the United States] will be to hide in the cities and masses…the urban environment is multi-dimensional. It includes the ground, underground and the third dimension (each building can hide enemies). This environment reduces communication capabilities (metal and concrete structures)… The Soldier is aware of these difficulties that affect his mental state. Furthermore, urban areas are always more populated (in 2025 nearly 70 percent of the world's population will live in cities). The population of cities may exceed ten million. Infrastructure problems and social needs may aggravate the problem…in the last twenty years, one-third the American military deployments occurred in urban areas. This figure is rising. This environment places all the participants on equal footing, whatever their technological capabilities" (Future Warfare, US Army War College, May 1999).

Since the end of the Cold War, and during the entire historical parenthesis of 1989-2001, uncontrolled spaces multiplied. Sixty years ago, Paul Valéry celebrated a new, ordered and marked out world: *"the time of a finished world is beginning."* But the trend was far from irreversible: the finished world will have lasted half a century. Chaotic territories and areas out of control, but also and above all, the "concrete jungles" surrounding the Southern "megapolises."

In the year 2000, there were 414 cities on the earth with more than one million inhabitants, 264 of them in the third world. In 1950, Africa counted six cities of one million inhabitants, 19 in 1980, and 50 in 2000. In 2015, there will be 33 "megapolises" of over 8 million inhabitants, 27 of them in the third world – there were only two in 1950.

In 2020, all the so-called "developing" countries will count over 6 billion inhabitants, half of which will be urbanized. They will be, reiterates Oswaldo de Rivero, (op. cit.), "Dilapidated megapolises where water will be scarce and food and energy too expensive for the average salary. These pitiable cities will then probably become true human hells, ecological time bombs, real threats for the political and ecological stability of the world."

This is how most of the inhabitants of these southern "megapolises" will live, or rather those of the shantytowns, the "favelas," and the slums that develop twice as quickly as "conventional" urbanization, which is already considerable. Thus, in 2000, 80 percent of current population of Addis Abeba in Ethiopia lived in shantytowns, as did 70 percent of the population of Casablanca (Morocco) and Calcutta (India), and 60 percent of the inhabitants of Kinshasa (Zaire) and Bogotá (Colombia).

But these "asphalt jungles" are extremely volatile: here and any second, as Mao Tse Tong used to say, "a spark can set fire to the entire plain." Hence, the extreme difficulties of intervening to repress an insurrection or eradicate drug traffic, all this within proximity of international airports, thus, of CNN's cameras. Look at the huge shantytown that is the Gaza Strip and from which Israel's army had to withdraw, despite its efficacy and its lack of inhibitions.

Drowned among the accomplice or submissive populations of the "shanty suburbs," terrorists, guerillas and drug lords go about their business – tribal wars, politico-military, fanatical or end-of-the-world-related activism; various different types of traffic – with impunity. For these illegal entities (drug lords, terrorists and guerillas, etc.) these peri-urban sanctuaries are ideal: misery, overcrowding, a multitude of unskilled young people, trapped in place, supplying all the necessary desperados, proximity to the economic heart of the system and the airports, proximity to the political and media center.

So, tomorrow “star wars?” No. Infinitely less high-tech, but more likely less glorious but bloodier, the “slum war.”

2) Beyond Bin Laden: The Dangerous Entities of World Chaos

Non-governmental, transnational, even global, new strategic threats have emerged from the chaos. Ferocious players, inaccessible territories: the terrorist nebulas, cartels, mafias, or militias are implacable enemies. In the chaotic zones of the southern hemisphere, few embassies, no meeting rooms, but anarchical “megopolises,” slums, the jungle against the backdrop of terrorism or war.

For, to use a more scientific vocabulary, the end of the bipolar order has caused the mutation of a host of entities that before were purely terrorist or purely criminal. Yesterday, most of non-state violence of a strategic level, or transnational terrorism, was generated by organized groups or groups used by the Special Forces on behalf of governments. Following orders and in exchange for payment, they operated mechanically by following stop/start pulses. Today, there is a nearly biological, uncontrollable and, to date, uncontrolled proliferation of complex dangerous entities, very difficult to identify, understand, define in territories or within flows themselves, that are as yet poorly explored.

Even at the doors to the western world, the new threats arise from militias, mutant guerrillas, hybrid entities peopled by terrorists, “patriot bandits” and military deserters commanded by illuminated “prophets,” dissident generals, war lords or just plain criminals that ignore all international laws, first and foremost those relating to the humanitarian aspect, and follow either the law of the jungle or “the law of God.”

Poorly known or elusive entities, nebulae or networks capable of alarming mutation and alliance changes, each one evolving in symbiosis with the mafia economies in the drug-dirty money-weapons triangle. The permanent and hierarchical entities have given place to small, temporary, mobile, fanaticized nodes, favoring “low-tech” resources whose motivations are less rational, even sometimes end-of the-world-based or apocalyptic.

Moral constraints seem to have deserted these nearly autistic entities that seek only to influence those within a tight circle of elected few. Making blind terror the end (the destruction of their “enemies”), they justify their means (terrorist attacks) (World Trade Center, Tokyo subway, etc.) by the will of a “prophet,” or the imminent end of the world.

Thus, the menacing entities of the new world disorder are many. Fanaticized terrorist nebulae, formerly politicized guerrillas now sold out to drug lords, mafias, and violent, irrational or end-of-the-world movements.

Radically New Hybrid Terrorisms

At the end of the sixties, the Irish Republican Army (IRA) took up the armed fight against the British. Nearly at the same time, extremist Palestinians began hi-jacking planes, while the Red Brigade and Red Army Fraction launched urban guerrilla warfare in what they called the “imperialist center” (Western Europe). That was more than 30 years ago. As it does now, terrorism made the headlines at that time. There is an enormous difference, however; in the past, major countries only faced minor problems of national security: airport surveillance, maintaining order in Ulster, and anti-terrorist police work. Although sensational, the terrorism of yesteryear was of little concern to the leaders of national defense.

Thirty years later, terrorism has exploded, one could say. It is everywhere and has even become one of the major components of war, after having slowly but surely infected it in the last three decades. In the hinge period of 1989-2001, terrorism stopped being marginal or folkloric to become the central security concern of our governments. Having today become a war, it simultaneously concerns the Minister of Defense and the Ministry of the Interior.

Having, henceforth, invaded everything, bombs explode daily for a thousand different reasons across the globe; terrorism has also undergone a profound change. The state terrorism of the Cold War, which was political or ideological, has virtually disappeared as such. Under a misleadingly unchanged appearance, what remains is part of a new logic.

Very diverse, these new terrorist players, nevertheless, share some characteristics:

- "De-territorialization," or establishment in inaccessible areas;
- Most often, the absence of any state sponsorship, which makes them even more unpredictable and uncontrollable;
- Hybrid nature, part "political," part criminal;
- Increasingly supported by individuals from the middle or cultivated classes of populations one had heretofore supposed integrated;
- Capable of mutating ultra-rapidly according to the dollar factor, henceforth, crucial;
- Pragmatic approach, attempting to prove the [terrorist] movement as they go – according to the Maoist practice that consisted in launching guerrilla warfare to learn war (for example the homemade bombs of the Algerian terrorists in France, July-Nov. 1995); and
- Enormous murderous capabilities, compared to the terrorism of the Cold War, which was more often symbolic. Thus, only the blockage of an aerosol prevented the Aum sect from causing 40,000 deaths in the Tokyo subway in April 1995; the attacks of September 11, 2001 in the United States killed 15 times more people than the bloodiest terrorist attack of the 20th century…

"Degenerate Guerillas"

In Europe, the most famous of these hybrid entities that associate the "political" and criminal, terrorism with drug trafficking, was for a long time the Kurdistan Workers Party. But the PKK is far from the only, henceforth, "narco-guerillas'' that exist in central Asia, Latin America and Africa. They can be found in Afghanistan, Burma, Columbia, India, Lebanon, Pakistan, Peru, the Philippines, Senegal, Somalia, and in Sri-Lanka. Via the great "diasporas," they are all present in most of the major metropolises of the developed world.

An essential difference with the state terrorism of the bipolar era, notably that of the Middle-East: this exchange of criminal goods and services occurs between caricatures of increasingly weak states and guerillas enriched by drug money, thus, even more self-sufficient than before. Yesterday, one state of the Near East controlled every millimeter of the terrorist trajectory of the extremist Lebano-Palestinian groups.

Today, idiotic powers count on narco-guerillas that are masters of their future to frighten the outside world, thus, enabling them to last a little longer...

The Superpowers of Crime

In April 1994, the Secretary General of Interpol, Raymond Kendall, declared, *"Drug trafficking is in the hands of organized crime... Interpol manages a file of 250,000 major criminals. 200,000 of them are linked to drugs."* As a result, the groups that control most of the production and trading in narcotics are few and well known. Columbian cartels for cocaine; Triads (Hong Kong, Taiwan and People's Republic of China) for the heroin of the golden triangle; and Italian, Turkish-Kurdish and Albanian mafias for that of the golden crescent: these transnational criminal organizations (TCO) are vital to world drug trafficking since they connect the cultivation sector controlled by the guerillas and the actors of tribal war to the end distribution handled by the urban gangs of the developed world's metropolises.

Not hesitating to kill or corrupt, each year the TCOs handle 34 to 57 billion euros and recycle perhaps half of it in the world economy. Today they merge illegal dealing in narcotics, weapons and clandestine migrants. Associating and strengthening their profit centers, tomorrow the TCOs will be even more powerful.

Violent Irrational Entities

In the spring of 1997 in Japan, the trial of Shokoa Asahara allowed the world to realize the widespread and complex extent of the Aum Shinrikyo organization, a sect capable of:

- Extorting millions of dollars, first from its "faithful";
- Recruiting hundreds of brilliant students, most studying the advanced sciences;
- Setting up a world procurement network (dangerous substances, weapons, explosives, etc.) managed by competent businessmen;
- Creating, notably in Russia, large "branches"; and
- Assassinating, over several years, "traitors" to the sect with total impunity.

"Eco-terrorist" Groups

At the end of April 1996, an explosive attack caused significant damage to the Lunebourg-Dannenberg (northwest Germany) rail line. Two days later, the German railway network was sabotaged (cables powering the line signaling system cut) at two locations, near Hanover and Göttingen. These attacks by the "Kollektiv Gorleben" group revealed to European public opinion the existence of a group of environmentalists who had taken action to "save the planet."

In North America, the arrest of Ted Kaczynski, author of twenty letter bomb attacks in fifteen years, three of which were fatal, shortly thereafter revealed the ties of the person the FBI called the "Unabomber" with the eco-terrorist movement. The names of his two victims (December 1994, April 1995) were on a list of enemies of nature and virgin forests published in a clandestine eco-terrorist bulletin entitled "Live wild or die!" – complacently reproduced in the February/March 1994 issue of the environmentalist-apocalyptic review "Earth First!" In 1994, Kaczynski himself participated in an "Earth First!" conference held at the University of Montana.

In the United States and Canada, other nature fanatics have already tried to poison water reservoirs and building ventilation systems. Militants of analogous, impenetrable micro-sects, willing to do anything to "open the eyes" of world public opinion, were caught around nuclear power plants, drilling platforms or fuel storage depots.

3) The Methods of Terrorist War

The new criminals have better assimilated the zeitgeist (spirit of the times) than most of the globe's state institutions. For today, the characteristics that make a multinational or a mafia organization high performing and prosperous are analogous: fluidity, even volatility, opposite the viscosity, heaviness of state institutions; "be light, anonymous and precarious" advised ironically the pamphleteer Gilles Châtelet.[2]

In the multinationals and new-look mafias, the network organization takes precedence over the pyramidal organization (that of the "loser mafias," the companies of yesteryear, and even the current nation-state). In both cases, the network is composed of interconnected, autonomous units, each one evolving on their own territory and connected to the others by a rapid information transmission system. The basic unit is an ultrasensitive detector that detects any newcomer from the outside world that is either profitable or dangerous for the network and transmits it to the node.

New Menacing and High-tech Entities

First, a simple reminder: spending money for the dangerous entities of world chaos is rarely a problem.

In 1995, the Columbian Police seized an IBM AS/400 computer in Cali whose memory contained all the telephone numbers and license plate numbers of the city, coupled with an ICR 900 scanner. Together, they formed a powerful communication interception and storage instrument that allowed the Cali Cartel to simultaneously tap into 180 radiotelephone lines. That same year, we learned that the Mexican Cartels had purchased "Rutan Defiant" kit airplanes. Made of composite materials, equipped with plastic propellers and covered with a coat of radar wave absorbing paint, they are "stealth planes" which, although rudimentary, are much less expensive than the famous American "stealth bombers."

In 1997, still on the cartel front, arrests and searches revealed the extent of the counter-attack of drug traffickers to the "militarization" of the fight against drugs. The Columbian Cartels finance with millions of dollars and employ, for their use, the training schools of the self-defense militia designed to fight the guerillas. It is in these training centers that they train their own praetorian guards, the "police" of the areas in which the drug producing laboratories and "anti-repression commandos," groups of killers targeting the police, magistrates, and the military involved in the war against drugs, are established. The Mexican Cartels spend fortunes to buy the best possible technology to spy on the American police and protect themselves: coded communication systems, equipment intercepting the communications of their enemies, and highly perfected bugging systems. In the field of "human resources," these cartels hire top-flight telecommunications, egronomic, and chemical engineers (to elude drug detection devices). Former officers of the special forces and intelligence services are paid their weight in gold.

One should not forget that now advanced information and communication technologies, the Internet plus "unbreakable codes," provide anyone, especially from an inviolable sanctuary, the free and global equivalent of one of these "Command and Control Centers" that up until the Gulf War were the prerogative of high-tech armies in the field.

New Menacing Entities and the Practice of Massacre

Imitation and contagion: such is the origin of the wave of massacres that have bloodied the world since 1997, from Columbia to Cambodia, from Cashmere to Mexico, and from India to Egypt, including Sierra

[2] "Living and Thinking like Swine", Exils, publisher, Paris, France - 1998.

Leone, Liberia – and now the United States. Let us not count the hidden murders, the shameful liquidations, secret vendettas, as old as the hills: this concerns the targeted, planned, media-covered massacre; from massacre that provides access to CNN and a deliberate element of the strategy of terror, to massacre that has evidently become one of the favorite weapons of the terrorists of world chaos.

"Inventor" of this type of massacre - the Algerian GIA. So much so that in December 1997, Amnesty International, whose choice of words is careful, speaks of this country in terms of "terrifying violence" and that the December 22, 1997 issue of "Libération" emphasizes that the Algerian press agency had that year used the word massacre more than 180 times in the headlines of its dispatches.

Why this contagion of massacre? Because it works. In one year, the GIA garnered a worldwide reputation: after Luxor, the Egyptian fanatical Muslims "existed" again; in Columbia, the United States now hesitates to help an army that is an accomplice to paramilitary-massacres:

- Usefully serve a "military'' strategy (GIA);
- Can nearly ruin a country (Egypt and its tourist industry after Luxor); and
- Can paralyze a giant, the United States, in a fight that for it is vital (war on drugs).

In short, committing massacres is existing, is making the headlines. A situation quickly understood by the guerrillas of the "United Revolutionary Front" of Sierra Leone[3], who add their own personal touch: the systematic mutilation of their victims, dismembered, their eyes ripped out, disfigured, but left alive to bear witness to a horrible "propaganda by action."

Result – Swarms and Networks: War in the 21st Century [4]

Here is the major challenge for the security forces of the nation-states of developed countries. The American superpower has been waging such a war against drugs for 20 years and today, it has indeed lost it: there is more heroin and cocaine in North America than 20 years ago, sold in purer form and for less than before.

What are the rules of the new-look war, that of swarms operating in networks (the concept of network being opposed here to that of a hierarchical entity such as an army)? Columbian Cartel, Algerian, Cashmere or Chechen guerillas, African or Balkan militia, al-Qaeda type terrorist entity, narco-army of Somalia or the golden triangle, Jamaican posse: all these actors of world chaos are non-state and transnational and basically operate in the same way.

Note first, and this is important in a world where information, communication is essential, that even though it is non-political and purely criminal, the "swarm" entity most often has its "legend." It cultivates its status of association of "men of honor" (mafia), its reputation of Robin Hood or defender of faith. The swarm communicates. It is neither autistic nor cut off from the world.

The basic element of the "building block game" is a combat group of ten to twenty men that all know each other. They come from the same neighborhood, the same clan, and the same tribe or went to the same

[3] Criminal band active since 1991 in the north (diamond zone) of the country.

[4] On the swarm war, see notably the RAND studies: "*The Advent of Netwar*''(1996) ; "*In Athena's Camp*''(1997) ; "*Swarming and the Future of Conflict*'' (2000) ; "Networks and netwars: the future of terror, crime and militancy''(2001). See also the special issue (in 1999) of *Studies in Conflict and Terrorism* on the theme "Netwar across the spectrum of conflict". These studies mostly result from the research of John Arquilla and David Ronfeldt.

place of worship. In short: they are immersed in the same civil society, the same culture, within which they are essentially invisible. Mobile, flexible, versatile, capable of diversified actions, the unit (which can be broken down into teams of four to five men[5]) moves easily, even across borders, and disperses as quickly.

The armament of the swarm is rustic, well controlled, and easily replaced; its hierarchy simple. This "Lego block" of guerilla warfare, drug traffic or terrorism (or frequently all three combined) can easily connect laterally to other analogous "Lego blocks," first thanks to the ancestral formula of conspiracy and secrecy, then due to either high-tech communication tools, cell phones, the Internet, faxes, use of MP3, coded images etc., or low-tech or even no-tech means (drums, optical signals, animal cries, etc.). The whole can cover its tracks and hide its intentions. It is also dispersed geographically and diverse in form and aspect. It is anything but an army, uniform by nature.

On an international scale, the swarm plays on the dialectic of the fief and the "diaspora." The immigrant in Europe, for example, is trapped by blackmail concerning the life of his family that remained in the fiefdom and cooperates willingly or not. The swarm knows how to exploit, to its benefit and in many ways, the humanitarian aid provided in or near its fiefdom.

Crucial point: this polymorphous nebula has no strict central hierarchy[6] and/or obedience to dominating chiefs of staff. It can even simply be "brainless." This nebula can be a community of faith (Islamists, sects) or of interest (drugs) with a chief or team that is recognized as having implicit authority to whom one swears allegiance for the present but which can be taken back the next day, and which coordinates the whole. An example of this point is the back and forth of the Algerian kataëb between Antar Zouabri's GIA and the Salafist Group for the Dawa and Jihad of Hassan Hattab. On the whole, however, one can agree on what is essential: hate of a common enemy, the jihad and the desire for dollars.

The structure (let us imagine a spider web) is flat, decentralized. Each "Lego block" of the swarm is highly independent with a local capacity for initiative. For coordination the nebula relies on no irreplaceable charismatic chief, but anonymous and interchangeable leaders. The swarm operates in pulses. A decision for massive attack is made? The available units quickly reach a given sector, attack suddenly and brutally, and disperse before the adversary with its heavy complex hierarchy has even reacted.

In the Caucasus during the first Chechen war, the swarm configuration resulted in the taking of thousands of hostages; several escapades of "infernal Chechen columns" in southern Russia; the hijacking of a Russian ferry in the Black Sea (January 1996) and a Turkish Cypriot Boeing 727 in March 1996; dozens of attacks against Russian officials and military; and even the threat of nuclear terrorism in Moscow.

Finally arises the problem of the development of a form of low intensity, light terrorism, evolving between the policy of silence against witnesses, pressure on the police, magistrates but also all organized authority (doctors, mailmen, etc.) that is slowly developing in the "freed" territories. The suburban gangs become hybrid gangs that sometimes seek a "political" screen, as was the case for the anti-Semitic attacks conducted by suburban delinquents suddenly interested in the Palestinian conflict.

The last development in Iraq, Afghanistan or Lebanon, the return of the Shiis inside modern terrorism (the Nasrallah warning after the assassination of Imad Mughniyeh in Syria, explaining that "the rules have changed") expressed new threats for the Occident.

[5] Like for example the Chechen "tank killer" units.

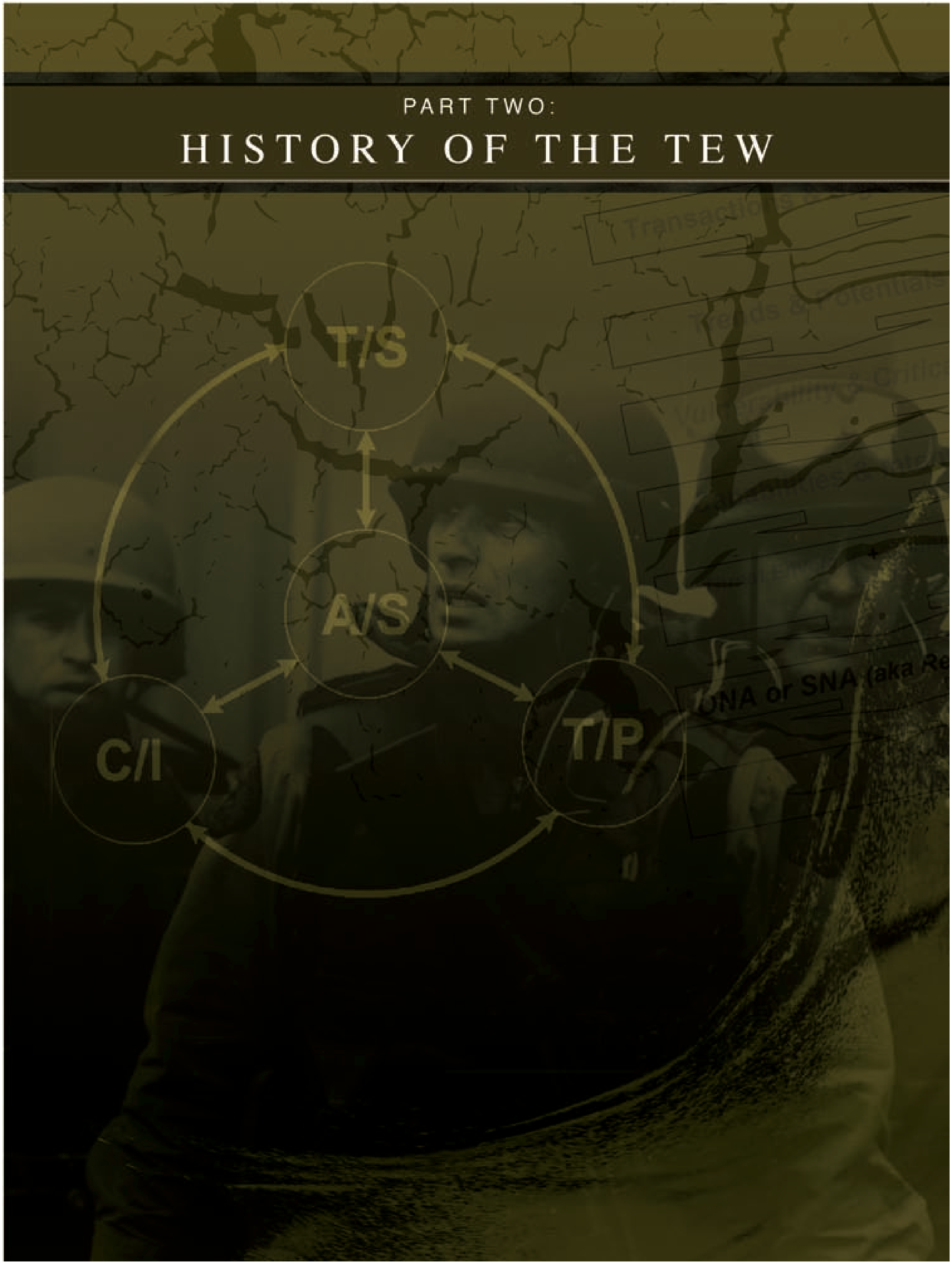
[6] Each unit having only an embryonic hierarchy.

In the New York Police Department's report on "Radicalization in the West," published at the end of 2007, it was possible to highlight the transfer from imported to homegrown terrorism.[7]

Those are the threats the Los Angeles County Sheriff's Department and other law enforcement agencies must deal with to protect freedom and citizens against attacks.

[7] Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," NYPD Intelligence Division, found at: http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf, no date.

PART TWO:
HISTORY OF THE TEW



I. The LA TEW and its Evolution

John P. Sullivan

The Los Angeles Terrorism Early Warning Group (TEW) held its first formal meeting in October 1996—a full five years before radical jihadist terrorism lashed out against the United States. In light of the interagency intelligence failures that led to 9/11, the TEW's founding seems prescient. At that time the problem of transnational "Fourth Generation" insurgents and criminals waging "netwar" was only the concern of a few maverick security analysts. Even the military was largely pre-occupied with building a "Network-Centric" force to deploy against competitor states such as China and Russia. The rise of dangerous non-state forces went largely unnoticed—until the world woke up one September morning to two burning towers.

Fortunately, the Los Angeles TEW were lucky enough to capitalize on the talents of an international community of military and law enforcement personnel, intelligence and policy analysts, and leaders from the business and medical worlds interested in networking to stop terrorism. This eclectic group formed a group brain, sort of a "Wikipedia" of counter-terrorism.

These security professionals don't just contribute intelligence—they also give insightful (and novel) presentations on emerging threats, technologies and strategies, increasing the collective knowledge of America's national security establishment. The TEW's records read like a "Who's Who?" of the international security community (from Canada, France, the United Kingdom, Israel, Germany, Spain and the U.S.). UCLA political scientists Amy Zegart and David C. Rapoport, famed RAND terrorism analysts David Ronfeldt and Brian Jenkins, *New York Post* military affairs columnist Ralph Peters, and a host of lesser-known but equally important analysts have all briefed the TEW.

Although many first became aware of the TEW after 9/11, it has dealt with many other security issues, including counter-narcotics missions, beefing up public infrastructure security, border security, the vulnerability of health and food supplies to terrorists, shoulder-fired missiles, and the tackling of present and future biological warfare threats.

The TEW grew from an *ad hoc* monthly meeting of concerned Los Angeles security analysts and emergency responders seeking to share information and build knowledge into an incident-specific intelligence fusion cell (really more of an operations-intelligence fusion effort). In its early years (from 1996 to 2001), the TEW focused on building tradecraft and processes. These started with target/response information folders and playbooks to aid response and threat assessment, as well as a monthly open source report (OSINTrep). These matured into what is now known as "Intelligence Preparation for Operations (IPO)" and the Transaction Analysis Model and Transaction Analysis Cycle. During this time frame, the TEW was called to develop response protocols for Anthrax hoaxes in 1998, as well as stand-up as an intelligence watch center for the Y2K/New Years 2000. The TEW also stood up as a special event intelligence fusion center for the 2002 Democratic National Convention.

On September 11, 2001, the Los Angeles TEW stood up to assess the impact of the 9/11 attacks on New York and Washington, DC. It stayed active as a full-time multiagency, multidisciplinary fusion center for Los Angeles County (all 88 cities in the County) until the intelligence fusion mission was transferred to a new Joint Regional Intelligence Center (JRIC) where TEW analysts were embedded to jump-start the new organization.

During that time period, the TEW also operated the National TEW Resource Center (N-TEW-RC) to help develop TEWs and fusion centers across the United States. The Model CONOP in part three of this text was developed at that time.

In recent years, the TEW has morphed from an intelligence fusion center to a strategic foresight workshop—its analytical capabilities have been absorbed into the Joint Regional Intelligence Center (JRIC). TEW members and analysts now speculate on future threats and run wargames designed to gauge Los Angeles' vulnerability to terrorism.

The TEW has provided intelligence that defused two cycles of anthrax hoaxes in 1999 and 2001. Additionally, TEW contributed vital intelligence during the Democratic National Convention in 2000, helping to prevent a repeat of the 1999 World Trade Organization (WTO) riots. The intelligence was used to successfully identify possible threats and shape the operational space to ensure a successful and mostly peaceful convention. The TEW also helped contribute intelligence during the run-up to Y2K, examining the threat of cyber-terrorism, systems failure, and violence by millennialist cults. Although thankfully none of those threats came to pass, the TEW's historical response demonstrates the utility of early warning intelligence.

During its active fusion experience, several TEWs have been established throughout the United States, replicating the success of the Los Angeles TEW's networked approach. Many of these still function as full-time regional fusion centers, others serve as informal meeting venues to forge professional networks in a particular region, and across regional boundaries. The Los Angeles TEW still exists as an informal future operations shop, continuing its monthly meetings, sponsoring exercises, conferences, and workshops, as well as helping develop analytical tradecraft, and continuing to nurture interdisciplinary awareness of emerging threats.

The Los Angeles TEW has been cited in many media reports, government and academic studies as a viable model for counterterrorism intelligence fusion. It has also been recognized for its innovative efforts. Two important honors bestowed on the TEW include being named among the "Top 100" innovative programs by Harvard University's John F. Kennedy School of Government: 16th Annual Innovations in American Government Awards (2003), and as a Finalist (top 5) in Mitretek Innovations in Homeland Security Award issued by Mitretek and the Ash Institute for Governance and Innovation at the Kennedy School (2004).

Throughout its history, the Los Angeles TEW has been dedicated to developing network approaches to network threats. It also sought to anticipate novel and emerging threats—i.e., develop early warning. As a result, the TEW developed an overarching mission statement for the Los Angeles TEW and the broader TEW network:

> *To develop operational intelligence for [our] area of operations, and contribute to the co-production of intelligence across the TEW and intelligence fusion community in order to prevent, counter and respond to terrorism and emerging threats by conducting indications and warning and operational net assessment.*

This mission statement is still valuable and relevant. It guides the continuing work of all those in the TEW community. It also contains a goal—the recognition of the "co-production" of intelligence as an essential element of understanding, anticipating, and countering global terrorist networks and the threats they pose. This text shows how these concepts emerged and matured.

II. Selected Essays on TEW Process and Evolution

The following essays provide a snapshot of the TEW's development and conceptual foundations. They illustrate the theory and practice of the TEW. These pieces outline the TEW's organization, the TEW intelligence co-production process, and the TEW's "transaction analysis cycle." Together, these essays demonstrate that the TEW is not just another form of intelligence "fusion" or "intelligence-led policing" but rather a mature approach to intelligence analysis and operations.

The essays selected for inclusion in this work are "Terrorism Early Warning and Co-production of Counterterrorism Intelligence," which was presented to a panel on Innovation in Analysis, Warning and Prediction at the Canadian Association for Security and Intelligence Studies in Montreal in October 2005; an expanded version of that paper "Intelligence Co-production and Transaction Analysis for Counterterrorism and Counter-netwar;" and "Developing a Group Strategic Threat and Modus Operandi Profile Analytical Framework," both presented to the International Studies Association Conference in San Diego in March 2006.

While some of the content overlaps, these papers help demonstrate the TEW's evolutionary path. In this work, the figures from all three papers are consolidated to reduce redundancy and for clarity of presentation. Additional references and papers on the TEW are included in the Appendices for those wishing greater detail than presented here.

Unpublished paper presented to 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.

Reprinted at INTSUM Magazine, Marine Corps Intelligence Association, Vol. XVII, Issue 8, Spring 2006.

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 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. [8]

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

[8] 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 C4I", 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.

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 reach back, 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 operation. 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)

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.[9] 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, 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) and 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),

[9] 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.

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 is a capability for acquiring or collecting information: sensors. The sensors could include a citizen’s report of suspicious activity to community police, other human collection means, 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, and 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. [10]

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’ (*see Figure 3*) 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 hy-

[10] 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.

potheses 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 Los Angeles 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 centered (like the TEW organization and IPO framework) on Analysis/Synthesis.[11] 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, Washington; Tulsa, Oklahoma (Oklahoma Region 7); New Orleans, Louisiana (Louisiana Region I); Greater Cincinnati; Albuquerque, New Mexico (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 Los Angeles TEW.

While the Los Angeles TEW model has demonstrated that networked fusion is possible, a number of challenges remain. First among these is organizational and bureaucratic competition. Networked forms com-

[11] Analysis/Synthesis is the core of the ‘Orientation’ phase of Colonel 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.

pete 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 tradecraft, 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.'

Unpublished paper presented to International Studies Association, 2006 ISA Annual Conference, San Diego, California; Panel on Intelligence and Operational Issues for Counterterrorism and Counterinsurgency, 24 March 2006

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

John P. Sullivan

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

Networked threats dominate the horizon. This paper describes some of the emerging tools and approaches to intelligence analysis necessary to navigate this threat horizon.[12] Terrorist and insurgent networks dominate the global scene, challenging state institutions and global security. On the terrorist front, the 9/11 attacks in New York and Washington, DC, the M-11 (Eme Once) attacks against the Madrid Metro, and the 7/7 Attacks on the London Underground exemplify this reality. The Iraqi insurgency or insurgencies, as well as the renewed Afghan insurgency and attacks against Nigerian oil infrastructure, together with other facets of the global Salafist jihad, are further contemporary examples of netwar.[13] Within this phenomenon, also known as Fourth Generation warfare (4GW),[14] extremist organizations, exemplified by the self-proclaimed global jihadi movement described as al-Qaeda and its affiliates,[15] are complex non-state actors operating as transnational networks within a galaxy of like-minded networks. These entities are transnational, exploiting the seams of traditional approaches to security and intelligence.

Transnational extremists—netwarriors or Fourth Generation warriors—operate across borders and exploit the traditional boundaries between national security and criminal enforcement. These networked global

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

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

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

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

insurgents mix political and religious fanaticism with criminal enterprises to exploit the seams between crime and war. Traditional intelligence and homeland security approaches are insufficient to address these issues without major structural overhaul and an infusion of new approaches, tools, and processes.

Traditional Approaches are Not Enough

The catastrophic terrorist attacks on the US on 9/11 were a wake-up call to the citizenry, Congress and intelligence, national security, law enforcement, and public safety communities. These attacks and the subsequent anthrax attack sequence, like a modern-day Pearl Harbor, are widely viewed as intelligence failures of a large magnitude.[16] Yet as grand as this intelligence failure was, efforts to improve intelligence collection, stimulate information-sharing, and restructure bureaucracies are not enough. Largely governmental attempts at reform have included shifting bureaucracies and an emphasis on 'connecting the dots.' Yet without structural and systematic efforts to revitalize intelligence analysis, attempts to bound uncertainty and predict future terrorist activities are of limited utility. As Sundri Khalsa, drawing from prior work by Garst and Heymann, notes, "warning failures are rarely due to inadequate intelligence collection, [they] are more frequently due to weak analysis, and are often due to decision makers ignoring intelligence (Garst 2000). Decision makers, however, ignore intelligence largely because analytical product is weak (Heymann 2000)." [17]

Predictive intelligence is the desired end-state for all intelligence consumers, that is decision-makers at all levels from head of state through tactical operator, investigator, firefighter or cop on the beat. Yet traditional approaches, be they military order of battle analysis for traditional combat or linear lead analysis and case support found in criminal intelligence practice, can fill the need for predicting the swarming activities of small, dispersed, diffuse non-state netwar actors. There are many barriers to achieving the all too elusive actionable intelligence. There appear to be too few good sources of data on events yet to happen, apparently too many variables, in effect a large signal-to-noise ratio, and a lack of understanding of the potential tools and methodologies available to forecast and understand future events. [18]

Captain Sundri K. Khalsa, a United States Air Force intelligence analyst, posits three propositions for correcting this situation:

- "Analysis, rather than collection, is the most effective way to improve warning;"
- "Hiring smart people does not necessarily lead to good analysis;" and
- "A systematic process is the most effective way to facilitate good analysis."[19]

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

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

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

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

These propositions are shared and validated by the Los Angeles TEW's experience in forging new approaches to counterterrorism analysis. To paraphrase Russo and Schoemaker, analysts fail when they follow a poor process in arriving at their product.[20]

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

Co-Production of Intelligence and Terrorism Early Warning

The Los Angeles Terrorism Early Warning Group (LA TEW) was established in 1996.[21] It currently includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans-and post attack), specifically tailored to the user's operational role and requirements. The TEW integrates criminal and operational intelligence to support strategic, operational, and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team.

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

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

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

[21] Additional details on the Los Angeles Terrorism Early Warning Group, its approach, and the emerging TEW network can be found in John P. Sullivan, "Terrorism Early Warning Groups: Regional Intelligence to Combat Terrorism," in Russell Howard, James Forest, and Joanne Moore (Eds.), *Homeland Security and Terrorism: Readings and Interpretations*, New York: McGraw-Hill, 2006, pp. 235-245; John P. Sullivan, "Networked Force Structure and C4I," 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.

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), Transaction Analysis Model, and the Transaction Analysis Cycle; it conducts exercises, and is forming a networked framework for node-to-node collaboration.

Intelligence Preparation for Operations (IPO)

Intelligence Preparation for Operations (IPO) is the first set of processes used by the TEW to reduce uncertainty and produce an understanding of potential threats. IPO is a civil analog to the military intelligence preparation of the battlefield (IPB) process; it is intended to serve response information needs.[22] IPO provides a standard tool set for situational recognition, course-of-action development, and response rehearsal. This process bridges the gap between deliberate planning and crisis action planning for all facets of a unified multi-organizational response organization. Figure 1 depicts and summarizes the IPO framework.

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

Step 1: *Define the Opspace*

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

Step 2: *Describe Opspace Effects*

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

Step 3: *Evaluate OPFOR (PTEs) and Threats*

The third step is to identify and evaluate the opposing force (OPFOR) or potential threat elements (PTEs)

[22] 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.

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

Step 4: *Determine OPFOR and Friendly COAs*

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

The I & W Envelope

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

Foundations of IPO's Core and Four Steps

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

Utilizing IPO relies upon knowledge of analytical tradecraft and concepts for understanding intelligence and conflict. These include understanding of deception and counter-deception, of swarming and counter-swarming, the psychology of intelligence, and decision dynamics, including the need to limit group think and avoid mirror imaging. In addition, the IPO process must at all steps consider 'centers of gravity' and 'decisive points' and be able to address both current and future operations.[23]

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

[23] 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.

The Transaction Analysis Model

As noted earlier, traditional analytical techniques and approaches fall short when dealing with networked, non-state threats. Segall identifies three potential methodologies to fill this gap. These are 1) trends and patterns, 2) frequency, and 3) probability.[24] Segall notes that 'trends and patterns' of data are a traditional staple of intelligence that often are linked with the analysis of intent and capability (as specified for example in the national Security Act of 1947). Such techniques are particularly valuable in addressing armed conflict to determine OPFOR actions based upon knowledge of tactics, strategies and the disposition of forces (state and non-state) as analysts seek to discern indicators from newly emerging trends, patterns or irregularities. [25]

Frequency is often added to trends and patterns (since trends and patterns often miss catastrophic substate events). Frequency alone is not enough; it must incorporate trends and patterns to predict or forecast a terrorist event. Nevertheless, frequency is valuable in analyzing communications or other transactions to forecast terrorist activity, potential attacks, and craft interdiction and investigative activities.[26] Probability is the final traditional tool to be incorporated in Segall's trinity. For Segall, determination of the probability of a terrorist event is based upon "risk analysis of latent threat and target vulnerability."[27] Yet traditional threat-based or criminal intelligence approaches to terrorism intelligence typically ignore or segregate vulnerability and criticality (or the impact of a given attack) from their toolset. Segall quotes a private interview with an anonymous member of Her Majesty's Security Services (formerly known as MI5) to emphasize the value of integrating trends and potentials, capabilities and intentions with vulnerability and criticality:

> "The methodology of intelligence analysis of terrorism probability pertains to risk analysis of vulnerability when coupled to trends and patterns methodology determination of threat intent and capability and vulnerability assessment coupled with frequency methodology determination of the statistical analysis of prediction and forecasting of the likelihood of such threats through computerization techniques."[28]

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

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

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

[25] Ibid. pp.224-225.

[26] Ibid. p. 228.

[27] Ibid. pp. 229-230.

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

When aggregated, transactions and signatures may form specific trends and potentials (stage two) indicative of terrorist, insurgent or criminal activity. Absent specific indicators or information outlining a specific terrorist 'kill chain,' likely target locations can be identified through an assessment of vulnerability and criticality (stage three). These assessments form a hypothesis (or one of multiple competing hypotheses) about the OPFOR's capabilities and intentions (stage four) to be tested through collection and analysis. Together all of these stages define the threat envelope.[29]

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

Transaction Analysis Cycle

Terrorist activity plays itself out over time, which can be expressed in a linear fashion as an event horizon or in a non-linear fashion. The 'Transaction Analysis Cycle' developed by Sullivan is a non-linear analytical approach for discerning terrorist activity within dynamic and diffuse data sets laden with noise and masked by a fog of uncertainty. Analysts are charged with detecting and anticipating threat activity from massive amounts of societal activities or transactions. These transactions originate from a variety of sources and correspond to both legitimate and illegitimate activities. This mass of data is fraught with noise and clutter. Some of the transactions reported or observed are consistent with criminal or terrorist activity. That is, the transactions (or clusters of transactions or patterns of activity) may have signatures. Threat signatures are "structures of data that may reflect the execution of threat tasks."[30] Some patterns or threat signatures can be related, and the connections among related signatures can facilitate hypotheses about high-level organized activities[31] or indicate trends and potentials.

The Transaction Analysis Cycle emerged as a way to teach analysts how to interpret activity in order to assess leads and other inputs while developing iterative collection plans to identify patterns and define hypotheses about a potential terrorist 'kill chain.' A kill chain is a pattern of transactional, linked activity that describes a structure of data consistent with threat activity. Boner describes this as a threat pattern that is characterized by a "hierarchy of tasks and subtasks that may be involved in its execution. For example, carrying out a chemical attack may involve recruiting an attack team, acquiring a nerve agent, devising a delivery method, testing, etc. Each of these tasks may in turn involve a number of subtasks."[32] The kill chain is an analog of a decision tree and contains branches and sequels for each of its tasks and subtasks. Each of these contains transactions and signatures that can be anticipated, with the resulting patterns of data contributing hypotheses about OPFOR capabilities and intentions. Boner notes that the "data structures

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

[30] Christopher M. Boner, "Novel, Complementary Technologies for Detecting Threat Activities within Massive Amounts of Transactional Data," *Proceedings of the 2005 International Conference on Intelligence Analysis*, Mitre Corporation and Office of the Assistant Director of Central Intelligence for Analysis and Production, 2-4 May 2005, McLean, VA found at https://analysis.mitre.org//proceedings/Final Papers Files/318 camera Ready Paper.pdf.

[31] Ibid.

[32] Ibid.

that are used to represent activity patterns and hypotheses are closely related."[33] Because of this, transaction analysis can help identify pattern variables such as task participants, groups, assets, locations, and other instrumental role players and entities. [34] This makes transaction analysis a valuable method for directing collections and forming investigative and analytical hypotheses.

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

The Transaction Analysis Cycle is a framework for generating patterns from large transactional datasets. It is centered (like the TEW organization and IPO framework) on Analysis/Synthesis.[35] 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 are consistent with the operations of a specific cell or group. These transactions and signatures (T/S) can then be observed and matched with patterns of activity that can be expressed as trends and potentials (T/P), which can ultimately be assessed in terms of a specific actor's capabilities and intentions (C/I). At any point, the analytical team can posit a hypothesis on the pattern of activity and then develop a collection plan to seek specific transaction and signatures that confirm or disprove its hypothesis.

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

Conclusion

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

[33] Ibid.

[34] Ibid.

[35] Analysis/Synthesis is the core of the 'Orientation' phase of Colonel 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.

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

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

Unpublished paper presented to International Studies Association, 2006 ISA Annual Conference, San Diego, California; Panel on Intelligence and Operational Issues for Counterterrorism and Counterinsurgency, 24 March 2006.

Developing a Group Strategic Threat and Modus Operandi Profile Analytical Framework

Andre DeMarce and John P. Sullivan

This paper will outline the conceptual contours of developing a Group Strategic Threat and Modus Operandi Profile (GSTMOP) Analytical Framework as an element of John P. Sullivan's IPO and Transaction Analysis Cycle counterterrorism intelligence frameworks. It will examine the constellations of group variables such as group psychologies, group behaviors and structures, ideology, available weaponry and materiel toward extrapolating how they directly influence group strategic targeting approaches, targeting preferences, and attack modus operandi particular to individual groups. Finally, it will examine terrorist psychology and group behavior dynamics from a networked counterterrorism operational framework.

A key finding of the 9/11 Commission's examination of the terrorist attacks of September 11th was that the government suffered a 'failure of imagination' in not being more prepared to combat the threat of al-Qaeda attacks against the US homeland.[36] This assessment resonates with past discussions of surprise and warning. It also highlights the impact of a "poverty of expectations," the dangerous analytic and warning pitfall described by Thomas Schelling where "the danger is not that we shall read the signals and indicators with too little skill; the danger is in a poverty of expectations—a routine obsession with a few dangers that may be familiar rather than likely."[37]

Local or regional counterterrorism agencies are faced with combating inherently shadowy terrorist adversaries. These adversaries range from small cells to social networks of operatives who camouflage their activities amongst the backdrop of societies and the transnational fissures and shadows of an increasingly globalizing world. The majority of transactions and signatures that point to indicators of potential terrorist operations are likely to be subtle, fragmented, globally diffuse, and ambiguous.

Security and counterterrorism analysts—such as those serving within the various Terrorism Early Warning Group (TEW)[38] nodes—must guard against a "failure of imagination" and "poverty of expectations." To do so they must embrace an analytic approach and framework that precisely and advantageously assesses and charts potential and likely operational trajectories and characteristics of terrorist groups likely to operate in their particular region. This includes scenario-based assessment of strategic threat and group modus operandi. In turn, transactions and signatures (i.e., indicators) discerned by intelligence collection

[36] Executive Summary of the Final Report of the National Commission on Terrorist Attacks Upon the United States; available from http://www.9-11commission.gov/report/911Report_Exec.htm; Internet; accessed 1 March 2006.

[37] Thomas Schelling, quoted in Mary McCarthy, "The National Warning System: Striving for an Elusive Goal," *Defense Intelligence Journal,* 3, no. 1 (Spring 1994): 13.

[38] Background on Terrorism Early Warning Groups (TEWs) and the TEW concept can be found in John P. Sullivan, "Terrorism Early Warning Groups: Regional Intelligence to Combat Terrorism," in Russell Howard, James Forest, and Joanne Moore (Eds.), *Homeland Security and Terrorism: Readings and Interpretations* (New York: McGraw-Hill, 2006), pp. 235-245.

mechanisms and sensors can be sounded against these profiles to aid in the development of competing hypotheses of terrorist activity to support adaptive indications and warning frameworks.

As Sun-tzu proclaimed, "One who knows the enemy and knows himself will not be endangered in a hundred engagements. One who does not know the enemy but knows himself will sometimes be victorious, sometimes meet with defeat. One who knows neither the enemy nor himself will invariably be defeated in every engagement."[39] Thus, an analytic red teaming approach—seeking to understand and 'get inside' the mindset of the group—is useful in developing a group strategic threat and modus operandi profile (GSTMOP).

Understanding the mindset, capabilities and intentions of groups potentially operating in specific areas through the analysis of the particular group's ideological objectives, group dynamics, modus operandi, and capabilities can aid analysts in better assessing how the group is likely to operate in or threaten a particular region. The GSTMOP could provide an assessed 'threat consciousness' or landscape of potential group threats and modus operandi characteristics against which counterterrorism analysts—ideally utilizing the Transaction Analysis Cycle concept developed by John P. Sullivan—could compare intelligence indicators and signatures suggesting terrorist activity. The GSTMOP analytic framework are meant to serve as contextual, predictive, and operationally instrumental elements of Intelligence Preparation for Operations (IPO)[40] and Sullivan's Transaction Analysis Cycle[41] processes to more advantageously forecast and discern group operations, signatures and threats.

This paper will outline the broad contours of an approach for developing group strategic threat and modus operandi profiles, and identify key variables and factors to be examined and considered by counterterrorism analysts working as individuals or within a team. This paper will neither attempt to provide a comprehensive list of variables nor a complete analytic framework, but rather serve as a starting point for refining this framework within the homeland security or counterterrorism analytic context, using the TEW collaborative analytical group perspective as the primary reference point.

The scope of this paper did not allow for an exhaustive literature review. However, notable analysts who have examined terrorist group motivations, dynamics and threats as referenced in this paper include Kim Cragin and Sara A. Daly;[42] Bruce Hoffman;[43] Jerrold M. Post, Keven G. Ruby, and Eric D. Shaw;[44] and

[39] Sun-tzu, *The Art of War*, trans. Ralph D. Sawyer, (Boulder, CO: Westview Press, 1994), p. 135.

[40] 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.

[41] See John P. Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," paper presented to the Canadian Association for Security and Intelligence Studies, CASIS 20th Anniversary International Conference, Montreal, Quebec, Canada, 21 October 2005, available from http://www.terrorism.com/modules.php?op=modload&name=Documents&file+get&download=432; Internet; accessed 19 March 2006.

[42] Kim Cragin and Sara A. Daly, *The Dynamic Terrorist Threat: An Assessment of Group Motivations and Capabilities in a Changing World* (Santa Monica, Calif.: RAND Corporation, 2004).

[43] Bruce Hoffman, "The Mind of the Terrorist: Perspectives From Social Psychology," in Harvey W. Kushner, ed., *Essential Readings On Political Terrorism: Analyses of Problems and Prospects for the 21st Century* (Lincoln, NE: Gordian Knot Books, University of Nebraska Press, 2002).

[44] Jerrold M. Post, Keven G. Ruby, and Eric D. Shaw, "The Radical Group in Context: 1. An Integrated Framework for the Analysis of Group Risk for Terrorism," and "The Radical Group in Context: 2. An Integrated Framework for the Analysis of Group Risk for Terrorism," both in *Studies in Conflict & Terrorism*, 25 (2002): 73-126.

Brian M. Jenkins, Bonnie Cordes, Konrad Kellen, Gail Bass, Daniel Relles, William Sater, Mario Juncosa, William Fowler, and Geraldine Petty.[45] In particular, the paper references and complements the analytic frameworks for examining terrorist group capabilities, motivations, and threats developed by RAND analysts Kim Cragin and Sara A. Daly, and Bonnie Cordes et al.

As Cragin and Daly note in the conclusion of their study, "…this report examines the threats posed to U.S. interests worldwide, but it would also be useful to adjust the framework to focus on threats to the U.S. homeland specifically. Finally, it should be noted that we focus intentionally on the organizational and operational requirement that affect militant organizations' capabilities. For the purposes of this analysis, we have set aside a more thorough assessment of intentions and motivations. Yet such an assessment clearly affects any 'hearts and minds' campaign the U.S. government might undertake to reduce recruitment or lessen general popular support for terrorists' goals."[46]

Thus, this paper seeks to chart the general contours of an analytic framework for homeland security—that is for local or regional counterterrorism analysts—that examines the strategic threat and modus operandi for terrorist groups in his/her area of operations. The paper will also pose questions and factors of consideration—drawing on those posed in the Cordes et al. study and the Post et al. framework—that analysts might examine to better understand a group's strategic threat, internal dynamics, and likely modus operandi within a particular area of operations.

I. Analytic Red Teaming Approach to GSTMOP Development

In developing a GSTMOP, it is advantageous to take an analytic red teaming approach to attempt to get 'inside the mindset' of the terrorist group. In-depth and insightful red teaming promises to serve as a useful tool in crafting and refining counterterrorism strategies and operations. Such strategies and means might then better anticipate and combat terrorist adversaries. This improvement would be achieved through an enhanced understanding of the group's particular driving factors—strategic goals, leadership and decision-making dynamics and processes, operational capabilities and rationales, organizational dynamics and behaviors, adaptive capacities, etc.—and their corollary and derivative operations.

Group operations are guided by group ideology, leadership, and internal and external dynamics. As Bruce Hoffman contends, "…the terrorist act is conceived and executed in a manner that simultaneously reflects the terrorist capabilities and takes into account the 'target audience' at whom the action is directed. The tactics and targets of various terrorist movements, as well as the weapons they favor, are therefore ineluctably shaped by a group's ideology, its internal organizational dynamics, the personalities of its key members, and a variety of internal and external stimuli."[47] Overall, the key to such a red teaming approach is to identify and understand the prevailing and driving factors and dynamics animating the particular group and its operations.

A deeper understanding of each group's unique 'mindset' (ideology, strategic agenda, and leadership) and operational behaviors (operational capabilities, modus operandi, and targeting preferences) can enable a more precise and advantageous assessment of not simply what the group is capable of attacking, but what

[45] Bonnie Cordes, Brian Michael Jenkins, Konrad Kellen, Gail V. Bass-Golod, Daniel Relles, William F. Sater, Mario L. Juncosa, William Fowler, and Geraldine Petty, *A Conceptual Framework for Analyzing Terrorist Groups* (Santa Monica, Calif.: RAND Corporation, 1985).

[46] Cragin and Daly, pp.86-87.

[47] Hoffman, p. 63.

the group wants/intends to attack, as well as how the group is likely to conduct operations.
A deeper understanding of each group's unique 'mindset' (ideology, strategic agenda, leadership) and operational behaviors (operational capabilities, modus operandi, targeting preferences) can enable a more precise and advantageous assessment of not simply what the group is capable of attacking, but what the group wants/intends to attack, as well as how the group is likely to conduct operations.

As Cragin and Daly astutely note and examine in developing their analytic framework, the terrorist group is a dynamic actor, constantly evolving, adapting and reacting to environmental stimuli. Thus, it is envisioned that the GSTMOP would be constantly revised to incorporate current intelligence on the dynamic and inter-relational nature and evolutionary and adaptive capacities and trajectories of the group vis-à-vis the shifting environment conditions, dynamics, and actors affecting the group. Further, this approach seeks to identify and analyze the key group dynamics and characteristics underpinning and driving not only contemporary operations and threats, but also those likely to shape group operations, decisions, and adaptations in future circumstances and contexts.

While the Post, Ruby, Shaw framework referenced earlier was originally developed to recognize and analyze a non-violent radical group's risk of becoming violent, it represents an excellent foundation for examining the internal and external variables and dynamics—as well as the observable indicators—affecting the behavior of a radical group. [48] These variables, with certain modifications to examine an already violent radical group, are useful in the development of the GSTMOP analytic framework and in assessing those critical group behavioral and environmental variables, dynamics, and indicators for a terrorist group in a particular area of operations. This framework, along with the aforementioned studies by Cragin and Daly, and Cordes et al., provided the conceptual inspiration for the analytic contours and questions utilized in the following sections to begin developing the GSTMOP.

Each terrorist group is unique in typology, particular motivations, ideological objectives, structure, etc., and operates in an equally unique manner depending upon the actors, audiences, and dynamics at play within its environment. Therefore, advantageous counterterrorism intelligence collection and operations must be appropriately tailored to the particular circumstances of the group.[49] Once the contours of the GSTMOP begin to develop, the Transaction Analysis Cycle concept of counterterrorism indications and warning, and analysis can be sounded against that GSTMOP. As Sullivan describes, 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.'[50]

Sullivan goes on to describe the Transaction Analysis Cycle process and its relationship to an analysis of a group's capabilities and intentions—a GSTMOP-type profile—in assessing potential terrorist group presence, operations, and overall threat:

> 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,

[48] See Post et al..

[49] Jerrold M. Post, "Current Understanding of Terrorist Motivation and Psychology: Implications for a Differentiated Antiterrorist Policy," Conference Report, *Terrorism: An International Journal,* 13, no. 1 (1990).

[50] Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," p. 6.

> 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.[51]

Thus, the development of the GSTMOP framework relies upon an understanding of the group's modus operandi, particularly the elements and phases of attack operations. These will in turn help the analyst recognize possible indicators—captured as transactions and signatures—of ongoing operations and hypothesize the phase, target, and/or tactics of the operation. If the transactions and signatures resonate with operational arcs and characteristics of the group within the hypothesized GSTMOP and threat scenarios, the Transaction Analysis Cycle should trigger an adaptive reorientation of intelligence collection postures. This would result in an alerting and refocusing of intelligence assets and sensors to 'stalk'[52] the likely transactions and signatures or indicators of the current or potential next phases of the hypothesized terrorist operation identified. The new, 'stalking' intelligence would help discern and confirm, or disprove the hypotheses of current terrorist activities.

Many terrorist groups and/or threats involve transnational dimensions, issues, actors, and networks that operate largely outside and in the shadows of many of the strictures, power contours, and jurisdictions of the state-centric international arena. These transnational terrorist, militant, and criminal groups and networks exploit the various state-centric international sinews, fissures, and dynamics both connecting and cleaving nation-states. Consequently, the dichotomy between domestic and international security is increasingly blurred as terrorist groups operating in the U.S. will likely have significant transnational connections, inspiration, or threat vectors.

Homeland security analysts must be able to anticipate terrorist threats involving groups of transnational basing, reach, approach, inspiration, and/or command. Therefore, local or regional counterterrorism intelligence analysts must perceive, appreciate, and incorporate international and transnational issues related to terrorist groups that might threaten their locality and national space. These are critically germane to understanding terrorist group mindsets, strategies, motivations, and operations, and, thus, threat assessments. The truly transnational terrorist threat compels the full appreciation and incorporation of global political and international security developments and information—particularly those related to existing or potentially emergent 'homegrown' terrorist groups—as an integral element of counterterrorism analysis.

[51] Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," pp. 6-7.

[52] Stalking is used to denote the active pursuit of terrorist indicators. Rather than passively collecting intelligence, the Transaction Analysis Cycle demands an active search or hunt for transactions and signatures indicative of terrorist operational sequences. This does not totally replace passive collection efforts, but augments them toward the assembly of the data necessary to prove or disprove alternative competing hypotheses.

As Sullivan notes:

> The immediate precursor for an attack may be in the local area, across the nation, in a foreign nation, in cyberspace, 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 terrorist 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.[53]

At a tactical or defensive level, comparative assessment of a group's likely strategic and/or intended targets and group capabilities, measured against the landscape of potential area targets and vulnerabilities, will help to refine the threat assessment. This enables public safety and security agencies to more advantageously marshal valuable counterterrorism resources to those targets and threats assessed as most likely.

In this vein, Sullivan suggests that named areas of interest (NAIs) "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."[54]

Thus, in the development of the GSTMOP, the analyst must study, analyze and incorporate salient information on the particular group's characteristics and activities abroad. Further, in scanning for indicators and signatures of terrorist group activity in a domestic context, analysts must scan not only local activities, but must also appreciate, analyze and incorporate group activities in the global dimension. These efforts should also consider international developments potentially affecting the group, as potential indicators of group intentions, operations and behaviors.

II. Toward a GSTMOP Assessment: General Factors/Variables for Consideration

The following section outlines four broad conceptual categories of factors and variables driving group operations for consideration by the homeland security and counterterrorism analyst in developing the GSTMOP. It also suggests relevant questions that might guide the development of the GSTMOP and the surveying and analysis of indicators. It must be emphasized that terrorist groups or networks are social organizations operating in a fluid environment. As a result, the following factors are largely inter-dynamic and overlapping within the group and in relation to the actors and dynamics of its environment. As such, the delineation of factors in the following categories are meant to assist with conceptual clarity and research organization. Further, the factors outlined are by no means an exhaustive listing, but rather seek to provide some key questions in assessing the prevailing mindsets, decision-making, group dynamics, etc. driving group operations in the present, as well as adaptations and reactions to changes in their environment of operations in the future.

The overarching analytic approach integrating these lines of inquiry into the trends and potentials, and capabilities and intentions aspects of the Transaction Analysis Cycle center on the comparison of observed

[53] Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," pp. 2-3.

[54] Sullivan, "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," p. 4.

indicators and signatures to the hypothesized and assessed GSTMOP contours for each group, and the responsive intelligence collection 'stalking' plans. Therefore, guiding questions for each category include:

- What transactions have been observed to date, and are they consistent with a particular group modus operandi signature—either of a group, a phase of operations, or a component part of an operation's kill chain?
- What hypotheses of group operations and corollary intelligence collection objectives do these transactions drive?
- How can we prove or disprove multiple alternative competing hypotheses in light of these transactions and signatures?
- Are they actual indicators? If so, of what?

Ideological-Strategic Mindset

A more in-depth understanding of the group's ideological-strategic mindset—its causes, motivations, and goals—will help orient the analyst to the broad categories of potential actors and audiences that might represent the targets of the group's instrumental and coercive violence as it endeavors to achieve its stated goals. Similarly, this understanding will help to discern those actors and audiences likely of greatest concern and impact to the group in pursuing its goals. The assessed purchase and resonance of the group's ideology and goals vis-à-vis the populace in the particular area of operation will give an indication as to the likely degree of sympathy or operational support the group might enjoy, as well as the size and nature of potential recruitment pools.

Further, this category of analysis will give insight into the group mindset and rationale strategically guiding operations, as well as the likely degree of violence and types of operations—including operational preferences and constraints—the group will employ as derived from its ideological creed and agenda.

On this point Hoffman notes:

> …all terrorist groups seek targets that are lucrative from their point of view. As such, they employ tactics that are consonant with their overriding political aims. Whereas left-wing terrorist such as Germany's Red Army Faction (RAF) and Italy's Red Brigades (RB) have selectively kidnapped and assassinated persons whom they blamed for economic exploitation or political repression to attract publicity and promote a Marxist-Leninist revolution, terrorists motivated by a religious imperative have engaged in more indiscriminate acts of violence, waged against a far wider category of targets: encompassing not merely their declared enemies, but anyone who does not share their religious faith. Ethno-nationalists arguably fall somewhere in between. On the one hand, the violent campaigns waged by groups such as the Palestine Liberation Organization (PLO), the Irish Republican Army, (IRA), and the Basque separatist group, ETA (Freedom for the Basque Homeland), have frequently been more destructive and have cause far greater casualties than those of their left-wing counterparts. But, on the other hand, their violence has largely been restricted to a specifically defined 'target set' (i.e., the members of a specific rival or dominant ethno-nationalist group). Perhaps the least consequential of all these terrorist group categories (in terms of both frequency of incidents and impact on public and governmental attitudes) has

> been the disparate collection of recycled Nazis, racist 'political punk rockers,' and other extreme right-wing elements who have emerged through the years in various Western countries. But even their sporadic and uncoordinated, seemingly mindless violence is neither completely random nor unthinkingly indiscriminate. Indeed, for all these categories, the point is less their innate difference than the fact that their tactical and targeting choices correspond to, and are determined by, their respective ideologies, attendant mechanisms of legitimization and justification and, perhaps most critically, their relationship with the intended audience of their violent acts."[55]

As Hoffman describes, the group's typology, ideology, and objectives broadly guide operational decisions in terms of targeting and the degree of violence employed. In addition, understanding the group's goals and objectives will provide insight into what actions by the key actors—including defensive and offensive counterterrorism strategies—might ameliorate or erode the particular environmental conditions, grievances, or interests serving as motivations for the group's violence. On this point, Post has argued that counterterrorism strategies must be equally differentiated and tailored to the particular group typology.[56]

Factors for Consideration/Questions:

- What is the group typology? Ethno-nationalist? Nationalist-separatist? Religious extremist? Jihadi? Xenophobic/racist?
- What is the group ideological narrative/manifesto?
- What are the group strategic goals? Political? Religious? Societal?
- What goals has the group emphasized? Which has the group debated internally? Which has it emphasized via communiqués and actions?
- What are the 'root causes' and core motivations of group militancy? What are the particular grievances of the group?
- How sweeping are the goals? Is the group pursuing revolutionary change or the pursuit of specific goals, and/or redress of specific grievances?
- What strategic/generic target categories has the group articulated, emphasized?

Key Environmental Actors, Dynamics, and Stimuli

This category and area of research and analysis is arguably the most important in developing the GSTMOP in that it seeks to reveal and understand how and why the group has, and/or might, instrumentally engaged and responded to the particular actors, audiences, and dynamics within its environment.

In this regard, it is important that the analyst have a sound understanding of the social-psychological dynamics of instrumental political violence and terrorism, and how the violence might be employed to pur-

[55] Hoffman, pp. 63-64.

[56] See Post, "Current Understanding of Terrorist Motivation and Psychology: Implications for a Differentiated Antiterrorist Policy."

sue the group goals. Instructive in this understanding is the illuminating description of terrorism and its dynamics and coercive effects offered by Alex P. Schmid:

> Terrorism is a method of combat in which random or symbolic victims serve as instrumental targets of violence. These instrumental victims share group or class characteristics which form the basis for their selection for victimization. Through previous use of violence or the credible threat of violence other members of that group or class are put in a state of chronic fear (terror). This group or class, whose members' sense of security is purposively undermined, is the target of terror. The victimization of the target of violence is considered extranormal by most observers from the witnessing audience on the basis of its atrocity; the time (e.g. peacetime) or place (not a battlefield) of victimization or the disregard for rules of combat accepted in conventional warfare. The norm violation creates an attentive audience beyond the main object of manipulation. The purpose of this indirect method of combat is either to immobilize the target of terror in order to produce disorientation and/or compliance, or to mobilize secondary targets of demands (e.g. a government) or targets of attention (e.g. public opinion) to changes of attitude or behavior favoring the short or long-term interests of the users of this method of combat. [57]

An examination of how the group has employed coercive activities in an instrumental capacity—not limited to only violence, but also including political and social engagement—aids in the understanding of both the group's operational trends and modus operandi, and, importantly, the apparent underlying driving rationale for these instrumental activities. This avenue of research should assist the analyst in developing a better assessment of how, and against which actors and targets, the group will apply instrumental violence in the future.

Factors for Consideration/Questions:

- What is the environmental—societal, political, economic, technological, historical—context?
- What are the prevailing environmental dynamics and/or sentiments?
- Who are the instrumental actors and audiences (see Schmid)—for example, the target of demands or coercion, the perceived constituency, adversaries—that the group must appreciate, engage, coerce, eliminate, etc. in order to achieve its goals? Which are the most important?
- What are the group relationships and dynamics vis-à-vis these actors and audiences?
- What instrumental actions has the group taken to engage—through coercive violence, and/or political and social initiatives—these actors and audiences?
- How has the group been affected by or responded to the actions of the actors and audiences, and any changes in its environment (political, societal, etc.)?
- What leader, decision-making process or rationale seems to have guided the instrumental activities?

[57] Alex P. Shmid, *Political Terrorism: A Research Guide* (New Brunswick, NJ: Transaction Books, 1984), p.111.

Internal Group Dynamics

This conceptual category and line of research seeks to develop a better understanding of group structure and internal group dynamics and their affect upon operational decision-making and group cohesion. Of particular interest are factors affecting the group leadership, command and control, and operational planning and preparation in an effort to discern the prevailing operational leadership elements and rationales.

Factors for Consideration/Questions:

- What is the structure of the group—cellular, hierarchical, 'homegrown,' and/or networked? Is it some combination of these structures?
- What is the structure/nature of the group leadership—charismatic leader, committee leadership, quasi-military hierarchy, or 'leaderless' movement?
- How much control does the leadership exercise over group operations, planning, and strategies?
- Is the group operationally entrepreneurial and adaptive, or does it act only when ordered by leadership?
- How cohesive is the group? Are there rogue or dissenting members or elements, and/or the potential for splinter groups/cells?
- How committed, subservient, and 'professional' are the members vis-à-vis leadership orders, and operations?
- Have unique cultural factors, norms, and/or behaviors significantly affected internal behavior?

Group Operational Capabilities

This category and line of investigation is aimed at developing an assessment and understanding of the group's operational capabilities, sophistication, and preferred modus operandi based both on the group's demonstrated attacks and operational capacity, and also on an assessment of the group's potential capabilities. It is an avenue of research that seeks to discern what operations the group is capable of, or constrained from mounting in relation to the group's strategic agenda and environment of impacting actors and audiences.

Factors for Consideration/Questions:

- What have been the group's preferred target categories, tactics, weapons?
- What are the group's apparent operational capabilities in terms of:
  - o Number of fighters and support operatives;
  - o Militant training and expertise;
  - o Weapons caches and weapon engineering capacity; and
  - o External actor or societal operational support or aid?
- What level of operational sophistication and complexity have the attacks demonstrated?
- Have any group operations failed or been interdicted? If so, how and why?

[58] See Cragin and Daly.

III. Conclusion

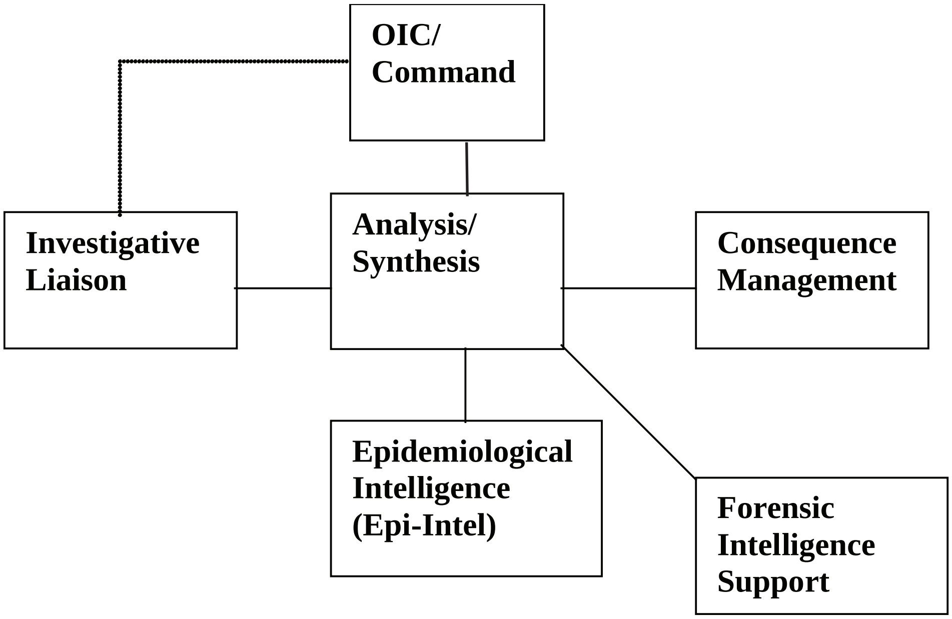
As a GSTMOP begins to take shape via the above analysis, it is then up to the analyst or analytical unit to discern the unique cocktail of prevailing, driving factors—and their relative weight and interplay—around which the group operates in given environments, particular situations, and in response to various environmental changes. It is at this stage that the analyst or analytical unit begins to develop a better understanding of the group mindset and capabilities, and can begin to chart potential threat landscapes, modus operandi characteristics, and operational scenarios for the group.

As noted earlier, the GSTMOP is meant to serve as a complementary tool and element within IPO and the Transaction Analysis Cycle frameworks and processes. The next steps required to more fully develop, refine, and apply the GSTMOP framework center on the outlining of a more comprehensive and inter-dynamic listing of the critical factors and variables of group intentions and capabilities, and a more formalized integration of this concept into the IPO and Transaction Analysis Cycle concepts.

FIGURES FOR SECTION II

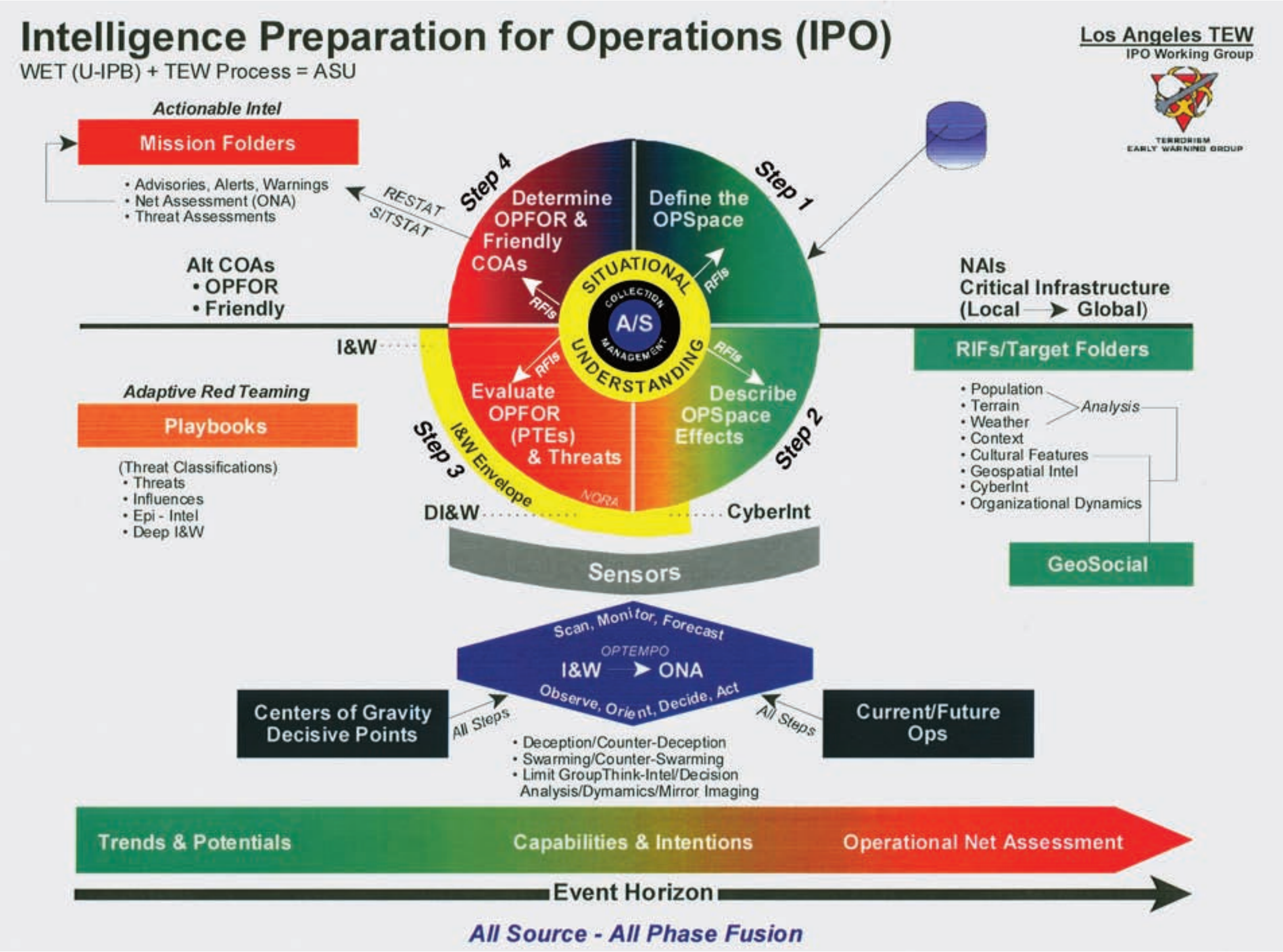
Foundational TEW Organization

(Fig. 1 in "Terrorism Early Warning and the Co-Production of Counterterrorism Intelligence" and "Intelligence Co-production and transaction Analysis for Counterterrorism and counter-netwar.")



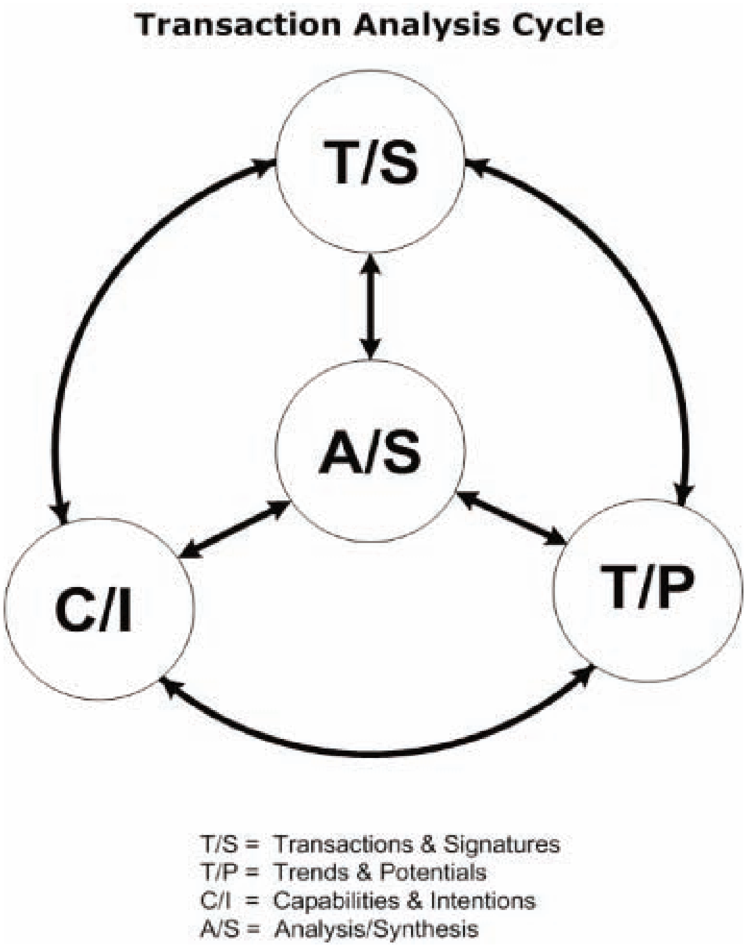
IPO Framework

(Fig. 1 in “Intelligence Co-production and Transaction Analysis for Counterrorism and Counter-Netwar” and Fig. 2 in “Terrorism Early Warning and the Co-Production of Counterterrorism Intelligence.”)



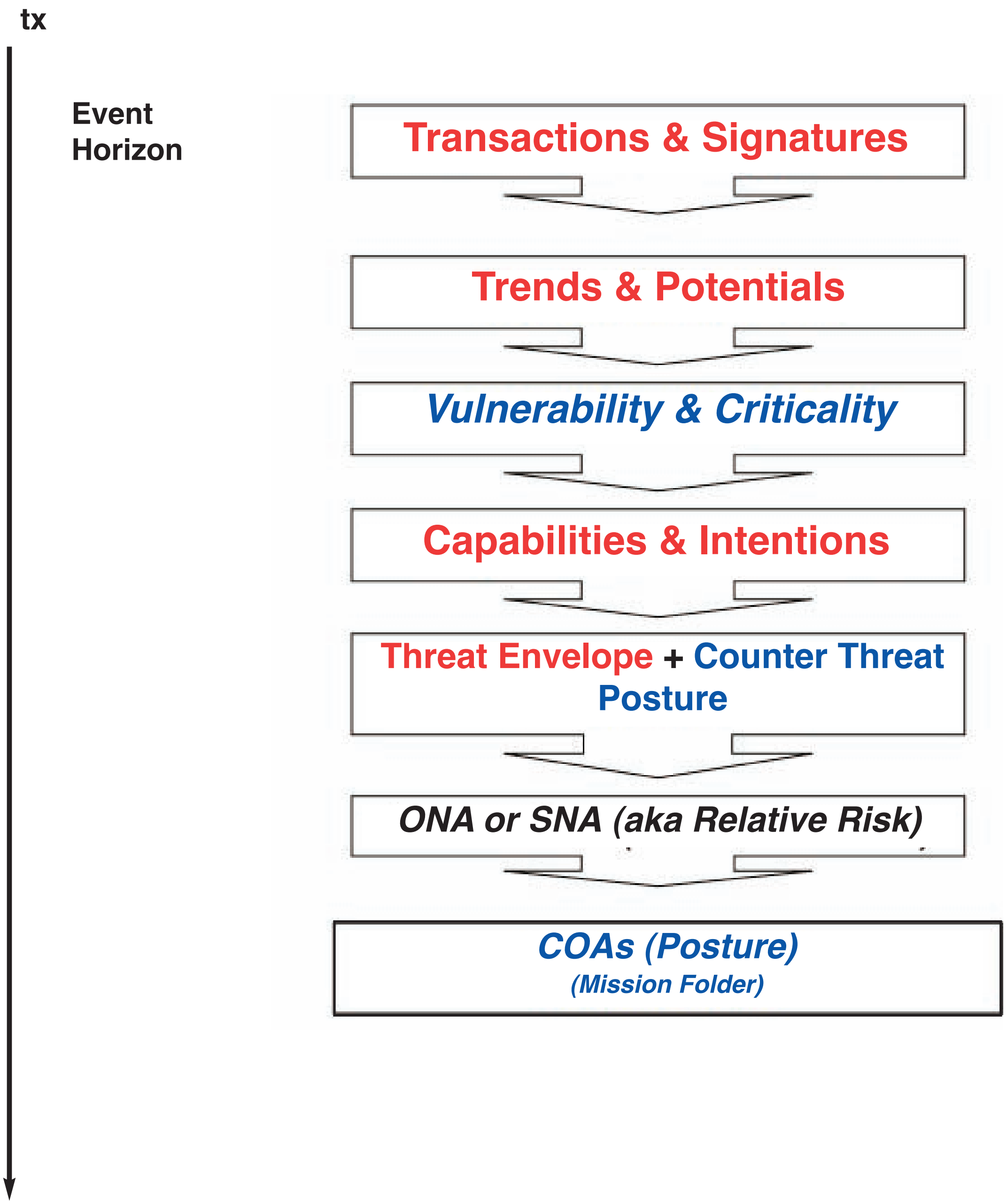
Transaction Analysis Cycle

(Fig. 3 in “Terrorism Early Warning and the Co-Production of Intelligence,” and Fig. 3 in “Intelligence Co-production and Transaction Analysis for Counterrorism and Counter-Netwar.”)


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

Transaction Analysis Model

(Fig. 2 "Intelligence Co-production and Transaction Analysis for Counterrorism and Counter-Netwar.")


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

PART THREE:

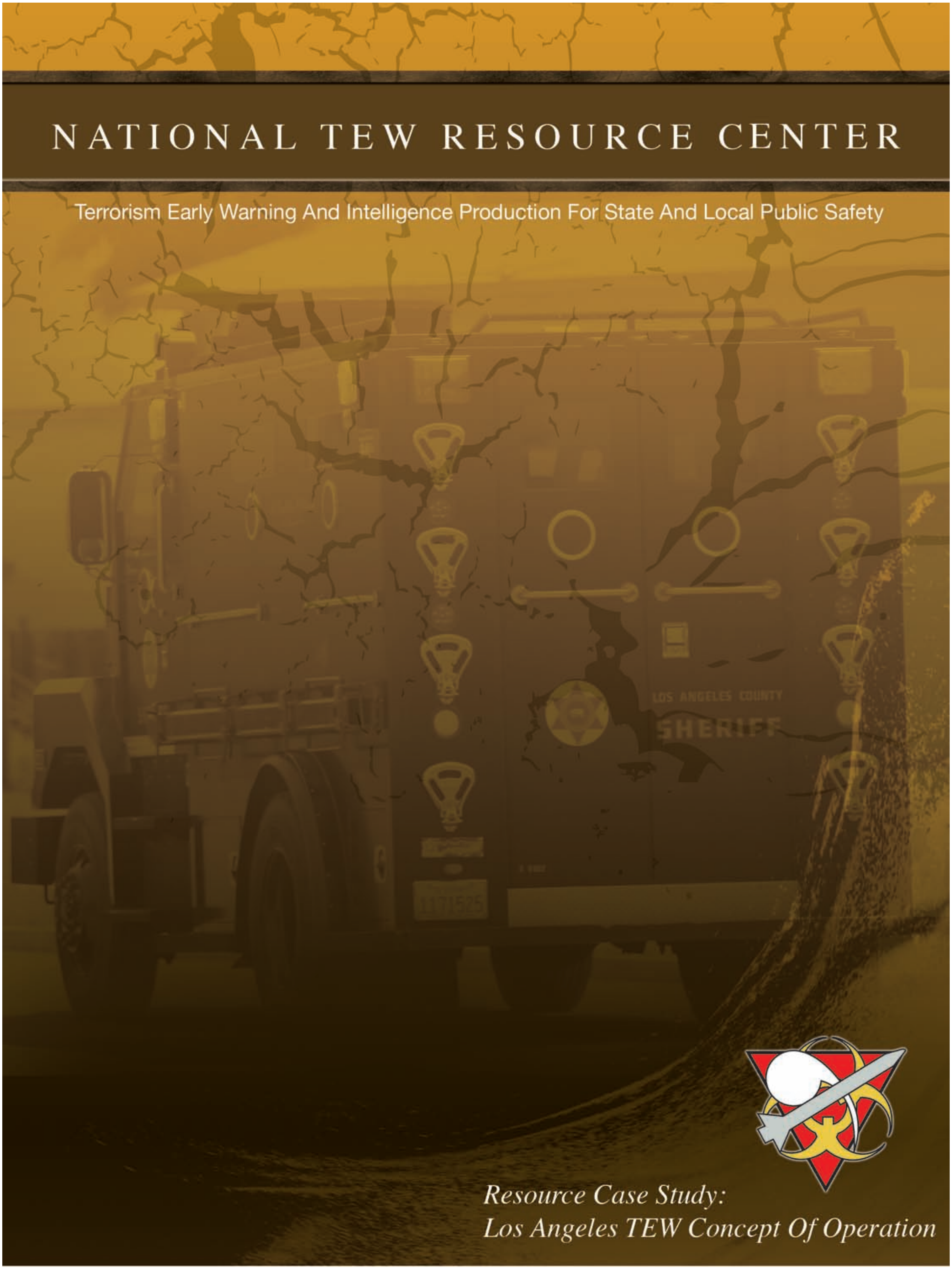
MODEL TEW CONOP

Unpublished text, Prepared by National TEW Resource Center, 2007.

The following section, part three of this text is a model TEW concept of operations. It was prepared by the National TEW Resource Center, based at the LASD Emergency Operations Bureau to capture the doctrinal practices of the LA TEW over a decade of evolution. It is reproduced here in its entirety.

NATIONAL TEW RESOURCE CENTER

Terrorism Early Warning And Intelligence Production For State And Local Public Safety



Resource Case Study:
Los Angeles TEW Concept Of Operation

Acknowledgements

This Resource Book is part of a continuing series issued by the National Fusion Process Resource Center. The National Fusion Process Resource Center is supported by the Los Angeles Sheriff's Department National TEW Resource Center with grant funds from the United States Department of Homeland Security.

This volume: *Terrorism Early Warning and Intelligence Production for State and Local Public Safety Agencies* provides a case study describing a historically effective concept of operations (CONOP) for fusion centers and terrorism early warning groups (TEWs) engaged in developing intelligence to combat terrorism and perform all hazards public safety missions. It recaps a decade of experience, practice and research captured by the Los Angeles Terrorism Early Warning Group (LA TEW) and its member agencies and associates.

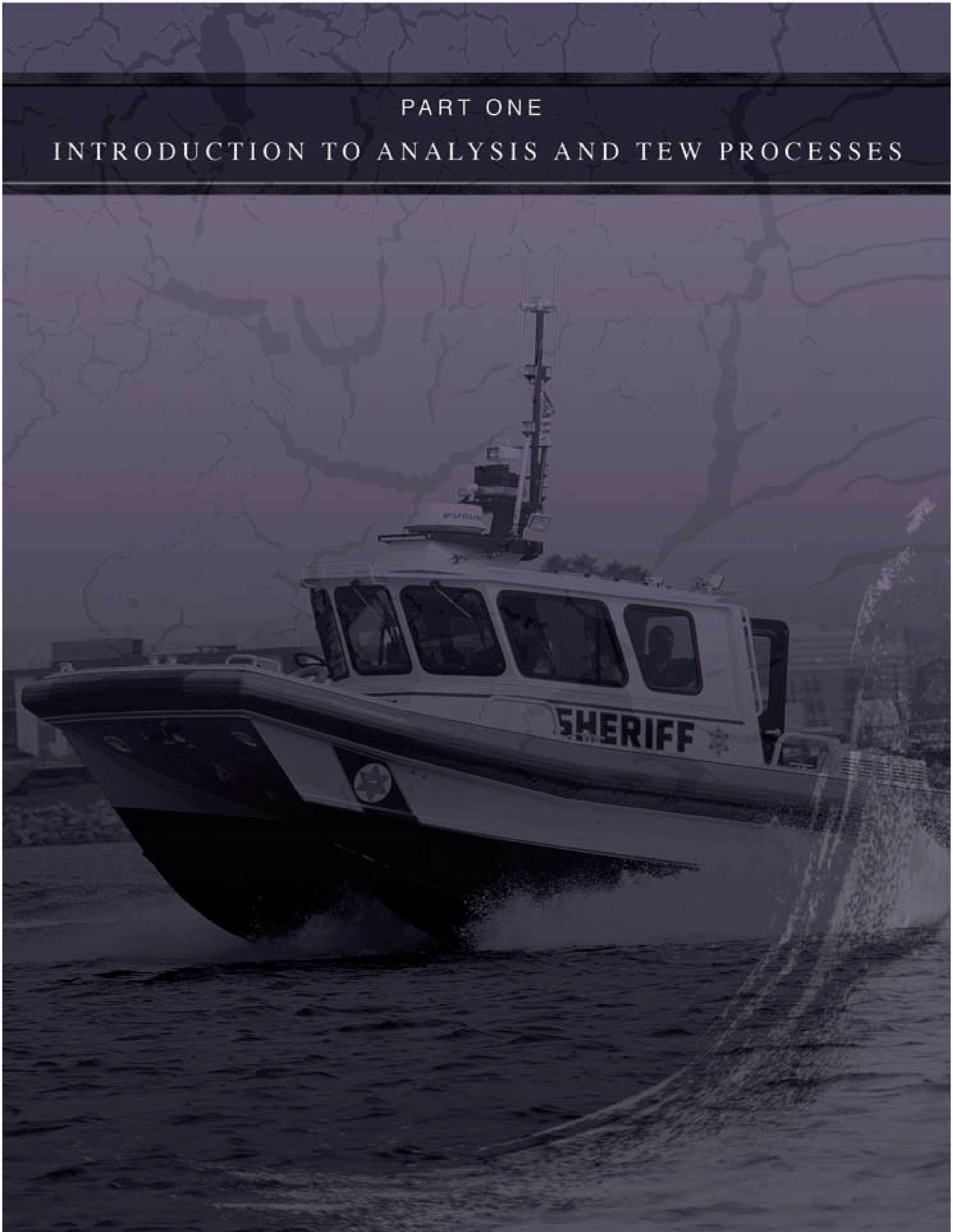
Lieutenant John P. Sullivan is the lead author of this volume. Chris Bausch, an adjunct member of the Los Angeles TEW, also made substantial contributions to this model CONOP. Other contributors include Sergeant Peter M. Jackson, Los Angeles County Sheriff's Department and various members of the Los Angeles TEW and the broader TEW and intelligence fusion communities.

TABLE OF CONTENTS

PART THREE

PART ONE

INTRODUCTION TO ANALYSIS AND TEW PROCESSES



Section 1.1 – INTRODUCTION

A. Purpose:

A CONOP is intended to outline a set of tactics, techniques and procedures (TTP) for operations. This model CONOP draws from the experience of the Los Angeles TEW to describe a model for TEW operations at other TEWs and may be applicable to operations at fusion centers as well. It describes concepts, theories and practices for conducting advanced counterterrorism intelligence operations, and sets forth guidelines for effectively integrating these practices into existing processes.

To accomplish this, the CONOP:

1. Describes the nature of the threat environment.
2. Defines the TEW mission and intelligence functions.
3. Defines the TEW operational objectives and mission essential tasks.
4. Describes implementation models and methodologies.

B. Scope:

This CONOP is a guidance document intended to describe tactics, techniques and procedures (TTP) available to the TEW and intelligence fusion communities providing all-source, all-phase intelligence to law enforcement, fire, emergency management and public safety agencies.

C. Goal:

The overarching goal of this CONOP is to document the processes that have evolved after a decade of experience in counterterrorism intelligence operations within the TEW, and establish an initial framework for institutionalizing TEW operational techniques.

D. Background:

The roles and responsibilities of the TEW are defined by the nature of the threat and threat environment. The current threat environment is highly complex, involving a new kind of warfare, one that is tailored to exploit the gaps and seams in our national composition, forcing our institutions of government into multiple, friction generating dilemmas. The threat environment also involves a new kind of adversary, one with a demonstrated capability and intention to target our population centers, avoiding completely any direct conventional military engagement.

As a result, local governments and local public safety agencies, charged with safeguarding the lives, property and services within their respective jurisdictions, are thrust directly into a preeminent role in this conflict. With the emergence of this role, local jurisdictions have an expanding requirement for threat intelligence composed of information from national sources, open sources, regional sources, and local sources, blended together into a fused intelligence product. Similarly, local jurisdictions have an expanding requirement for a local intelligence fusion capacity that is capable of harvesting the information stream, extracting the data nuggets that have value, injecting a local context, and developing a comprehensive intelligence picture.

E. The Operational Environment:

The TEW concept was developed to fill the need for recognizing potential threats, known as indications and warning (I&W), and developing situational awareness when a specific threat materializes, known as Operational Net Assessment (ONA), at the local/regional levels. Implicit in this approach is a recognition that:

- ❑ Traditional processes are too slow to combat networked transnational threats.
- ❑ Bureaucratic competition and organizational barriers create seams in national preparedness and intelligence sharing.
- ❑ The distinction between "Global" and "Local" is increasingly anachronistic. (Consider the impact of globally linked diaspora communities in fueling non-state conflict and terrorism.)

The TEW concept and approach is based on the recognition that local and regional agencies are producers as well as users of intelligence. The following precepts form a foundation for both individual TEWs and the need to link these TEWs into a national network.

- ❑ Intelligence for domestic civil protection (homeland security) is not solely a top-down, Federally-driven process.
- ❑ Intelligence must move top-down, bottom-up and laterally. There is also a need for bi-lateral police information sharing and cooperation, independent of federal agencies.
- ❑ Local police, public safety and health agencies may be first to observe indicators.
- ❑ Local responsibility to protect public and craft response.
- ❑ There is a need for accountability, structure/guidelines (i.e., doctrine) for access to national intelligence products.
- ❑ Regional entities (such as Terrorism Early Warning Groups) are partners in processing and disseminating intelligence (including providing local context and analyzing products) – there is significant value added by local knowledge.

Further, while an emphasis on prevention and deterrence (P&D) is a critical aspect to TEW operations, the domestic intelligence effort is not exclusively related to supporting criminal investigations or pre-attack, pre-event prevention. Intelligence sharing and access to a wide range of intelligence products is needed during attacks in order to develop effective consequence management efforts.

The Los Angeles TEW has evolved a comprehensive methodology for conducting counterterrorism intelligence operations that facilitate both a prevention and response orientation. Inherent to this methodology are activities that ensure jurisdiction-wide interagency cooperation, information sharing, and a robust flow of tactical reporting through government, business and community channels. This multi-disciplined, networked intelligence approach extends beyond the jurisdictional boundaries and includes close interaction with federal, state and regional information analysis centers. As a result, both the prevention focused Indications and Warning (I&W) activities, as well as the response focused Operational Net Assessment (ONA) activities at the core of TEW operations, are underpinned by a firmly established and aggressively maintained 'common' situational awareness.

The operational space can also be described, in national strategic terms, as an international crossroads, or a super-hub in the web of global interconnectivity. The mesh of this global web includes numerous cultural, economic, military, and social lines of influence, identity, communication, and dependency between the United States and the global community. For this reason, the TEW concept of operations calls for identifying, examining, and understanding as many of these 'threads' of influence as possible. Furthermore, the concept of operations calls for analysis and synthesis activities to examine the information stream within a local ↔ Global context as part of the I&W effort.

F. The Continuum of Operations:

The term *continuum of operations* is an expression used to describe a range of three possible threat or terrorist attack related circumstances that could exist in the operational space. The continuum is a helpful tool for describing how the TEW intelligence effort is tied to the dynamics of operational space. While it is possible for each of these circumstances to exist at the same time, for the purpose of this document, they are described within the context of a single incident and are related sequentially. Throughout this document the terms *pre, trans,* and *post*-attack will be used within the following context. Section 3.4 will describe these conditions in more detail.

❑ The three operational conditions:

1) Pre-attack phase—before an incident.

2) Trans-attack phase—during an incident.

3) Post-attack phase—after an incident.

The following section describes the essential components that make up the operational framework of the TEW.

Section 1.2 –
TEW Operational Framework Overview

A. TEW Mission:

The TEW mission is to develop operational intelligence for area of operations, and contribute to the co-production of intelligence across the TEW and intelligence fusion community in order to prevent, counter and respond to terrorism and emerging threats by conducting indications and warning and operational net assessment.

B. TEW Functional Objectives:

In accordance with its mission statement, the TEW provides operational intelligence support specifically within the following two intelligence functions: Indications & Warning (I&W) and Operational Net Assessment (ONA). Functional *objectives* are used to provide the operational context needed to translate functions into processes, tasks and activities.

Indications and Warning (I&W) Objective Overview-While conducting I&W, the TEW objective is to prevent and counter terrorism and emerging threats. This objective includes early recognition of threat or terrorist attack indicators, timely alerting and warning of appropriate agencies and tailored intelligence support to interdiction operations.

The TEW monitors trends and potentials that may result in terrorist threats or attacks within Los Angeles County and surrounding jurisdictions. This early warning element evaluates leads and reports of suspicious activity from public safety agencies, together with open source and sensitive data, and researches threat information to guide training, planning, and response efforts. The TEW works to identify precursor events when assessing trends and potentials, with the goal of prevention and deterrence.

Operational Net Assessment Objective Overview-While conducting Operational Net Assessment (ONA), the TEW objective is to support the response to threats and terrorist attacks and facilitate a high operational tempo (optempo) by producing timely, accurate and relevant intelligence, including tailored decision support and consequence mitigation intelligence products (utility).

During a known threat period or in the aftermath of an attack, the TEW actively monitors and assesses the current situation and status of all events that may impact the Los Angeles County Operational Area. In addition, the TEW employs advanced technological means (known as forensic intelligence support) to facilitate situation assessment and course of action development for the public safety community.

The TEW essentially provides a platform for networked, multilateral, horizontal communication of the threat information and intelligence needed to manage a complex urban operation. The TEW's net assessment process provides all-source/all-phase fusion to support decision-making and all public safety operations with an emphasis on future operations. The TEW bridges the gap between crisis action planning activities, i.e., the Rapid Response Planning Process (R2P2), and deliberate planning to provide the information necessary to achieve interoperability for complex, interagency, interdisciplinary, coalition-type operations.

C. TEW Mission Essential Tasks:

Tasks that must be accomplished in order to perform the functions addressed in the previous sections are identified on the Mission Essential Task List (METL). The TEW METL identifies the high-level process activities that are afforded the highest priority in respect to the commitment of personnel and resources during operations. Each task represents a critical aspect of the TEW mission that, if ignored, would result in an organizational failure in conducting either the I&W or Operational Net Assessment functions. METL, when evaluated during operations or exercises, is also instrumental for providing metrics for measuring organizational performance.

- **Target Management**
- **Threat Management**
- **Risk Assessment**
- **Collection Management**
- **Information Processing**
- **Intelligence Analysis**
- **Threat Recognition**
- **Consequence Assessment**
- **Intelligence Co-Production**
- **Dissemination and Feedback**

A brief description of each essential task follows. Each task will be addressed in much more depth in Part Two.

D. Target Management:

Target management supports both I&W and Operational Net Assessment by identifying and prioritizing potential targets within the operational area and ensuring measures are established for reducing each target's relative risk. Target management includes the following four sub-tasks: 1) Target Inventory, a process that identifies the jurisdiction's target contour and silhouette, 2) Target Modeling, a process that catalogs important response information for each potential target into a response information folder (RIF), 3) Target Integration, a process that identifies a potential target's vulnerabilities and generates both target hardening recommendations and random antiterrorism measures (RAMS), and 4) Target Forecasting, a process that determines a target's criticality as well as response resource requirements. Target integration and target forecasting activities are conducted as part of the risk-assessment.

E. Threat Management:

Threat management is a mission essential task that supports both the I&W and Operational Net Assessment functions by identifying and characterizing the jurisdiction's threat. Threat management is made up of four activities: 1) Threat Inventory, 2) Threat Modeling, 3) Threat Integration, and 4) Threat Forecasting. These activities and associated sub-tier activities emphasize identifying complex threat vectors such as CBRNE WMD, as well as local threat elements, determining their potential for interacting with global threat actors—such as al-Qaeda cadre—in the execution of an attack on local targets. Additionally, threat management emphasizes assessing local threat element activities within the context of a globally active kill-chain. (The term kill-chain is a reference to a terrorist group's attack processes.)

Note: Throughout this document, the expression OPFOR stands for Opposing Force, referring to all classifications of threat actor, threat group, terrorist, adversary, etc.

F. Risk Assessment:

Risk-assessment reviews threat factors, identifies vulnerabilities and determines criticality to define a target's *threat-envelope*. During the vulnerability analysis, risk-assessment compares the potential target's security attributes with OPFOR capabilities, intentions, tactics, techniques and procedures (TTP), and recent attack trends, identifying vulnerabilities and developing target hardening recommendations. Risk-assessment also involves conducting consequence and impact assessments to identify criticality issues. During threat management, threat-target profiles are developed into threat-target pairs to establish a baseline for conducting the *risk-assessment*.

G. Collection Management:

The collection management and planning task involves ensuring the quality—relevance and timeliness—and quantity of the information that feeds the intelligence process. The collection management task aims to identify information channels for satisfying each priority collection requirement tied to indicators and sub-tier specific information requirements. The strategy development includes leveraging/exploiting all available information resources, including Open Source Intelligence (OSINT), as well as information channels tied to classified resources, investigations, field units, Terrorism Liaison Officers (TLO), Infrastructure Liaison Officers (ILO), and the flow of "leads" reported into the TEW on a daily basis.

H. Information Processing:

For the TEW, intelligence is derived from all potential sources (classified, sensitive but unclassified, and open sources or OSINT) to provide information at all phases of a threat/response (pre-, trans-, and post-incident concepts described at the conclusion of this section).

I. Intelligence Analysis:

The essential *intelligence analysis* role of the TEW is to compile, fuse, analyze, and disseminate criminal intelligence and other information (including but not limited to threat assessment, public safety, law enforcement, public health, social service, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal activity.

The process involves TEW interaction, collaborations and information sharing with every level and sector (discipline) of government, private sector entities, and the public. The capstone activity within the TEW analysis process involves 1) a continuing emphasis on conducting all-source/all-phase information fusion as the central component to 2) an aggressive threat transaction analysis and synthesis effort that 3) develops, improves and exploits the *intelligence model*—adding information to it, and extracting new understanding from it—developed within the Intelligence Preparations for Operations (IPO) process.

J. Threat Recognition:

The TEW serves as a regional focal point for *situational awareness,* analyzing and synthesizing all-source information, and scanning the information stream for indications of an emerging threat. To do this, the TEW exploits information extracted from all available sources, ranging from raw leads collected through local channels to finished intelligence reports provided though national and global information channels such as OSINT and national intelligence products.

K. Consequence Assessment:

The emphasis of consequence assessment is to anticipate how potential hazard events will behave and identify what response resources will be needed to mitigate the hazard. The net-assessment provides the Unified Command Structure (UCS) and Emergency Managers in the EOC with current situational intelligence, threat course of action forecasts, hazard consequence forecasts, resource availability/requirement profiles and outlines Random Antiterrorism Measures.

L. Intelligence Co-Production:

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↔global fusion, or co-production, the TEW has developed an organizational structure and processes, including an Intelligence Preparation for Operations (IPO) based intelligence model, and the Transaction Analysis Cycle; it conducts exercises and is forming a networked framework for node-to-node collaboration.

M. Dissemination and Feedback:

The final task on the METL, and the last link in the intelligence logic chain before it cycles back to the beginning, is the dissemination and feedback task. Dissemination, at the most fundamental level, involves ensuring intelligence products are provided to the decision-maker. The feedback component of this task involves both active and passive measures taken by intelligence producers to stay abreast of the intelligence consumer's needs, ensuring intelligence products are relevant and have 'utility' value. These factors reach beyond the scope of merely satisfying information requirements. Positive feedback from the intelligence consumer in terms of relevance and utility reflect key measures of success for an intelligence operation and indicate the intelligence production process is effective and efficient.

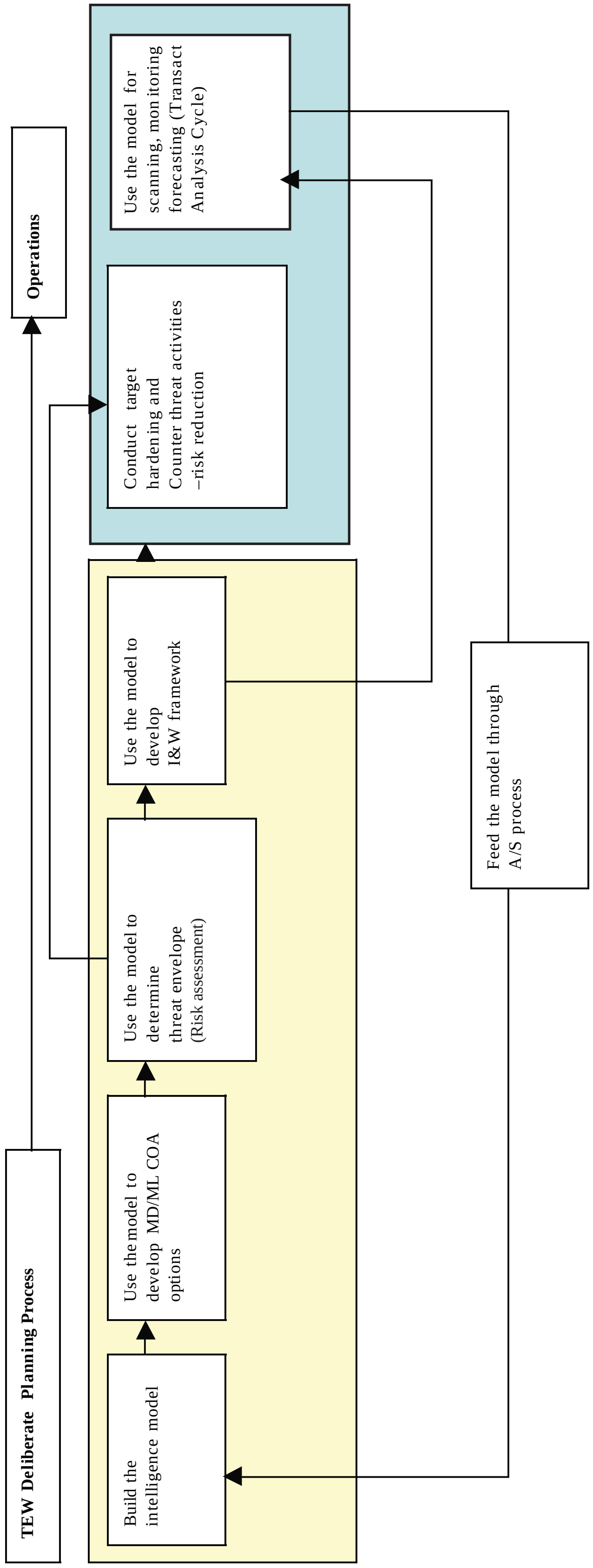
N. Flow of Operations:

TEW Deliberate Planning Process – The deliberate planning process is designed to provide intelligence support oriented on the following three operational priorities: 1) developing response information resources, 2) reducing the jurisdiction's target contour, and 3) anticipating hostilities. The flow of operations during the deliberate planning process involves mission essential tasks arranged in a logical order of precedence to do the following:

1. Develop (or improve) the intelligence model describing the dynamics of the conflict environment, including environmental attributes, targets, and threat dynamics. The model is developed using guidelines provided within the Intelligence Preparation for Operations (IPO) framework. The intelligence model then becomes a critical frame of reference for understanding situational developments. Additionally, as the model is developed, the response information packages and other important reference materials are created. Priority one is complete.

2. Naturally, once an intelligence model is developed, the first question one would ask is, "What is going to happen?" The intelligence model is used to identify threat course of action (COA) *options*. These COA options include threat-target combination as part of the assessment.

3. The next logical question that one might ask is, "Are the targets they may be planning to attack vulnerable?" "If they are attacked, what will be the impact?" Again, the intelligence model is used to identify the threat envelope around potential targets, resulting in target hardening and threat reduction recommendations. Priority two is complete.


TEW Deliberate Planning Process
Build the intelligence model
Use the model to develop MD/ML COA options
Use the model to determine threat envelope (Risk assessment)
Use the model to develop I&W framework
Conduct target hardening and Counter threat activities –risk reduction
Use the model for scanning, monitoring forecasting (Transact Analysis Cycle)
Operations
Feed the model through A/S process

4. At this point, one might ask, "How will we know they are coming?" In this regard, the intelligence model is the key to developing the I&W framework that will be used to develop a collection strategy and guide the threat recognition effort.

5. Finally, with the I&W framework developed, conduct scanning operations and watch for threat precursors using analysis/synthesis techniques that involve applying newly developed information to the intelligence model and extracting new understanding as a result. Priority three is underway, remaining a continuous task.

TEW Crisis Action Planning/Rapid Response Planning Process (R2P2) - Under circumstances involving an emerging threat or actual terrorist attack, the intelligence effort can transition to a more specific set of issues. Crisis Action Planning/R2P2 is then triggered. Crisis Action Planning/R2P2 involves developing situation-specific, incident-oriented decision support products within highly compressed timeframes. The process was designed with a basic assumption that when a critical event has happened or may be developing, the intelligence process must operate at a significantly higher optempo. The use of pre-scripted protocols and playbooks ensure the most effective use of time, guiding TEW personnel through the crisis action planning effort.

One of the first intelligence products to be developed and disseminated is a 'hasty' or 'provisional' net assessment. This product is intended to provide a decision-maker with a comprehensive orientation to all aspects of the situation and ensures all relevant knowledge has been shared with the appropriate commanders and managers. The intelligence emphasis now runs on two simultaneous tracks. The original I&W, long-range scanning effort continues along one track in addition to an R2P2 effort moving out on the second track to engage the emerging problem. During R2P2, the following occurs:

1. A new, more detailed intelligence model is developed based on the specifics of the situation.

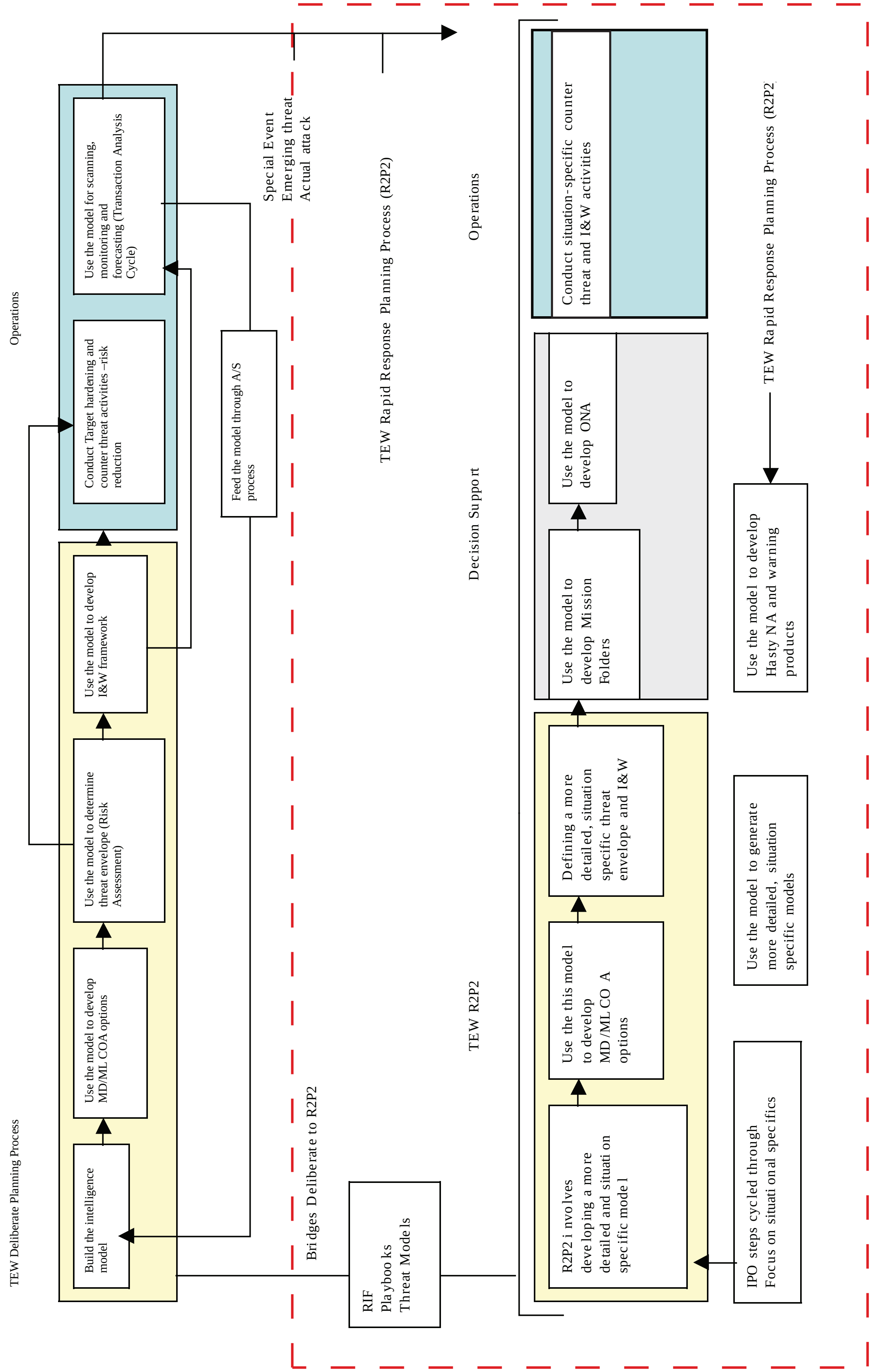
2. The new intelligence model is used to develop more specific threat COA options based on whatever particulars can be derived from the intelligence reporting (for example, specific targets, OPFOR, weapons, etc.).

3. A more detailed and specific assessment of the COA options leads to a more specific assessment of threat envelope variables and generates a more specific I&W framework.

4. Detailed mission folders and net assessment products are developed using the pre-packaged respons information support packages assembled before the crisis.

5. The I&W focus monitors developments to identify evidence confirming or denying the COA forecast.

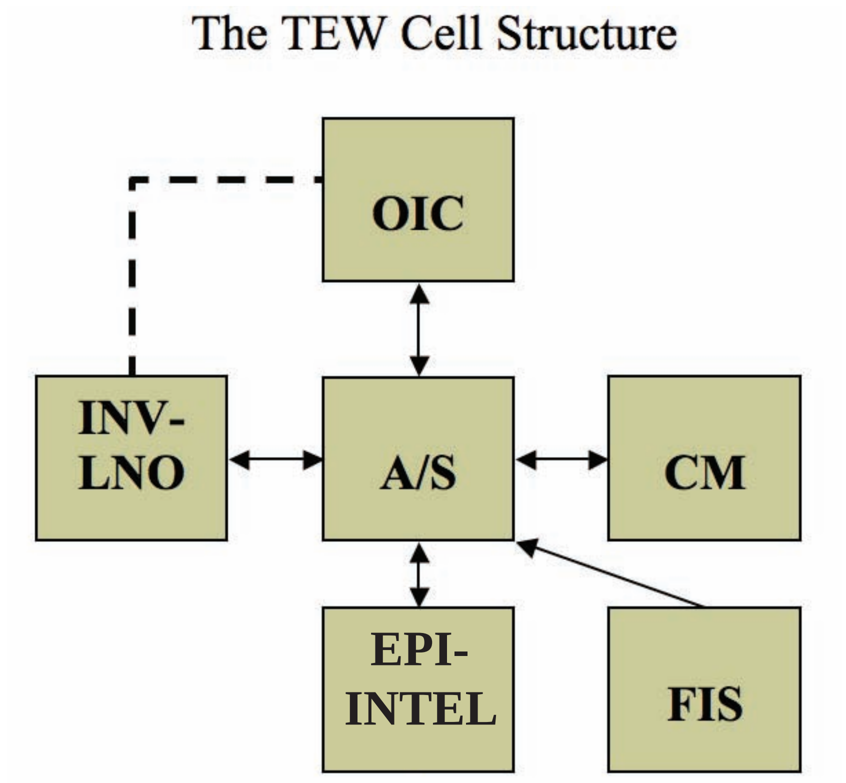
In both situations, the process involved a similar arrangement of task and activities that include developing the intelligence model, using the model to identify potential threat COA options, conducting risk assessments to determine criticality and vulnerability factors, developing the I&W framework, matching the indicator list to information resources, and then tracking the information stream for threat precursors.


TEW Deliberate Planning Process
Operations
Build the intelligence model
Use the model to develop MD/ML COA options
Use the model to determine threat envelope (Risk Assessment)
Use the model to develop I&W framework
Conduct Target hardening and counter threat activities –risk reduction
Use the model for scanning, monitoring and forecasting (Transaction Analysis Cycle)
Feed the model through A/S process
Special Event
Emerging threat
Actual attack
Bridges Deliberate to R2P2
RIF
Playbooks
Threat Models
TEW Rapid Response Planning Process (R2P2)
TEW R2P2
Decision Support
Operations
R2P2 involves developing a more detailed and situational specific model
Use the this model to develop MD/ML CO A options
Defining a more detailed, situation specific threat envelope and I&W
Use the model to develop Mission Folders
Use the model to develop ONA
Conduct situation-specific counter threat and I&W activities
IPO steps cycled through
Focus on situational specifics
Use the model to generate more detailed, situation specific models
Use the model to develop Hasty NA and warning products
TEW Rapid Response Planning Process (R2P2

Section 1.3 –
TEW Organizational Framework Overview

A. TEW Organization:

The TEW organization is designed to compliment operational requirements. The cellular structure is arranged to facilitate the conduct of both I&W and Operational Net Assessment intelligence functions, ensuring that multi-discipline subject-matter expertise underpins each aspect of the intelligence process, including requirements management, collections management, intelligence production, and dissemination. Further, the TEW is organized with an Analysis/Synthesis cell positioned as the organizational and operational hub with the other cellular nodes making up the spokes. This arrangement ensures that analysis/synthesis activities receive a rich flow of all-source/all-phase information.

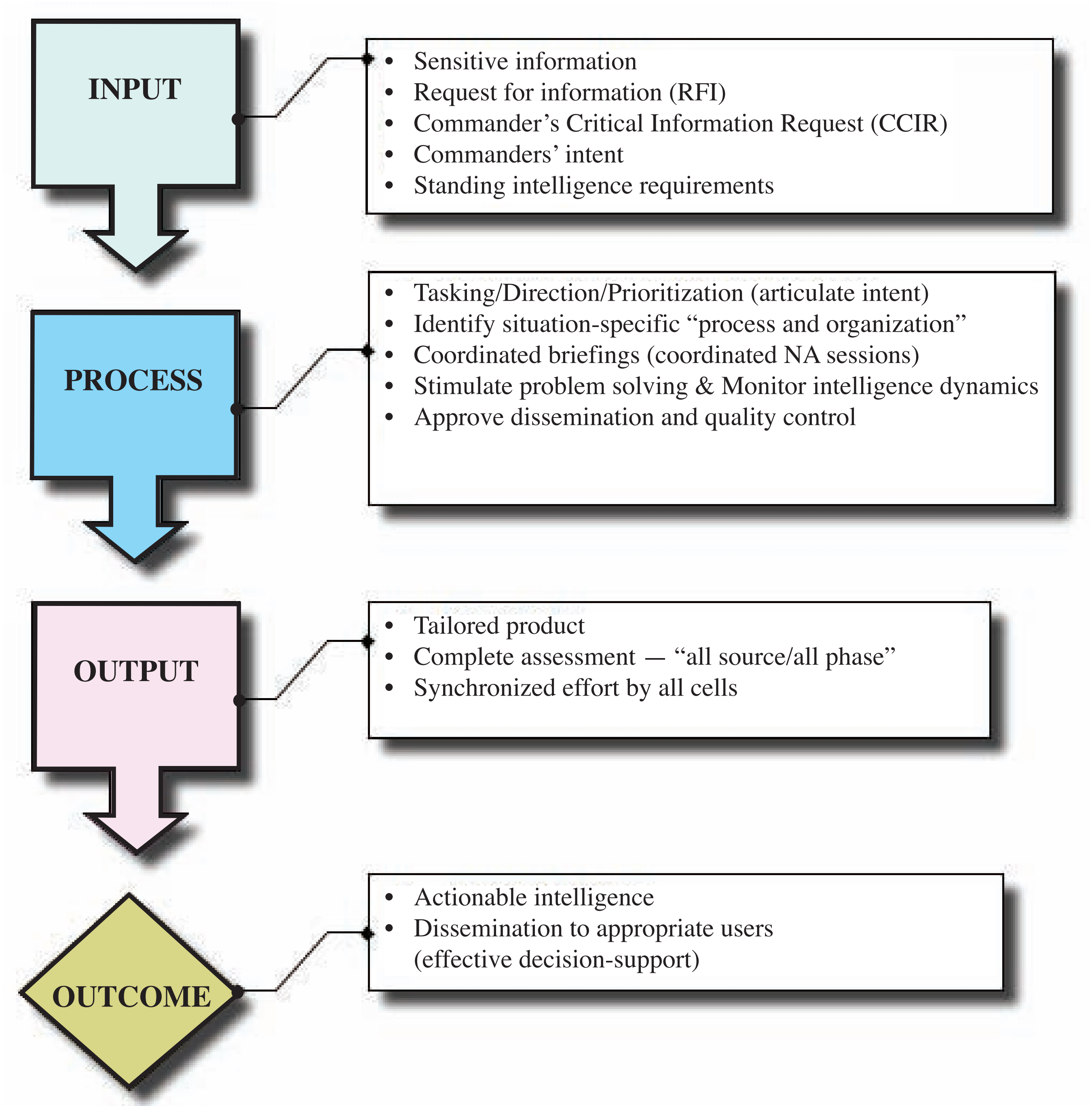


The TEW is organized into six cells: the Officer-in-Charge or OIC (Command), Analysis / Synthesis, Consequence Management, Investigative Liaison, Epidemiological Intelligence (Epi-Intel) and Forensic Intelligence Support cells. The Forensic Intelligence Support cell, which includes technical means and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

The OIC (or Unified Command) cell is a team that provides direction, sets intelligence requirements, and is responsible for interacting with prevention and response organizations and incident command entities. The Analysis/Synthesis cell coordinates net assessment activities and develops the collection plan (including tasking requests for information to the various net assessment elements). The Analysis/ Synthesis cell is also responsible for the intake of leads and reports, and developing the results of all the cells' analysis into actionable intelligence products (including advisories, alerts, warnings, and mission folders to assist response). 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. Finally, 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.

The following is a breakout of the organizational cells making up the TEW structure and an outline of each cell's *Inputs, Process, Output, and Outcome:*

The Officer-in-Charge Cell provides supervision and direction over the TEW. Additionally, the OIC provides tasking, ensures priority intelligence requirements are defined and processed through the TEW and developed into an appropriate intelligence product. Finally, the OIC provides quality control, ensuring products are disseminated and requirements are satisfied.



INPUT

- Sensitive information
- Request for information (RFI)
- Commander's Critical Information Request (CCIR)
- Commanders' intent
- Standing intelligence requirements

PROCESS

- Tasking/Direction/Prioritization (articulate intent)
- Identify situation-specific "process and organization"
- Coordinated briefings (coordinated NA sessions)
- Stimulate problem solving & Monitor intelligence dynamics
- Approve dissemination and quality control

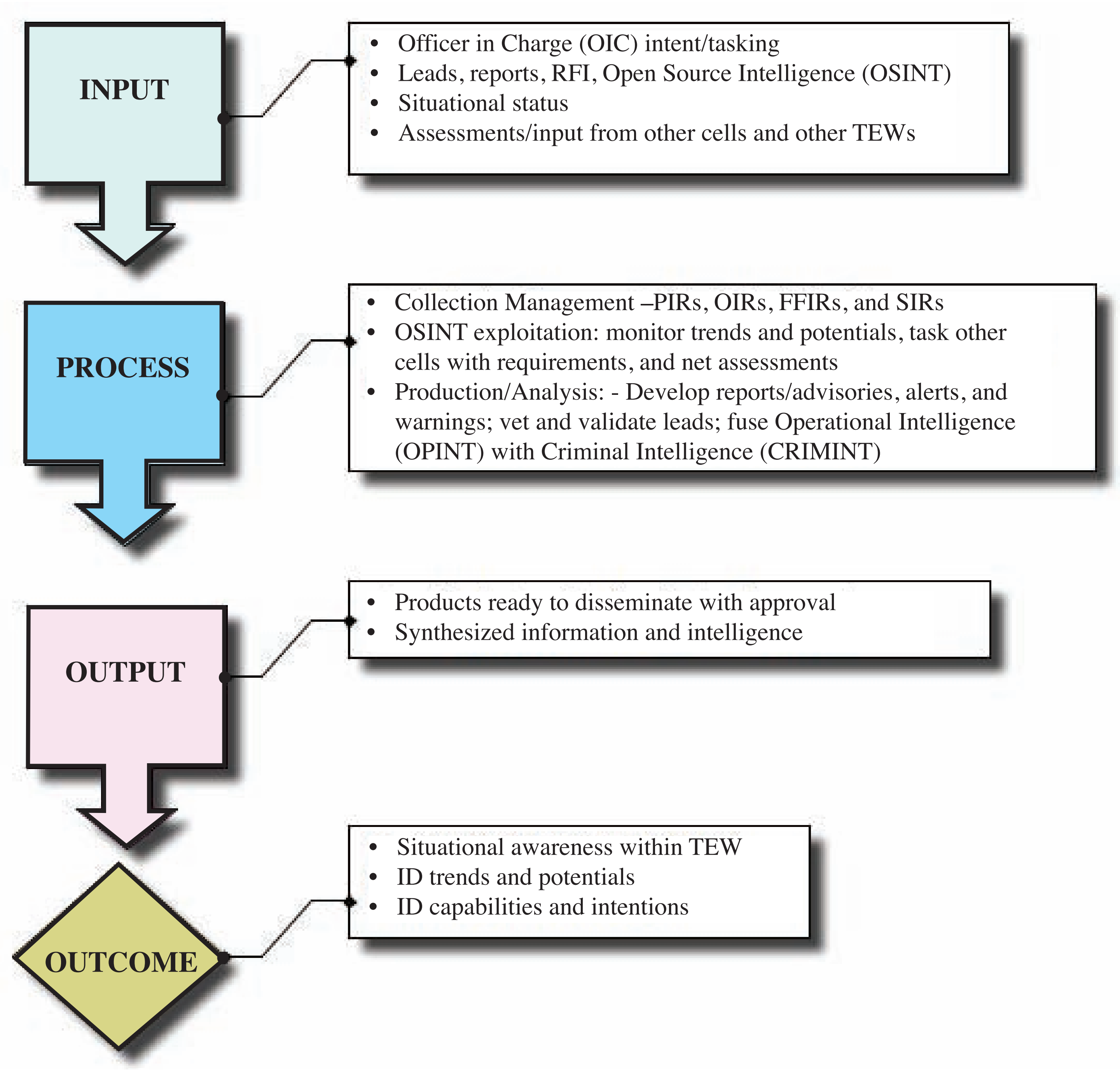
OUTPUT

- Tailored product
- Complete assessment — "all source/all phase"
- Synchronized effort by all cells

OUTCOME

- Actionable intelligence
- Dissemination to appropriate users (effective decision-support)

The ***Analysis/Synthesis Cell*** serves as the primary analytical element of the TEW, coalescing information processed through the subject matter experts from each of the other cells. The Analysis/Synthesis cell receives direction from the OIC and assists in breaking priority intelligence requirements into specific information requirements that can be tasked out to the other cells and further drive the collection strategy.



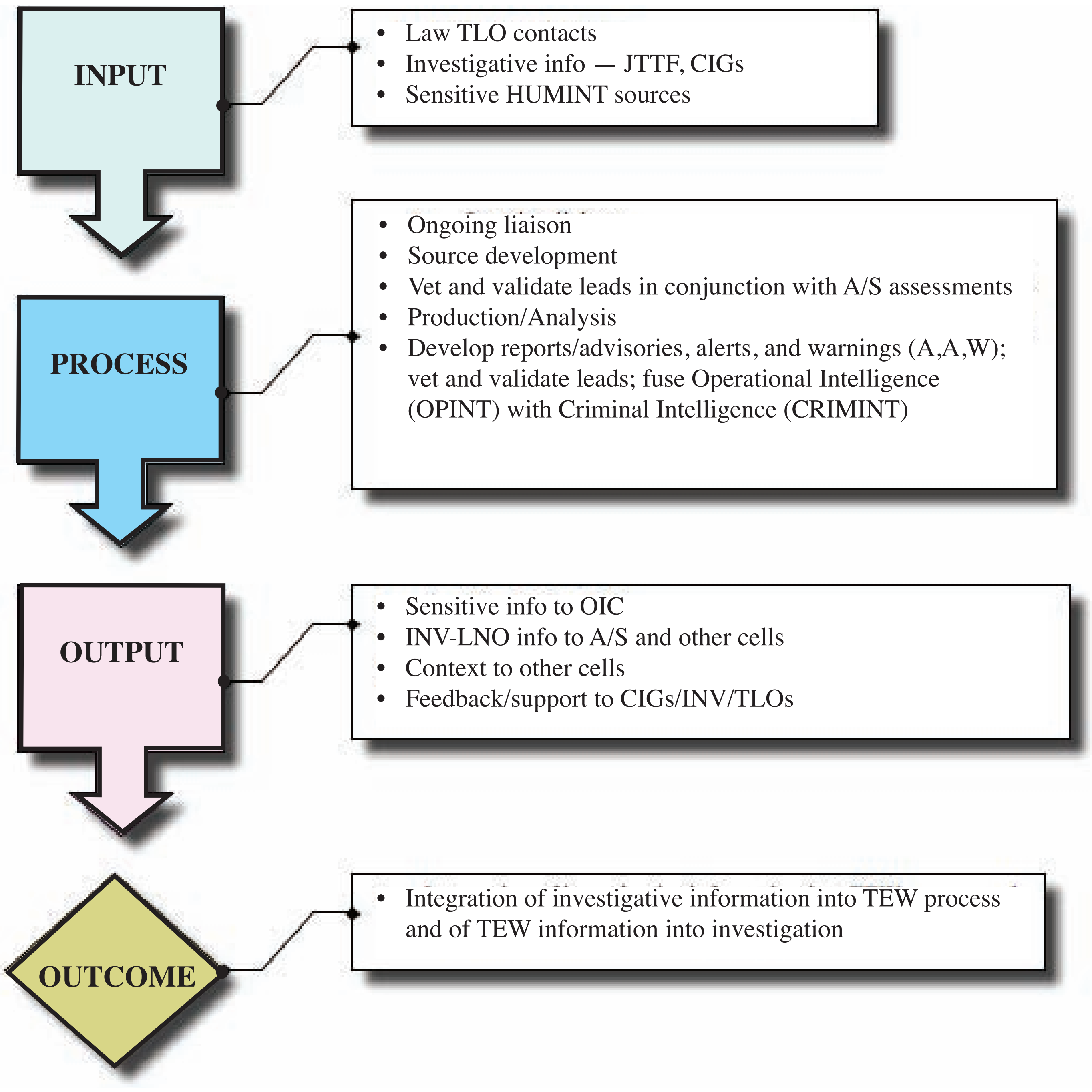
- Officer in Charge (OIC) intent/tasking
- Leads, reports, RFI, Open Source Intelligence (OSINT)
- Situational status
- Assessments/input from other cells and other TEWs

- Collection Management –PIRs, OIRs, FFIRs, and SIRs
- OSINT exploitation: monitor trends and potentials, task other cells with requirements, and net assessments
- Production/Analysis: - Develop reports/advisories, alerts, and warnings; vet and validate leads; fuse Operational Intelligence (OPINT) with Criminal Intelligence (CRIMINT)

- Products ready to disseminate with approval
- Synthesized information and intelligence

- Situational awareness within TEW
- ID trends and potentials
- ID capabilities and intentions

The ***Investigative Liaison Cell*** provides the linkage between the predictive intelligence mission of the TEW and the criminal intelligence function of other allied law enforcement agencies. As terrorism intelligence and criminal intelligence often share source characteristics, it is critical to ensure lateral cooperation. The Investigative Liaison Cell provides this conduit of cooperation.



INPUT

- Law TLO contacts
- Investigative info — JTTF, CIGs
- Sensitive HUMINT sources

PROCESS

- Ongoing liaison
- Source development
- Vet and validate leads in conjunction with A/S assessments
- Production/Analysis
- Develop reports/advisories, alerts, and warnings (A,A,W); vet and validate leads; fuse Operational Intelligence (OPINT) with Criminal Intelligence (CRIMINT)

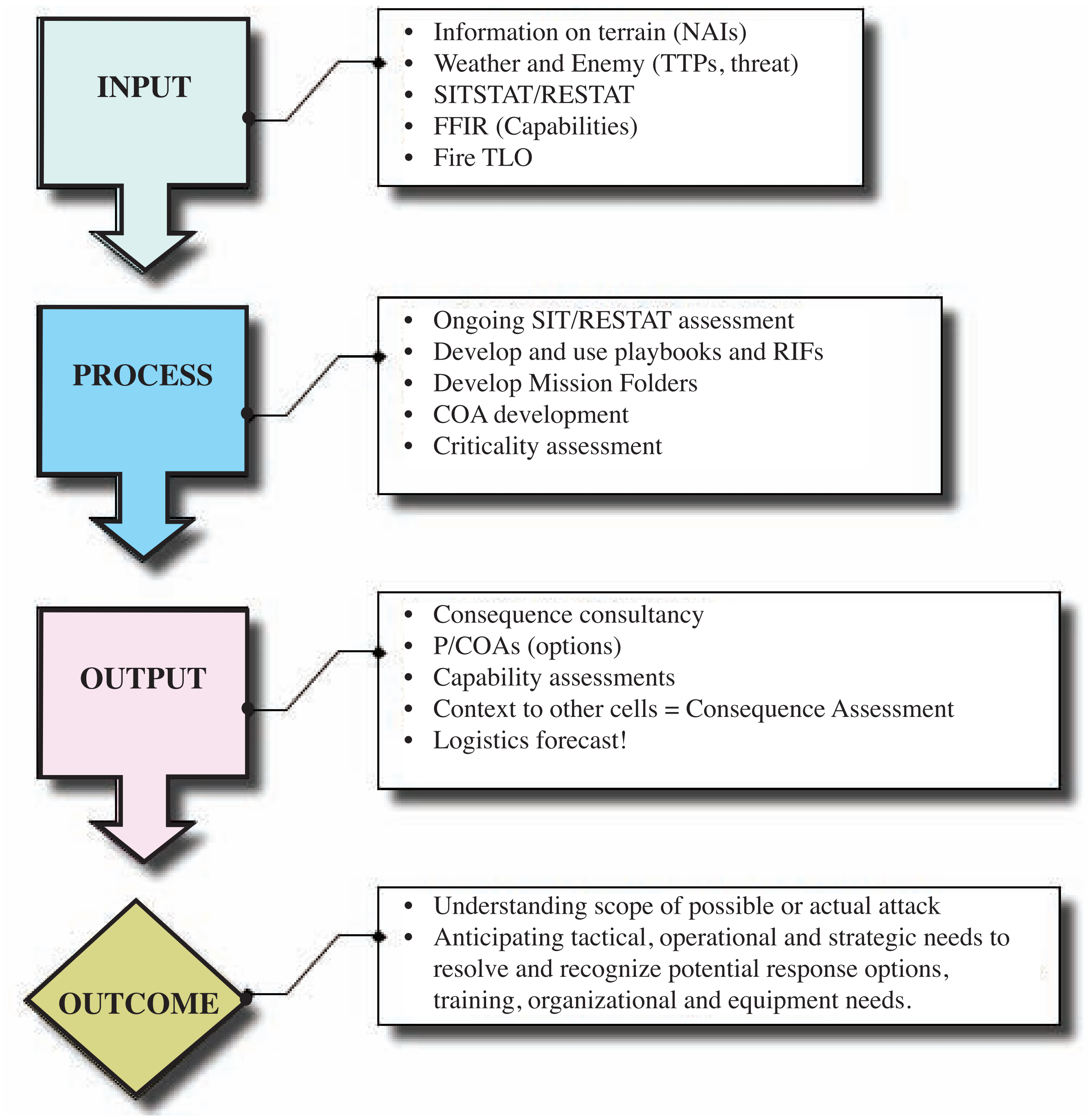
OUTPUT

- Sensitive info to OIC
- INV-LNO info to A/S and other cells
- Context to other cells
- Feedback/support to CIGs/INV/TLOs

OUTCOME

- Integration of investigative information into TEW process and of TEW information into investigation

The ***Consequence Management Cell's*** primary focus is on developing Mission Folders for assisting Incident Commanders in developing courses of actions for dealing with an incident. The Consequence Management Cell collects and processes incident-specific intelligence; develops a situational picture of the incident; models potential expansion issues; and recommends tactics, techniques and procedures for mitigating the effects of the incident.



INPUT

- Information on terrain (NAIs)
- Weather and Enemy (TTPs, threat)
- SITSTAT/RESTAT
- FFIR (Capabilities)
- Fire TLO

PROCESS

- Ongoing SIT/RESTAT assessment
- Develop and use playbooks and RIFs
- Develop Mission Folders
- COA development
- Criticality assessment

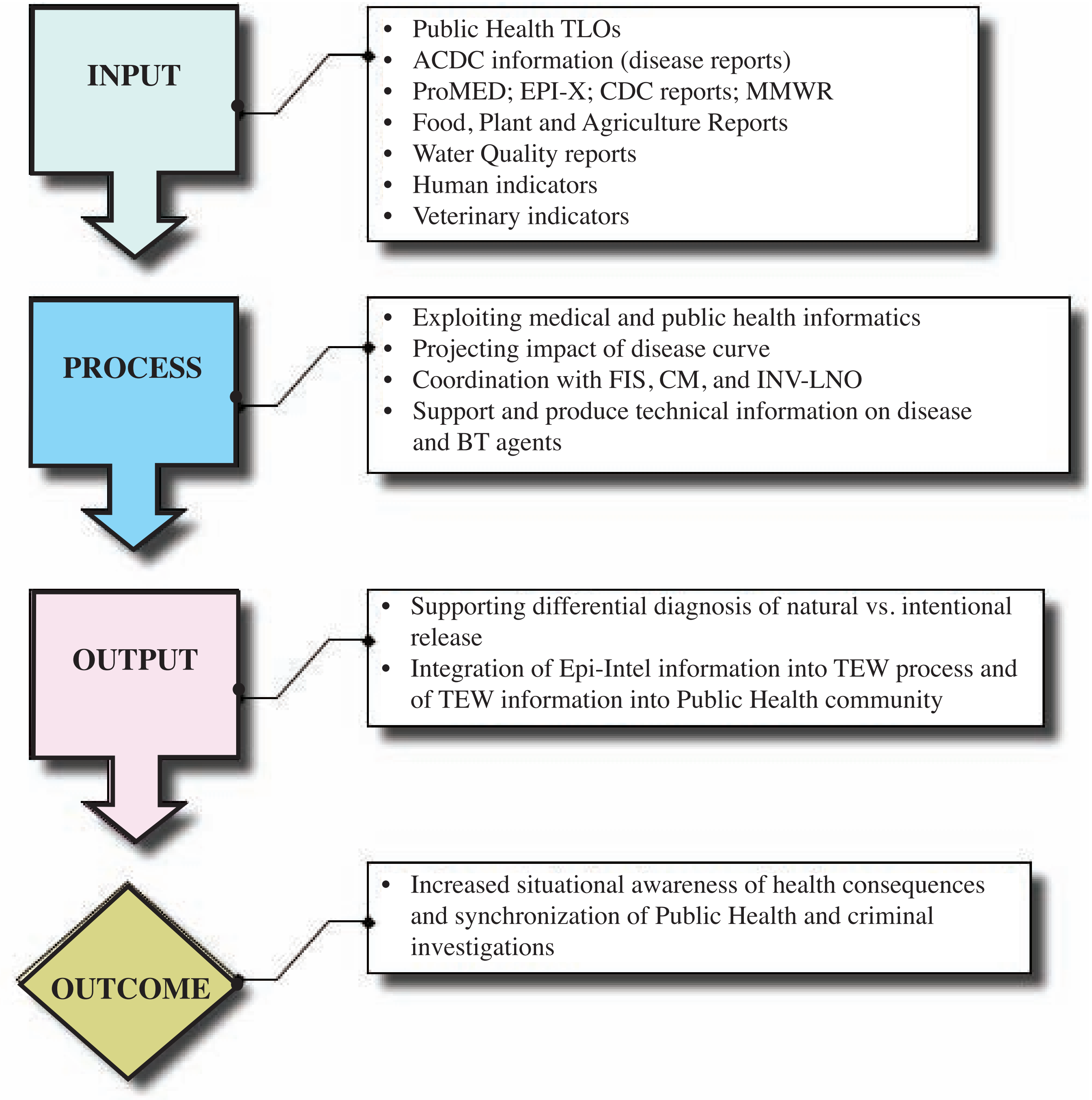
OUTPUT

- Consequence consultancy
- P/COAs (options)
- Capability assessments
- Context to other cells = Consequence Assessment
- Logistics forecast!

OUTCOME

- Understanding scope of possible or actual attack
- Anticipating tactical, operational and strategic needs to resolve and recognize potential response options, training, organizational and equipment needs.

The ***Epidemiological Intelligence Cell*** provides the conduit between the TEW and the public health community. The EPI-Intelligence Cell's primary functions include disease surveillance and tracking suspicious outbreaks and other bio attack early warning indicators.



INPUT

- Public Health TLOs
- ACDC information (disease reports)
- ProMED; EPI-X; CDC reports; MMWR
- Food, Plant and Agriculture Reports
- Water Quality reports
- Human indicators
- Veterinary indicators

PROCESS

- Exploiting medical and public health informatics
- Projecting impact of disease curve
- Coordination with FIS, CM, and INV-LNO
- Support and produce technical information on disease and BT agents

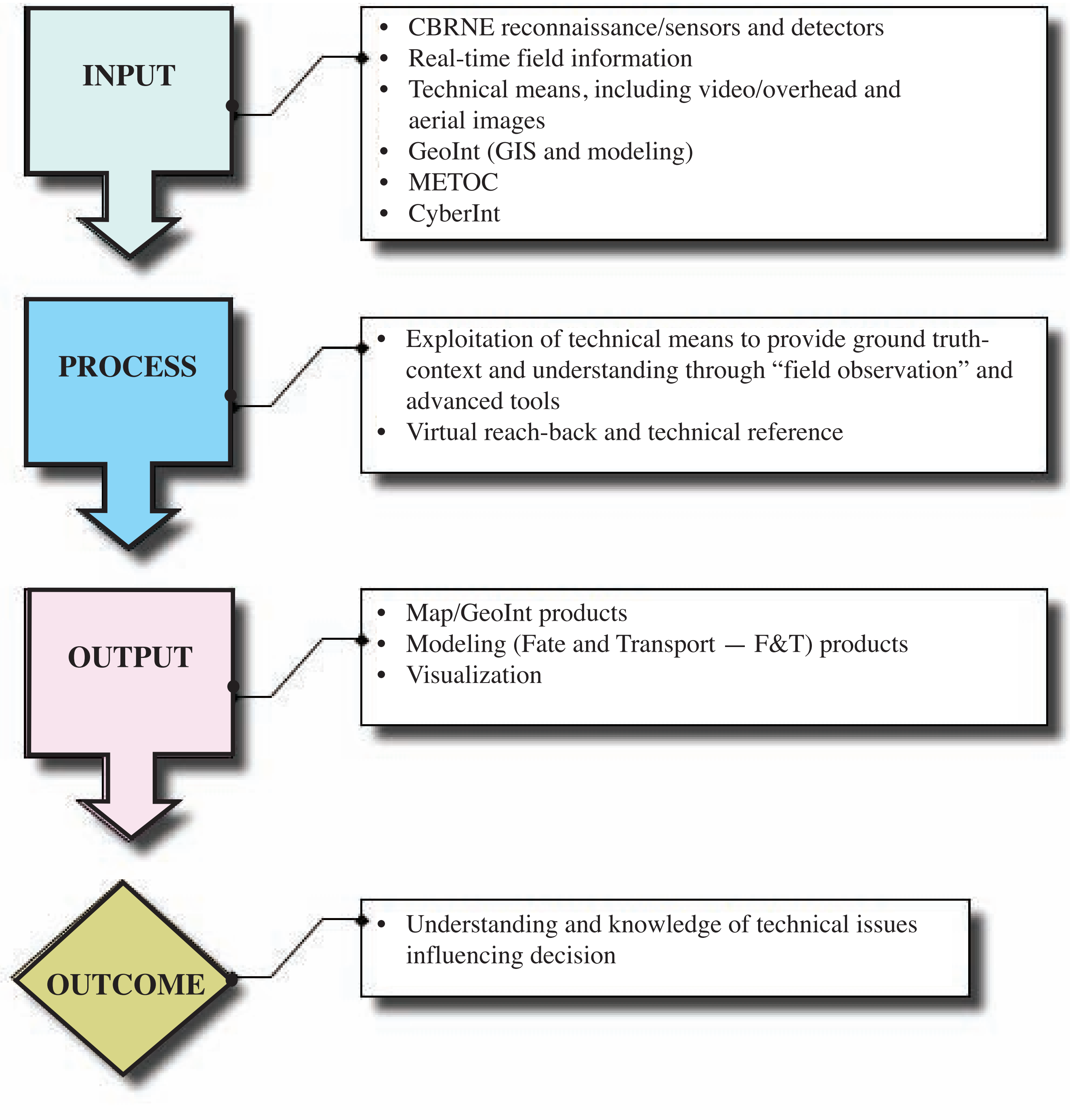
OUTPUT

- Supporting differential diagnosis of natural vs. intentional release
- Integration of Epi-Intel information into TEW process and of TEW information into Public Health community

OUTCOME

- Increased situational awareness of health consequences and synchronization of Public Health and criminal investigations

The ***Forensic Intelligence Support Cell*** provides a technical support function including field assessment, HAZMAT reconnaissance, sampling and specialized detection in support of an incident commander. Additional technical support includes Geospatial intelligence and reach-back to national resource centers.



INPUT

- CBRNE reconnaissance/sensors and detectors
- Real-time field information
- Technical means, including video/overhead and aerial images
- GeoInt (GIS and modeling)
- METOC
- CyberInt

PROCESS

- Exploitation of technical means to provide ground truth-context and understanding through "field observation" and advanced tools
- Virtual reach-back and technical reference

OUTPUT

- Map/GeoInt products
- Modeling (Fate and Transport — F&T) products
- Visualization

OUTCOME

- Understanding and knowledge of technical issues influencing decision

B. Agency Participation:

A critical aspect of the TEW organizational model is the participation of law enforcement, fire, public safety, health and emergency management specialists drawn from key agencies from across the jurisdiction to staff the TEW's organizational cells. Additionally, the TEW relies on active coordination and cooperation with regional, state and federal agencies. In addition to drawing permanent personnel from these agencies, an effective means for expanding the reach and breadth of information flow, as well as the expertise available to the TEW is the Terrorism Liaison Officer (TLO) program. The TLO program expands the information exchange network through the appointment of representatives within public safety, emergency management, public health, emergency support services and other key agencies in county, city or special districts to act as collaboration channels and facilitate information exchange between participating agencies and the TEW.

C. Supporting Committees:

A TEW can rely upon several committees comprised of personnel from participating agencies to perform its functions. These committees can be used during the early phases of implementation in absence of a full-time standing TEW or to support a full-time TEW by expanding its reach into the response community. As previously stated, the "Net Assessment Group" comprises the core of an operational TEW. It can be stood up on an ad hoc basis or, when sufficient resources exist, as a permanent fusion structure. Other committees that have been utilized in Los Angeles and elsewhere include a Playbook Committee, an Emerging Threats Committee, and an IPO Working Group. Others have been established on an as-needed basis to support short-term or specialty needs that arise when building capability.

D. Tactical Liaison Teams:

During large-scale complex field response or in order to support special events, representatives of each TEW cell can be configured into a tactical liaison team to provide support to a field command post and facilitate reachback to the TEW itself. These teams can be tailored for the specific incident type according to its unique intelligence support needs. A tactical liaison team can also be used to provide surge capacity to another TEW during a critical event.

E. Interaction with Other Agencies:

The Investigative Liaison (INV-LNO) Cell is the TEW linkage with investigative agencies. This cell is responsible for processing, tracking, and collecting all criminal and national security intelligence information and leads related to terrorism. This cell is the primary point of contact with all classified, national and state databases and with investigative and intelligence efforts at all levels of government.

The INV-LNO cell is responsible for vetting and validating leads and assessing specific threats. This cell is also responsible for tasking other specialized investigative entities to develop a complete intelligence picture. Information and intelligence developed by the INV-LNO cell is integrated with other information/intelligence products developed by its partner Net Assessment cells through the Analysis/Synthesis cell.

F. Interaction with Other Public Safety Agencies:

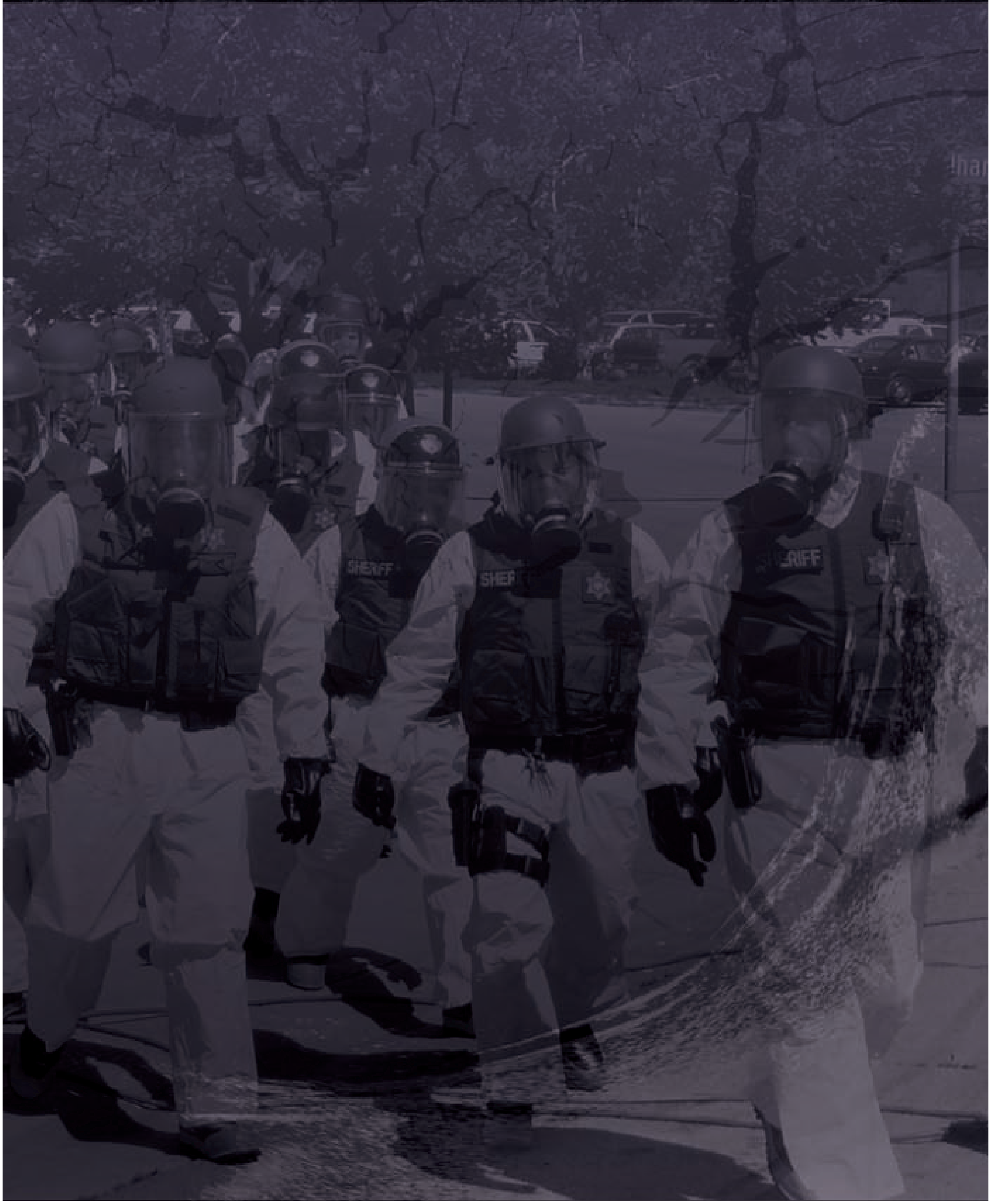
During an actual event or incident response, it may be desirable to send a TEW liaison officer (LNO) to a field command post, emergency operations center or to other intelligence fusion centers operating in support of a specific response. For example, in Los Angeles where the TEW provides intelligence support to the County Emergency Operations Center (CEOC), a designated senior TEW representative is provided to the CEOC management staff to facilitate the flow of sensitive, time critical information and provide technical assistance.

During major field responses, a TEW representative can be provided to the Incident Commander for the same purpose. TEW LNOs can also be deployed to support investigative efforts. Generally, this is a function of the Investigative Liaison cell. In addition, the Forensic Intelligence Support cell has the specific responsibility of liaison with the Hazmat group and/or Weapons of Mass Destruction Civil Support Team (CST) during a field response involving a CBRNE agent.

G. Initiatives:

The TEW is involved with a number of initiatives. These include a full-time cadre comprised of staff contributed by agencies to staff a watch and fusion center for assessing pre-incident indicators and threats. In addition, the TEW holds a monthly meeting to foster coordination and skills development, and coordinates a network of "Terrorism Liaison Officers" (TLOs) at each law enforcement, fire service, and health agency in the county. TLOs serve as the conduit to bring threat information to the TEW for assessment and for bringing actionable intelligence from the national level and the TEW to field personnel. TLOs also coordinate with private infrastructure partners. Private sector partners are encouraged to establish Infrastructure Liaison Officers (ILOs) to interact with the TEW's network of TLOs. Within this framework, community police are the first link to the public. The expertise and familiarity of local beat officers, or fire companies when related to life safety threats, is supported with strategic analysis and intelligence support from the TEW. The TEW can then gain an understanding of what is happening on the street and can tell field personnel what to look for based upon global trends and specific threat information.

PART TWO
MISSION ESSENTIAL FUNDAMENTALS & ANALYTICAL TRADECRAFT



Section 2.1 –
Decision-making and Intelligence Fundamentals

A. Overview:

Part One of this CONOP provided a basic overview of the TEW concept, describing its evolution within the current threat environment as well as the key components of its operational framework—mission, functional objectives, tasks and organization. Part Two builds on this basic overview by drilling down into each of the functional objectives, thus describing the fundamental processes and activities inherent to each. The presentation methodology is intended to be more instructional, addressing topics at the survey level, outlining concepts, processes and activities, offering explanations and examples, and providing a base frame of reference for understanding TEW operations.

B. Intelligence and decision support:

> *Successful intelligence operations are a result of consistent dedication to the fundamentals of sound intelligence analysis that is 1) founded in a clear understanding of the nature of the conflict and the intelligence consumer's needs, and 2) driven by a well-defined process for working through the information stream, identifying and then developing the key fragments of information into useable intelligence products that satisfy the consumer's requirements and reduce uncertainty*

The following section provides a brief overview of the underlying concepts, principles and processes that proved instrumental in shaping TEW operations. As identified in the opening quote, an effective intelligence operation is one that understands and effectively feeds the decision-making system it supports. The design and evolution of the TEW was significantly influenced by this principle, and, as a result, TEW processes have an inherent decision-support emphasis. With this in mind, we begin with a review of the fundamentals of decision-making theory, emphasizing the concepts developed by Colonel John Boyd, the father of the Boyd Cycle, also known as the OODA loop.

C. Decision-Making Concepts:

The ability to move rapidly through the decision-making process has positive tactical consequences. The intelligence process, when focused on product relevance and utility, significantly enhances friendly force operations by contributing to an increasingly faster decision cycle. So what is so important about making faster decisions?

The amount of time it takes an organization's decision-making system to generate actionable decisions is called its "tempo" of operations (optempo). Organizations that are able to rapidly execute decisions are said to have a high optempo. Any organization seeking to interact with an environment that is characterized by rapidly changing conditions will need to have an optempo that can move faster than the environment or it will not survive.

The requirement for a high optempo capacity is even more important in a conflict environment involving two opposing and hostile wills. In this type of environment, a common goal is to overwhelm the opponent's decision-making system (also command and control system) and drive the opposition force to paralysis by presenting them with multiple, increasingly more complex problems, and eventually internal friction melts the system down.

History shows that the decision-maker who best analyzes, decides, and controls the pace of interaction with an opponent will prevail, whether that opponent is an unthinking force of nature or malicious thinking enemy. The validity of this phenomenon has been demonstrated and documented through numerous studies conducted by the military, academia, business enterprises, and emergency responder groups. Many of these efforts have produced models – illustrations and flow charts – that describe the decision-making process in an endeavor to discover opportunities for increasing an operation's optempo. A simple Google search of "decision-making" will offer ample resources if one were inclined to decipher highly complex charts and graphs. However, as an alternative for those who only want to understand decision-making fundamentals, they should review the work developed by John Boyd, the creator of the Boyd Cycle, also known as the OODA loop.

The OODA loop offers the most preferred technique for addressing decision-making concepts. The model is used extensively, particularly by the military, as a decision-making process template. It graphically depicts decision-making as a simple four-phase cycle that involves Observing the environment, Orienting to what was observed, Deciding on a course of action, and Acting. All organizations operate within some form of OODA loop. Organizations with rapidly turning OODA cycles are able to operate at a high optempo and can influence their environment more rapidly, forcing a slower adversary to be continuously reacting, increasingly reducing their ability to conduct coordinated actions. When this happens, the side with the faster OODA loop has seized the initiative and is dictating the flow of the conflict.

The OODA loop model is applicable as an assessment tool for tactical, operational and strategic operations. Further, it works when applied to other conflict environments as well, such as firefighting or law enforcement where extraordinarily high optempo decision cycles are required. The OODA loop is also useful for identifying and rectifying systemic impediments in an organization's operating processes. The military's doctrinal approach to battlefield command and control, for example, has recently shifted favor away from the traditional centralized layered hierarchy model over to the network centric (swarming) model in order to facilitate the rapid execution (high optempo) of battlefield decisions.

The military is continuously refining procedures in order to enhance the efficiency of the Observe and Orient phases of the decision-making system. These efforts produced the Intelligence Preparation of the Battlespace methodology, a practice that integrates the intelligence and operations staff components around a comprehensive decision support process. Further, OODA loop principles have driven advances made in battlefield sensor technologies as well. With the emergence of precision guided weapons and new sensor packages, it is now possible for concepts such as sensor-to-shooter to become a reality, creating an operational environment where military commanders cycle through Observation-Orientation-Decision-Action almost instantaneously.

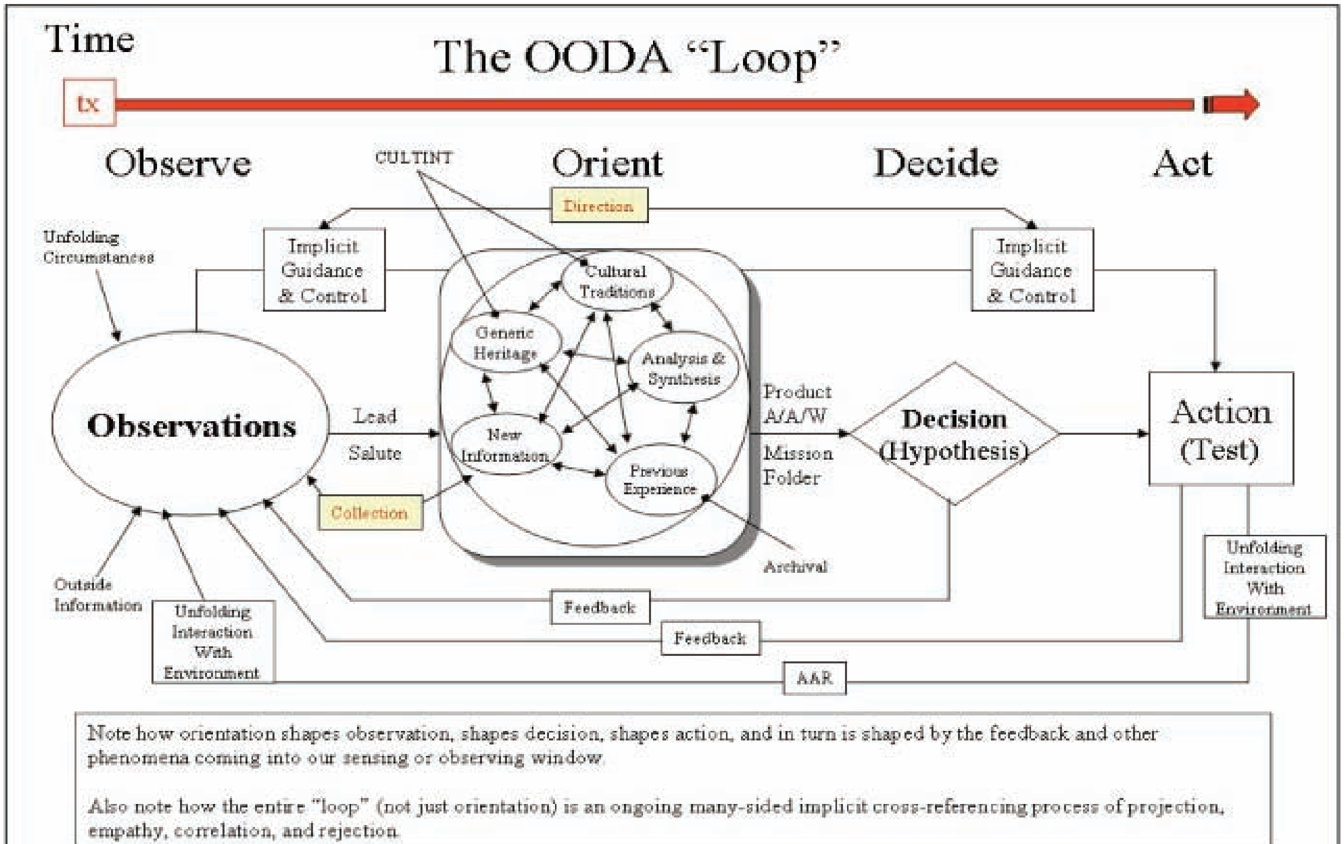
Individual functions that contribute to the decision cycle are also assessed to ensure internal processes do not create choke points or friction points that bog the cycle down. Intelligence production, for example, is a critical component of the Observe and Orient phase of the OODA loop. A decision-maker's ability to rapidly cycle through both these phases is strongly dependent on an effective intelligence process with the capacity and capability to provide a steady flow of quality intelligence. In any operational environment involving the use of intelligence, the process used to develop decision support products must be tailored to satisfy both the system's knowledge requirements and its desired pace of operations.

Intelligence is developed within a process that involves refining information into a product that facilitates a timely decision. In fact, the effectiveness of an intelligence operation is determined largely by the quality of the intelligence it produces, measured primarily by factors such as timeliness, accuracy, relevance and utility.

While the intelligence product's timeliness and accuracy are critical, the primary value of the product is determined by its relevance and utility within the decision-making system it is intended to support (customer satisfaction). A product that is relevant provides a decision-maker with actionable intelligence, meaning the intelligence provides specific knowledge the decision-maker needs to execute a decision "right now." Intelligence reports that are tied to decision points, also referred to as decision triggers, provide situational intelligence the decision-maker needs and reflect relevance to critical aspects of an operation in terms of time, space and context.

Intelligence that has utility will be easily deciphered because it is presented in a format tailored to facilitate rapid assimilation. Intelligence utility, however, involves more than simply getting the decision-maker to rapidly absorb situational factoids. Utility refers to how well the product provides contextual meaning and communicates implications. Intelligence utility, in the most perfect circumstances, will enhance, amplify and deepen a decision-maker's ability to recognize key patterns and anticipate results. Achieving this situational understanding enables a faster and less encumbered decision-making process.

OODA loop principles and concepts were instrumental in shaping the TEW approach to conducting intelligence operations. TEW founding members recognized that for counterterrorism efforts to be effective, friendly forces must be able to plan, decide, execute and assess at a faster pace than the adversary. Because counterterrorism operations are inherently focused on 1) uncovering indications of hostilities, and then 2) conducting operations to deny, deter or degrade the terrorist aims, intelligence must be able to rapidly scale operations, surging to support a high optempo when "the chase is on."



Note how orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

Competitive advantage comes from quickness over the entire "loop," not just or even primarily from the O-to-O-to-D-to-A sequence.

TEW designers also recognized that there was a high probability that the aftermath of a successful attack would require a massive response into highly complex, rapidly changing and dangerous situations involving multiple, possibly contaminated, mass casualty incident sites.

These basic observations dictated that the TEW operational framework be built around an intelligence production process that could rapidly turn within its own OODA loop and achieve its own high optempo capacity to recognize an emerging threat faster than the terrorist adversary is able to strike. Additionally, the TEW would need an intelligence process that was able to generate decision support products for responders that would enable the Unified Command to operate faster than a toxic hazard expands. The resulting operational framework included the development of a host of enhanced (high optempo) counterterrorism intelligence techniques embedded within a comprehensive Intelligence Preparation for Operations (IPO) process.

D. Intelligence Overview:

Within the context of TEW operations, intelligence involves acquiring knowledge of the operational space in addition to knowledge of the threat forces with designs on attacking it. Knowledge is generated in support of efforts focused on counterterrorism, incident response, and consequence management processes. It is the result of the collection, processing, exploitation, evaluation, integration, analysis/synthesis, and interpretation of available information about the operational space and the threat.

Uncertainty is a fundamental characteristic of conflict. Intelligence, however, aims to reduce uncertainty by providing accurate, timely, and relevant knowledge about the threat and the surrounding environment to unified commanders and emergency managers. Intelligence evaluates the variables making up the operational environment, determines the capabilities and intentions of threats, and develops estimates of threat courses of action that provide insight into possible future actions (utility).

Intelligence also identifies potential attack opportunities that come about when factors such as friendly vulnerabilities, social, economic or political instability, and resource shortfalls converge to form high risks scenarios. Finally, intelligence assists in the development of friendly courses of action by helping field response commanders and Emergency Operations Center personnel sort through the chaotic, complex and fluid threat environment.

Intelligence cannot provide absolute certainty: rather, intelligence attempts to reduce the uncertainty facing domestic decision makers to a reasonable level by collecting relevant information, placing it into context to provide knowledge, and conveying it in the most appropriate form to enhance understanding.

Intelligence operations can also be understood using the acronym WET, standing for weather, enemy and terrain. Intelligence activities in support of tactical military operations are often described using the term WET. The intelligence effort, while given specific direction through the priority intelligence requirement process, is consistently addressing, assessing, and deciphering the WET aspects of the conflict. Intelligence identifies the variables, and influences within each of the WET dimensions, methodically drilling down into each variable's component parts, cataloging their respective characteristics and then defining how each dimension's defining features will combine to influence operations. The WET concept is a valid way to describe the intelligence focus in the current counterterrorism conflict environment as well, and it may be helpful to return to this simple concept if overwhelmed by more difficult topics presented later.

Intelligence, then, is fundamentally a set of interrelated processes that are designed to capture, organize, analyze and decipher information extracted from the environment, thereby reducing uncertainty. The following section describes the primary arrangement of processes that accomplish this.

E. The Intelligence Cycle:

The intelligence cycle provides the doctrinally established order of intelligence functions. These functions transcend the specific requirements of any particular conflict and amount to a generic description of the primary approach to conducting intelligence operations regardless of the tactical, operational or strategic situation. The following is a listing of the general functional components of the basic intelligence cycle [Intel Cycle Diagram]:

1) The cycle begins with the formulation of *prioritized intelligence requirements* that dictate the intelligence focus, starting with the development of a collection strategy.

2) A *collection strategy* that in turn defines the incoming information stream.
3) An information stream that then feeds the data-to-information *processing* activities, resulting in raw intelligence.

4) Raw intelligence that is then developed through *analysis* into actionable knowledge or understanding, satisfying the original requirement of step one.

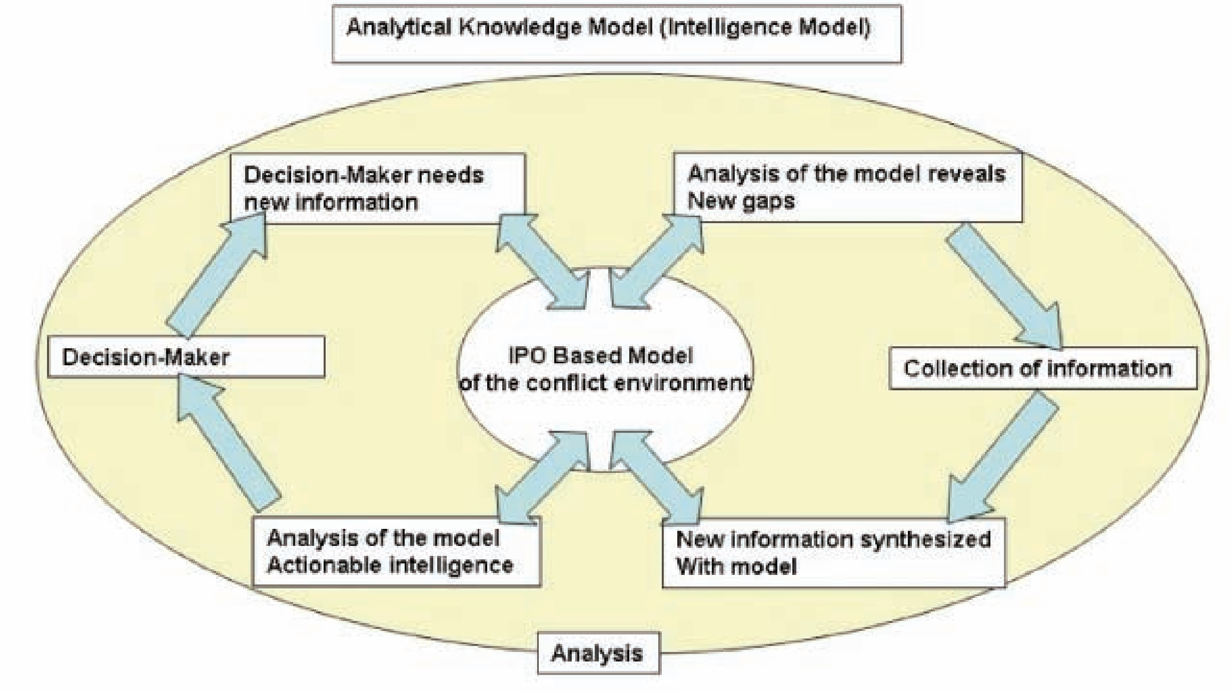
5) Intelligence requirements that are then packaged into appropriate formats and *disseminated* rapidly to the decision maker who needs the intelligence.

The intelligence cycle's functions are each underpinned by sub-processes. Each of these sub-processes are further defined by an array of specialized tasks, most being dependent on the utilization of multiple tools and technologies as well as intuition and imagination. These tools and tradecraft techniques are crafted and tailored by the needs of the users and vary across a range of different intelligence missions and conflict scenarios. For any intelligence organization, the use of analytical tools and methodical processes provide a means to establish task continuity, facilitates efficiency, reduces redundancies, and maximizes the effective use of intelligence resources.

The actual characteristics of an intelligence operation, therefore, can vary widely. The fundamental processes found in the intelligence cycle, however, once the sub-tasks and activities are cleared away, are relatively standard and represent a consistent enough introductory baseline.

The basic intelligence cycle, however, fails to describe a critical feature common to all intelligence operations. This particular feature underpins all intelligence cycle processes, providing the backbone across the entire intelligence enterprise. Without question, activities anchored to some form of analysis inherently drive each intelligence function, process, task and technique. For example, what information is collected, how it is pulled together, when it will have value, and where it is found are all questions considered through an analytical method. Similarly, how information is processed and organized is determined based on the needs of the actual 'analysis' process. Even the manner in which intelligence is ultimately conveyed requires a degree of analysis to determine an effective presentation approach suited to the material being presented, the time criticality of the intelligence, and the decision-maker's preferred means of consumption.

This 'ubiquitous' analysis factor suggests that the intelligence processes described in the intelligence cycle are constantly cycling around, and drawing on an analytical wellspring as a source of context and continuity. A more comprehensive description of how intelligence processes cycle and flow, therefore, includes the presence of an analytical knowledge model at the operational core of the intelligence activities.

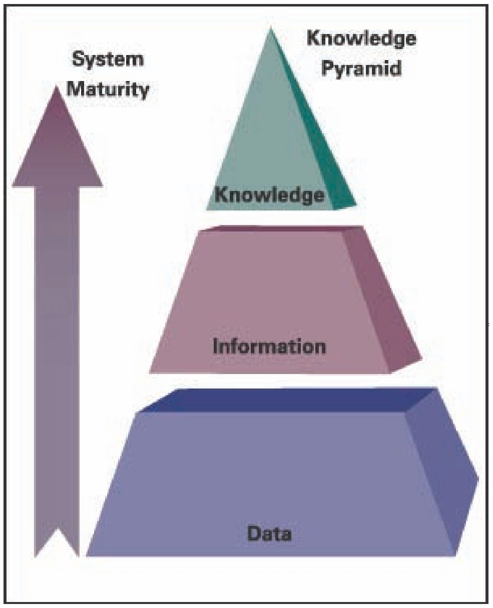

Analytical Knowledge Model (Intelligence Model)
Decision-Maker needs new information
Analysis of the model reveals New gaps
Decision-Maker
IPO Based Model of the conflict environment
Collection of information
Analysis of the model Actionable intelligence
New information synthesized With model
Analysis

The knowledge model—also referred to as the intelligence model within this CONOP—continuously evolves and matures as more is learned about the characteristics of the conflict environment's dynamics, notably the WET aspects. The model provides an analytical anchor point for framing every aspect of the intelligence effort within a collective context.

Intelligence processes are designed to work with, refine and develop information as the raw material needed to produce intelligence. The following section describes how information is defined as a commodity with requisite characteristics of a 'raw' material so that it can be mined and refined into intelligence products.

F. The Information Resource:

Information as a Resource - Information is one of the most precious resources available to any decision maker. By nature, humans are information processors who seek knowledge of the past, present, and prospects for the future. Without valid information, decision makers have no logical basis for choosing one course of action over another. Increasing information generally decreases uncertainty in decision-making, up to a point of diminishing returns, where too much information can confuse a situation.



Characteristics of Information - Information has many characteristics and does not come without cost. Acquiring sufficient, accurate, and timely information can be very expensive. It can be perishable and is generally imperfect. Consequently, information from one source should be verified with another source whenever possible. Frequently, information derived from one source can be used as a cue in researching other sources or in collecting additional or different information. Information can be acquired through various methods. Each has advantages, and all have inherent and environmental limitations and constraints. The observer, as a source of information, is often biased. Observers are also limited by what can be seen. Since it is difficult to observe an elaborate and dynamic system, the tendency is to "freeze" the situation and examine individual system parts in a static state. In doing so, essential ingredients are frequently lost. There is often the danger of attributing a great degree of precision to imperfect assessments or measurements. Because of these many limitations, information varies in validity and reliability.

Raw Information - Since information does not present itself for exploitation, it must be sought, gathered, assembled, and processed into usable form. The outcome is the transformation of raw information into intelligence suitable for making valid decisions. There are three levels of intelligence support: strategic, operational, and tactical. Strategic intelligence is required for the formulation of strategy, policy, and military plans and operations at national and theater levels. Operational intelligence is required for planning and conducting campaigns and major operations to accomplish objectives within theaters or areas of operations. Tactical intelligence is required for planning and conducting tactical operations. Intelligence sources are the means or systems used to observe, sense and record, or convey information.

G. Intelligence Information Sources - Collection:

Sources of Information - Information can take many forms and be derived from many sources. Information can result from observing or reporting an event. It can be derived from the manipulation of facts through computation. It can also result from professional opinions, judgments, and interpretations by participants. Information may be objective or subjective. For intelligence production purposes, information has been classified in accordance with both how it is sourced and the methods for extracting it from the environment.

As such, there are six basic intelligence sources, also called information collection disciplines:

1. Signals Intelligence (SIGINT)
2. Imagery Intelligence (IMINT)
3. Measurement and Signature Intelligence (MASINT)
4. Human-Source Intelligence (HUMINT)
5. Open-Source Intelligence (OSINT)
6. Geospatial Intelligence (GeoINT)

The TEW however, collects raw intelligence primarily through OSINT, HUMINT and GeoINT. Additionally, the TEW is exploring techniques for extracting raw intelligence from cyberspace (CyberINT). These approaches touch both SIGINT and OSINT domains.

All Source Intelligence - The culmination of the intelligence cycle is the development of all source intelligence. All source intelligence incorporates information derived through HUMINT, SIGINT, IMINT, MASINT, and OSINT. The intention of this type of effort is to develop reinforcing information and to use multiple sources to corroborate key data points. The advantage of an all source approach is that each of the intelligence disciplines is suited to collecting a particular type of data, which allows the intelligence organization to examine all facets of an intelligence target, and gain a better understanding of its operation.

Pulling all this information together, giving it order and extracting meaning, is the focus of intelligence analysis. The following section describes the fundamentals of conducting analysis.

H. Intelligence Analysis:

Basic Analytical Process - Intelligence analysis is a process used to methodically reduce uncertainty in a conflict and develop intelligence products needed by the intelligence consumer. Analysis inherently draws on and contributes to the intelligence model throughout each of the steps outlined below. Basic analysis includes the following principle steps:

1. Identifying known facts about the threat and the environment.

2. Identifying where there are key gaps in the current intelligence picture.

3. Evaluating historical data to spot environmental and threat factors of influence.

4. Identifying patterns and trends within these factors.

5. Comparing the picture of known facts (ground-truth) to the historical patterns and trends (the model) to develop assumptions to fill the key intelligence gaps.

6. Identifying the principle factors that, if they occur, would disprove each assumption. These are called *linchpin* factors.

7. Identifying the principle factors that combine to form the basis for each assumption. These are called *drivers*.

8. Reviewing the drivers and linchpins regularly to ensure assumptions remain valid.

9. Reviewing the intelligence picture, combining facts and assumptions, and developing threat Course of Action (COA) hypotheses following the same process used to develop the assumptions.

10. Identifying within each hypotheses, the indicators, or observable factors that collectively confirm or disprove each hypotheses (linchpins and drivers are included).

11. Assisting the collections manager develop a collection strategy that targets the indicators identified for the COA hypotheses

The analysis process is regularly cycled through with a frequency determined by the optempo. At any one moment in time, the intelligence analysis effort will have a ground-truth picture, a situational analysis concept (assumption combined to ground-truth), a set of threat COA hypotheses, and an information stream that delivers bits and pieces of situational content that must be regularly extracted and fused, vetted, validated, compiled, blended, correlated, prioritized, and added to the intelligence model. As the new picture develops, new facts are added, new gaps emerge, assumptions are made to fill the gaps, and this process continues in a cyclical fashion.

Because analysis is essentially a cognitive problem solving process, it is susceptible to numerous traps and pitfalls that result in analytical error. These pitfalls are caused by natural tendencies associated with human cognition that can be overcome through creative and imaginative analytical techniques. These pitfalls and principles for reducing their influence of the final intelligence product are addressed in the following section.

I. Analysis Pit Falls and Principles:

Group Think – When an idea-sharing environment is not fostered, an analytical pitfall may emerge involving each member of the group, thus conforming his or her opinions to what they believe to be the consensus of the group. This results in a situation in which the group ultimately agrees upon an outlook, assumption, or idea which individual members might individually consider incorrect. The group-think dynamic can take numerous forms, including Mind-Set and Mirror-Imaging.

Mind-Set – Another analytical pitfall, a mindset refers to a set of assumptions, methods or attitudes held by one or more people or groups of people which is so established that it creates a powerful incentive within these people or groups to continue to adopt or accept prior behaviors, choices or tools. This phenomenon of cognitive bias is also described as mental inertia, or a paradigm, and results in situations in which analysts only see what they are predisposed to see, missing evidence of alternative possibilities altogether.

Mirror Imaging – This analytical pitfall involves applying the behavior rules, logic and values generated out of one's own set of experiences and cultural socialization as a frame of reference for problem solving. This is a 'Mind-Set' related phenomena that results in narrowly construed assumptions, outlooks and ideas that fail to consider alternate possibilities because they seem too outrageous, illogical or nonsensical.

Methods to Manage Analytical Pitfalls

Deferred Judgment - The idea-generation phase of analysis is often separated from the idea-evaluation phase, with all judgments deferred until all possible ideas have been thought out.

Cross-Fertilization of Ideas – Ideas are combined to form more and even better ideas. As a general rule, if the appropriate environment is fostered for doing so, people generate more creative ideas when teamed up with others.

Competitive Analysis - This is the deliberate fostering of separate analysis centers (decentralization) so that, while each has full access to the same information, a comparison can be made between the alternate assessments.

Devil's Advocate - This is an analytical technique that involves using a team of analysts to play the role of devil's advocate and challenge the reasoning, logic and conclusions of an assessment, offering competitive viewpoints as appropriate.

Analysis of Competing Hypotheses (ACH) – ACH is a tool to aid judgment on important issues requiring careful weighing of alternative explanations or conclusions. It helps an analyst overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult to achieve.

ACH is an eight-step procedure grounded in basic insights from cognitive psychology, decision analysis, and the scientific method. It is a surprisingly effective, proven process that helps analysts to avoid common analytic pitfalls. Because of its thoroughness, it is particularly appropriate for controversial issues when analysts want to leave an audit trail to show what they considered and how they arrived at their judgment.

1. Brainstorm the possible hypotheses with other analysts. Consider the hypotheses you do not want to waste time on to simply be unproven hypotheses. Always consider the possibility that an opponent is trying to deceive you. Keep the number of hypotheses manageable; seven is a good number.

2. Make a list of significant evidence for and against each hypothesis. Include your own assumptions or logical inferences about another individual's or country's intentions, goals, and standard procedures. Note the absence as well as presence of evidence. Ask yourself the question: If this hypothesis is true, what should I expect to be seeing or not seeing? What you are not seeing may represent the need for greater data collection.

3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence by marking which items are most helpful in judging the relative likelihood of alternative hypotheses. Use your own marking system, pluses, minuses or whatever.

4. Delete evidence and arguments that have no diagnostic value. Save these items in a separate list as a record of information you considered. You are establishing an audit trail for your work. If others disagree with your assessment, they can be provided with this separate list.

5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove hypotheses rather than prove them. Look at the minuses in your matrix. Hypotheses with the most minuses are the ones you should start with. You should be spending more time than you thought you should on these least likely hypotheses. The one that is most likely is usually the one with the least evidence against it, not the one with the most evidence for it.

6. Analyze how sensitive your conclusion is to a few critical pieces of evidence. Consider the consequences for your analysis if that critical piece of evidence were wrong, misleading, or subject to a different interpretation. Put yourself in the shoes of a foreign deception planner to evaluate motive, opportunity, means, costs and benefits of deception as they might appear to the foreign country.

7. Report your conclusions by discussing the relative likelihood of all the alternative hypotheses. If you say that a certain hypothesis is the most likely one to be true, you are saying that there is anywhere from a 55 percent to 85 percent chance that future events will prove it correct. That leaves anywhere from 15 to 45 percent possibility that any decision made on your judgment will turn out to be a wrong decision. You should discuss these possibilities in your narrative report.

8. Identify things in your report that the policymaker should look for that would alter your appraisal of the situation. In other words, specify in advance what it would take for you to change your mind.

ACH, in addition to the other analytical techniques described in this section, are employed within the TEW as required by the situation. The TEW Analysis and Synthesis (A/S) Cell is the central integrating hub of the TEW organization. This cell tasks out requests for information to all other functional cells, then collects and integrates their individual products into a cohesive assessment. This includes capturing investigative information, intelligence from all sources (criminal, classified sources, open source/OSINT, cyberINT, imagery, reconnaissance, databases, etc.) and analyzing and synthesizing it. The A/S cell also synchronizes information from the Investigative Liaison (INV-LNO) cell, Consequence Management (CM), Epidemiological Intelligence (Epi-Intel), and Forensic Intelligence Support (FIS) cells into a usable product for decision-makers.

Combined, the analysis process that has evolved within the TEW is called the Transaction Analysis Cycle, a topic that will be addressed in greater detail in subsequent sections. The following section describes information fusion, an integral sub-process within intelligence analysis.

J. All-Source/All-Phase Fusion:

Information fusion or data fusion - Fusion is a merging of diverse, distinct or separate elements into a unified whole (Merriam-Webster dictionary). It is the process of acquisition, filtering, correlation and integration of relevant information from various sources, like sensors, databases, knowledge bases and humans, into one representational format that is appropriate for deriving decisions.

The fusion of redundant information from different sources can reduce overall uncertainty and thus increase the accuracy of the analysis. Multiple sources providing redundant information can also increase the robustness of the system.

The concept of fusion has emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence. The fusion process supports the implementation of all-source-all-phase, risk-based, information-driven prevention, response, and consequence management programs. At the same time, it supports efforts to address immediate and/or emerging threat-related circumstances and events. Data fusion integrates data from different sources, including law enforcement, public safety, and the private sector, resulting in meaningful and actionable intelligence and information. The fusion process also allows for turning information and intelligence into actionable knowledge.

Additionally, because the OPFOR strives to misinform (deceive) or deny information to intelligence gathering agencies, intelligence based solely on single source data is more susceptible to deception. Intelligence becomes more useful and more reliable when information from all possible sources is collected, combined, evaluated and analyzed in a timely manner.

Application of Fusion – Information fusion is not always possible, but the principle should be used whenever possible to enhance intelligence support without degrading the timeliness of that support. There are times when information from one source cannot be confirmed by others or is highly perishable. Factual and important single source information should be disseminated immediately if actionable. Follow-up data should be presented when it becomes available.

K. Intelligence Production:

Hierarchy of Intelligence Products – Information fusion and intelligence production can also be viewed through a hierarchy of products. There are five categories in intelligence production, each one being a building block. They are: raw or unevaluated data, processed data, analyzed basic data reports, integrated intelligence, and intelligence end products. Through information fusion, improved products are built from those lower in the hierarchy.

Raw or Unevaluated Data - This is the basic building block from which all intelligence products are derived. It includes all unexploited reports or 'leads' received by the TEW.

Processed Data - The second level in the hierarchy is made up of materials that have been refined to a stage where they can be analyzed. This can include Open Source (OSINT) materials, SALUTE reports, or reports from other TEWs. This data is provided through TLO, ILO, INV-LNO, or community channels.

Raw Intelligence
is information that is collected from a single source and quickly evaluated. Reports may be produced from this intelligence and delivered to consumers if the information is time sensitive.

Finished Intelligence
is more fully analyzed and evaluated information. It is usually based upon raw intelligence collected from many (or all) sources and analyzed in this context.

Analyzed Basic Data Reports - Basic data reports are used to form a database and result from a collation process oriented toward improving the intelligence model. Reports classified as 'information-only' are compared and collated (synthesized) within the intelligence model, improving the aggregate knowledge-base without offering any inherent immediate forecasting value.

Integrated Intelligence - These products result from detailed analysis and fusion of multiple intelligence sources. Examples include orders of battle, scientific and technical reports of complex threat vectors, reports relating to developments of OPFOR capabilities and intentions, and reports pertaining to situational developments. Integrated intelligence products are, in turn, used to produce other intelligence products.

Intelligence Products - This category includes materials intended for dissemination to users. End products result from additional analysis, evaluation, and fusion of materials produced at lower levels in the hierarchy. This finished intelligence includes products developed during threat early warning and operational net-assessment.

L. Criminal v. Operational Intelligence:

Criminal Intelligence and Crime analysis - Traditional law enforcement intelligence operations involve the collection of criminal intelligence based on legal protocols and guidelines that establish the appropriate set of conditions—reasonable suspicion of a criminal act—under which the information on a suspect can be collected and developed. The intent is to develop the appropriate evidence to ensure a suspected criminal is convicted. Crime analysis, a separate but related discipline, conducts tactical, operational and strategic analysis using multiple sources of data to identify crime trends or patterns of criminal activity that are used by law enforcement to develop appropriate crime deterrence and interdiction plans. At the tactical level, the crime analyst uses crime scene data to identify connections with similar events that could point to serial criminal behavior or identify patterns in the activity that law enforcement could use to develop investigative leads and eventually arrest suspected perpetrators. Operational and strategic analysis, however, look for environmental conditions in combination with crime data to identify hot-spots and isolate possible contributing factors. These studies are then used to develop community oriented crime reduction plans.

Operational Intelligence - The TEW integrates local, state and Federal echelons toward information fusion and dissemination. The TEW processes not only criminal intelligence, but also operational intelligence. Operational intelligence is the processed information needed to understand the current and future situation, including the capabilities and intentions of an adversary in order to conduct operational missions at all phases of response. The TEW bridges criminal and operational intelligence, hence the term "all-source/all-phase fusion" is used to describe TEW operations. The TEW also serves as the bridge between crisis and consequence management intelligence, providing products to law enforcement, the fire service, and medical and public health communities. Operational intelligence products include advisories, alerts, warnings, issue-specific white papers and mission folders. Mission folders integrate threat specific playbooks, venue specific target folders, intelligence information, resource information, archival information on technical dimensions of threat agents, resource status, and potential courses of action for incident mitigation and response.

M. Situational Awareness and Understanding:

As addressed earlier, the fundamental role of intelligence in any conflict environment is to reduce the degree of uncertainty. Establishing, maintaining, sharing and constantly improving situational awareness achieves this. Establishing situational awareness requires the intelligence operation to routinely track the most dynamic and influential variables within the conflict environment in order to provide an accurate description of "what is" at any moment in time. Further, intelligence operations seek to identify predictable patterns in environmental variables – situational understanding – in order to provide assessments that reach beyond simply describing "what is," but also identifying potential outcomes, or "what will be."

TEW processes and procedures have been designed with the recognition that success in either the I&W or Operational Net Assessment (ONA) functions is highly dependent on effective situational awareness which, in turn, is dependent on the quality and diversity of available information (collection). TEW processes, primarily utilizing the IPO process, have become effective in developing situational awareness by exploiting key high-value and high-payoff reporting resources and information channels.

For example, the TEW (either actual staff or by employing a "virtual" capability) monitors key public gatherings, the status of emergency services, and the status of all critical infrastructural components. The impact of actual attacks both within and without the Operational Area is regularly assessed in order to gauge resource needs and shortfalls and to support the development and assessment of potential courses of action (COAs) for incident resolution.

Additionally, the TEW emphasizes a multi-agency, multi-disciplined approach, drawing from a diverse resource pool, including law enforcement, fire, health and emergency management agencies to address the intelligence needs for counterterrorism and critical infrastructure protection. The TEW integrates local-federal echelons and operates pre, trans, and post-incident. It relies upon criminal leads, investigative information and open sources to detect potential indicators of terrorist threat. It utilizes all available sources to scan/monitor, indicators of imminent attack, as well as trends and potentials that influence training and doctrinal needs. Additionally, during an actual threat period of attack, the TEW provides consequence projection (forecasting) to identify potential courses of action to the unified command structure.

Section 2.2 –
TEW Intelligence Functions

A. Indications and Warning (I&W):

I&W is an intelligence activity that uses hindsight in order to gain foresight. The fundamental aspects of I&W is based on the same rationale used routinely by people faced with a decision that involves a predictive assessment. For example, stock brokers when deciding on a stock purchase, credit companies when considering a loan application, and employers when reviewing a resume are all reviewing past performance in order to anticipate the future. In each case, the decision is predicated on a set of standard metrics or *indicators* the decision-maker has developed to help interpret past performance. The performance history, on the other hand, is a record of facts that provide *indications of* possible future activity. I&W intelligence similarly involves 1) the development of *indicators*—what to look for within the conflict environment—and 2) the analysis of current intelligence to identify the presence of *indications*—what has actually occurred.

As such, I&W is essentially a prediction oriented intelligence function. The I&W process involves a comprehensive analysis of the conflict environment and the host of variables that define it, primarily the threat actors, local target profiles, and the state of global-to-local social conditions. The analysis seeks to identify the dynamic influences these variables exert on each other by scrutinizing how their component factors have lined up in previous attacks. The analysis methodically evaluates the characteristics that define each variable, noting influences, impulses, attractions and repulsions, and any other relationship possibilities that stand out as recognizable trends and patterns that can be used as indicators for predictive assessments during I&W.

B. I&W Intelligence Background:

"Warning-intelligence" evolved out of the experiences of World War II where intelligence services were continually called upon to analyze enemy doctrine, known force dispositions, and captured planning documents in order to produce assessments of enemy intentions and anticipate future enemy actions. The warning-intelligence techniques developed during WWII became even more critical in the post-war era to fill the strategic need for anticipating hostile intentions in an environment characterized by superpower military showdowns. During this Cold War period, strategic warning-intelligence was refined and formalized, becoming a distinct intelligence discipline called Indications and Warning (I&W) Intelligence. The tradecraft of I&W Intelligence soon became a core competency throughout the Intelligence Community (IC) at the strategic, operational and tactical levels.

The nature of the current threat environment, however, has challenged the traditional I&W approaches. The ability to anticipate hostilities in the latter half of the 21st century relied on observing key political, economic or military actives that were known to be associated with hostile intentions. At the strategic level, a large-scale deployment of conventional military forces to a border area could indicate intentions to invade a neighboring country. At the operational level, the location of key armor units and the positioning of heavy artillery would indicate the most likely main attack axis. At the tactical level, the unit formations indicate the intended course of action that unit has adopted for an engagement. Additionally, the effort to identify key indicators within the traditional approach could rely on a vast archive of intelligence detailing foreign military doctrine and capabilities.

The current threat environment, however, involves a dramatically different set of operational conditions, and there is no intelligence archive or doctrinal publications to draw upon to guide the development of indicators. Furthermore, anticipating the threat of terrorist attacks inherently involves the application of intelligence capabilities deeper and broader than ever before in the nation's history, covering the local, domestic landscape and extending out across the entire globe.

A terrorist's attack, for example, involves a chain of activities involving actors from across the globe that ultimately result in an attack on a local jurisdiction. The lines between strategic, operational and tactical levels of conflict have been significantly blurred, as have the lines between domestic criminal activities and global warfare. Consequently, a successful national intelligence effort requires the participation of non-traditional participants, including domestic intelligence organizations like the TEW, that are capable of conducting counterterrorism-based I&W Intelligence activities focused on anticipating threats to local and regional targets.

The TEW approach for conducting I&W generates indicators that serve as threat triggers applicable to the following general conditions:

- ❑ Environmental risk factors and threat group capabilities and intentions are aligned or moving in that direction – indicating a threat *opportunity* has emerged or may soon emerge *(Attack-lane I&W)*.

- ❑ Threat group activities appear to be consistent with one or more elements of an attack effort (planning, resource mobilization, recruiting, etc.) – indicating an attack may be coming together *(Kill-Chain I&W)*.

- ❑ Threat group activities that suggest a growing interest in or direct efforts to acquire the materials, facilities, equipment or expertise associated with a WMD – indicating an attempt to acquire, design or develop a WMD *(WMD- Threat Vector I&W)*.

- ❑ Activities, mannerisms, appearances and identifiable signatures of people, equipment or weapons that public safety official at a potential target site can look for to detect a possible imminent attack *(Last chance I&W)*.

C. Attack-lane I&W:

Terrorist attacks are not random acts of violence. They are highly planned and deliberately conducted at the time and place that offers the greatest potential for achieving maximum impact. This attack philosophy is, in a sense, like using a small caliber bullet to detonate a nuclear bomb. Similarly, a terrorist attack is intended to be a catalyst that exploits existing circumstances that are already highly combustible and only need a spark to be ignited. Achieving this kind of amplified effect requires a precise alignment of factors, including:

- ❑ The terrorist group factors—capabilities, intentions and resources,
- ❑ The target factors–criticality and vulnerability,
- ❑ The weapon factors—lethal impact and effect, and
- ❑ The timing factors—social, political and economic climate appropriately volatile.

Because of this consideration, one aspect of the I&W strategy is aimed at recognizing indications that these threat combinations are aligning to form a threat axis. It provides a warning trigger that an attack opportunity is emerging. This condition is particularly significant if the alignment is occurring within an attack-lane. All threat elements and known terrorist groups' targeting profiles are used to identify potential targets in the operational space. When these relationships are identified, an *attack-lane* is considered to exist between the terrorist and the target. The emergence of an opportunity—alignment of factors—within an attack-lane would likely trigger an in-depth assessment and possibly a red-team analysis of potential threat courses of action (COAs).

A significant and often overlooked component to this aspect of I&W is the cultural landscape. This involves observing how the social, political and economic forces are interacting globally and tracking how each is influencing the communities locally. These forces drive the *event-emotion* dynamic in which an event occurring either globally or locally, that may be routine or spontaneous, will foster distinctive and predictable attitudes and emotions within specific communities, setting conditions that could be the precursors to the kind of circumstances a terrorist attack could exploit. For example, global events impact gas prices. Rising costs at the pump create growing agitation locally. Local agitation impacts the national political system. Factors have combined to create conditions that increase the criticality of the domestic oil refinery infrastructure systems and elevate its value as a potential target. As this situation escalates, an opportunity window opens along an attack-lane for those terrorist groups with known capabilities and intentions to attack oil refinery targets.

D. Kill Chain I&W:

Finding a threat group's patterns involves an examination of the groups' past attacks. The effort to do this requires assessing their demonstrated capabilities, stated objectives, methods for exploiting environmental conditions during tactical execution of attacks, and all associated activities in order to find recognizable threads of continuity that would be useful for understanding their specific criteria for target selection, weapon selection and attack timing.

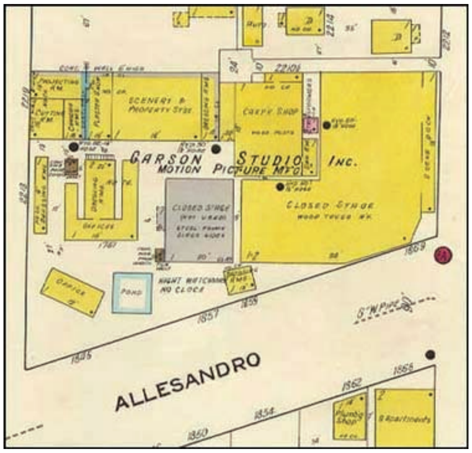
In addition to assessing how threat groups exploit environmental conditions, the examination of past attacks is useful in developing a template or model describing the arrangement, sequencing and coordination of a group's activities. This model is described as the threat group's *kill-chain* and becomes a key contextual frame of reference for evaluating their various activities.

E. WMD-Threat Vector I&W:

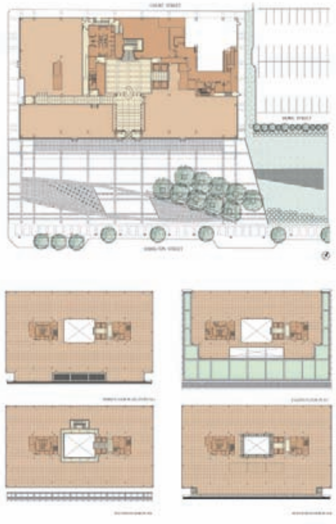
Additionally, the process defines indicators related to attempts to pull together the capabilities, resources or expertise necessary to design, develop and/or deliver a WMD. While the responsibility for tracking this issue falls on national intelligence agencies, state and local agencies should also be vigilant to recognizing these critical indicators. A comprehensive I&W routine, regardless of the level of government the effort takes place at, seeks to develop a complete picture of the threat's capabilities and intentions. The emergence of trends suggesting a threat group is attempting to acquire WMD represents a significant part of the larger threat picture and is a critical component of local intelligence center's situational awareness.

F. Operational Net Assessment Overview:

In the event of an attack, the TEW transitions to providing incident specific intelligence to both the Unified Command Structure (UCS) and the County EOC. Under these conditions the TEW develops multiple intelligence products to assist the effort to mitigate the event. In circumstances where the intelligence developed in the TEW is time critical and extraordinarily perishable, output could include products such as advisories, alerts and warnings. Under circumstances where there is more time to develop, refine and finish the intelligence output, the TEW produces intelligence summaries and intelligence reports. The primary intelligence product developed during an actual event, however, is the *Operational Net Assessment* (ONA) and the Mission Folder.



The *ONA* provides the UCS and emergency managers in the EOC with situational intelligence, threat course of action forecasts, hazard consequence forecasts, resource availability/requirement profiles and outlines Random Antiterrorism Measures (RAMs). The ONA process is focused on describing the scope, magnitude and potential impact of an event and is a critical resource for *consequence mitigation*. Feeding off critical site information drawn from the site's RIF, ONA provides a description of the current threat envelope and becomes a decision support resource for both emergency responders and emergency managers.



The ***Mission Folder*** is also incident-specific, combining pre-event intelligence preparation (playbooks and RIFs) with time sensitive threat information, providing the UCS with a set of friendly force *Course of Action* (COA) recommendations. Additionally, Mission Folders provide situation and resource status, scene/location information, and general reference information useful for decision-making.

Section 2.3 –
Assessing the Conflict Environment

A. Environmental Factors:

Terrain and Weather - The terrain analysis is best accomplished using aerial imagery that is electronically or manually marked up to highlight the analytical findings. The tactical terrain studies include, but are not limited to, identifying lines of communication, key terrain, cover, concealment, obstacles, and response infrastructure. The weather effects are then identified, primarily noting seasonal patterns and their influences on the jurisdiction.

Tactical Aspects of Terrain and Weather Study - The approach includes a tactical terrain analysis that provides information that could compliment the RIF in the event there was a crisis at one of the NAI. The study is best accomplished using imagery of the area, electronically or manually marked up to highlight the analytical findings. The tactical terrain study includes, but is not limited to, identifying the following aspects of the terrain:

Lines of communication:

- □ Roads and highways
- □ Inter-structural access and egress
- □ Infiltration avenues –alleys and subterranean passages
- □ Radio dead-space

Key terrain:

- □ Areas where tactical operations will provide decisive advantage
- □ Cascading access control points (choke points) and associated control sectors
- □ Primary observation points and fields of fire

Cover, Concealment Obstacles:

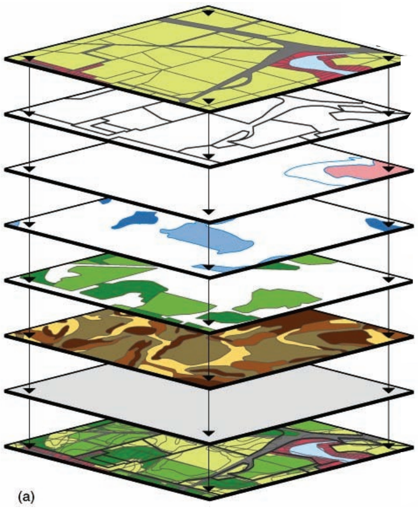
- □ Structures, buildings, industrial apparatus

Response infrastructure:

- □ Fire stations
- □ Police or Sheriff stations
- □ Helicopter Landing Zone (HLZ) study
- □ Casualty collection points
- □ Evacuation areas
- □ Decontamination sites

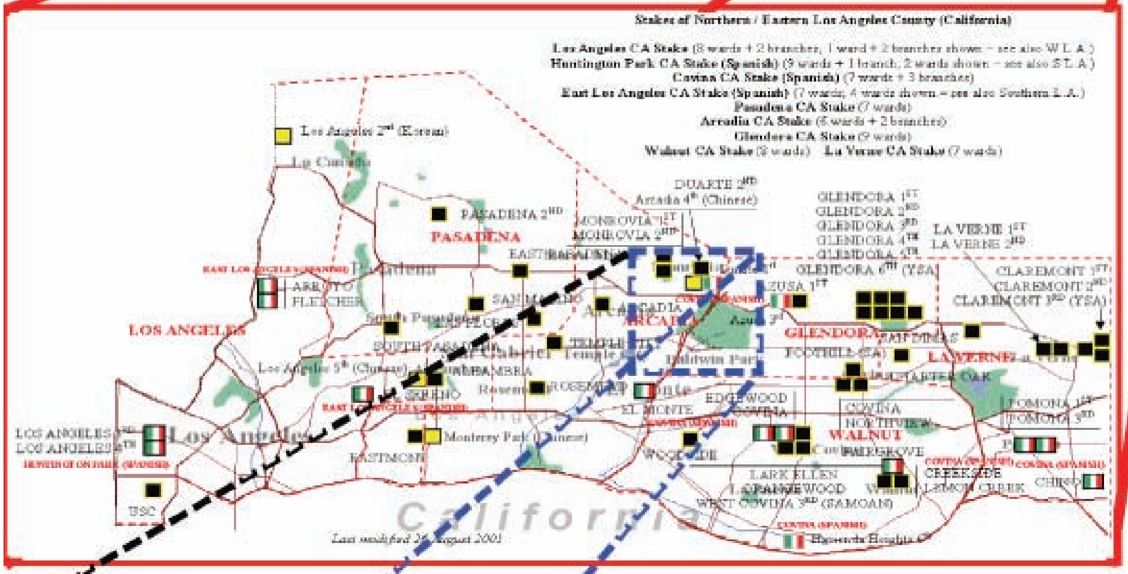
Weather:

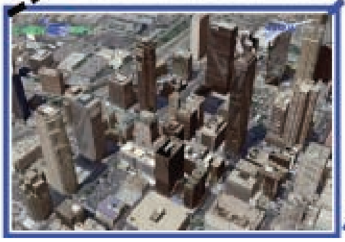
- □ Climate patterns
- □ Winds
- □ Hazard zones –fire, flooding and slides



The resulting Tactical Aspects of Terrain and Weather product include annotated maps and an assessment of the opportunities and limitations for both friendly forces and threat group activities.

LOS ANGELES
SAN GABRIEL MOUNTAINS
Hansen
San Fernando Valley
Sepulveda
Santa Fe
LOS ANGELES
Whittier Narrows
Brea
Fullerton
SAN BERI
LACDA Basin
Location of COE Reservoirs
US Army Corps of Engineers
Los Angeles District
Long Beach
Point Fermin
SANTA ANA
ORANGE


Stakes of Northern / Eastern Los Angeles County (California)
Los Angeles CA Stake (8 wards + 2 branches; 1 ward + 2 branches shown – see also W.L.A.)
Huntington Park CA Stake (Spanish) (9 wards + 1 branch; 2 wards shown – see also S.L.A.)
Covina CA Stake (Spanish) (7 wards + 3 branches)
East Los Angeles CA Stake (Spanish) (7 wards; 4 wards shown – see also Southern L.A.)
Pasadena CA Stake (7 wards)
Arcadia CA Stake (6 wards + 2 branches)
Glendora CA Stake (9 wards)
Walnut CA Stake (8 wards) La Verne CA Stake (7 wards)
Los Angeles 2nd (Korean)
PASADENA 2ND
PASADENA
DUARTE 2ND
Arcadia 4th (Chinese)
MONROVIA 1ST
MONROVIA 2ND
GLENDORA 1ST
GLENDORA 2ND
GLENDORA 3RD
GLENDORA 4TH
GLENDORA 5TH
GLENDORA 6TH (YSA)
LA VERNE 1ST
LA VERNE 2ND
CLAREMONT 1ST
CLAREMONT 2ND
CLAREMONT 3RD (YSA)
LOS ANGELES
ARROYO
FLETCHER
AZUSA 1ST
ARCADIA
GLENDORA
LA VERNE
SAN DIMAS
FOOTHILL (SA)
Los Angeles 5th (Chinese)
ALHAMBRA
ROSEMEAD
EL MONTE
EDGEWOOD
COVINA
NORTHVIEW
WALNUT
FAIRGROVE
POMONA 1ST
POMONA 3RD
LOS ANGELES 3RD
LOS ANGELES 4TH
Monterey Park (Chinese)
EASTMONT
WOODSIDE
LARK ELLEN
ORANGEWOOD
WEST COVINA 3RD (SAMOAN)
CREEKSIDE
LEMON CREEK
CHINO
USC
California
Last modified 26 August 2001



Geosocial Factors - The next environmental factor to be assessed is the geosocial aspects of the environment. This includes identifying the demographic and cultural characteristics of the operational space. The demographics and cultural analysis includes pulling together recent demographic studies through local census bureaus, community policing programs or other appropriate government agencies in order to identify and understand the most critical and fluid aspect of the environment—the people.

The end-state for demographics and cultural studies is to produce an assessment of the diverse world views and cultural pre-dispositions that exist across the jurisdiction. This "snap-shot" study includes population numbers, age distribution, income groups, socio-economic factors, cultural data, and crime data.

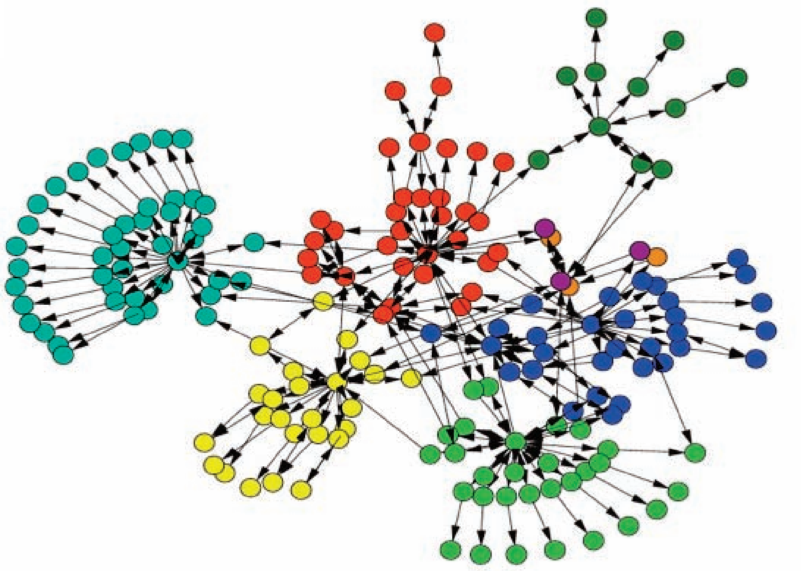
Another aspect of the geosocial situation is the *Significant Events Calendar* that identifies important dates, celebrations and memorials that are important to each community. Special events are identified on the calendar, including visits from government officials, foreign dignitaries and other high visibility personalities.

The calendar also includes significant dates that may have attached symbolism considered to be provocative to certain sectors. Finally, the significant events calendar includes all aspects of the environment that follow a regular schedule, such as the annual flu season.

Global ↔Local Connections - Environmental conditions that seemingly would only impact remote corners of the globe can instantly become a driving and influencing element of local conditions as the issues facing foreign communities become manifest in the attitudes and dispositions of a jurisdiction's foreign-national communities.

The jurisdictional demographics study is used to identify sectors of foreign nationals. Countries of origin are noted for each of these sectors, and wedge issues in those countries are evaluated. The evaluation provides a tool for identifying communities where sympathies, grievances, or alliances with roots in the home country are still getting played out.

The global↔ local influence assessment continues across as many sectors and sub-sectors as possible, including economic, religious, political and social sectors in order to get a reasonable read on global influences affecting the jurisdiction.



The complexities of the conflict environment also include those inherent to the urban landscape. Russell W. Glenn, a RAND analyst specializing in urban operations, has explored the challenges imposed by the multi-dimensional urban battlespace of the future. As Glenn observes, the urban environment is characterized by density—a density of people and terrain features. Urban terrain, with its subterranean, surface and building or rooftop features poses a challenge to military commanders and their operational and intelligence staff, not to mention the forces on the ground.

Structures of a variety of types, including many of them vertical (i.e., high-rises), converge with roadways, boulevards and alleys above ground to create multiple avenues of approach, firing positions and obstacles. Underground subways, tunnels, sewers and basements form another dimension. These features (picture a makeshift shantytown of cardboard boxes, packing crates and scrap metal poised on top of high-rise office towers or housing projects) diminish lines of sight and inhibit standard sensors and communication capabilities.

Density of people accompanies terrain (after all, terrain is adapted to meet the needs of the populace). Thousands, up to tens of hundreds of thousands, of inhabitants per square kilometer (or in Glenn's view 'cubic kilometer') occupy urban space, obscuring the opposing force (OPFOR), non-combatants and friendly forces alike. Complexity is often the only predictable result.

Section 2.4 –
Target Management Activities

A. Target Management Overview:

Target management includes activities such as critical infrastructure assessments, target identification, impact and resource assessments, vulnerability analysis and target hardening. The primary intelligence product developed during this task is the Response Information Folder (RIF).

B. Critical Infrastructure:

The critical infrastructure assessment process identifies the infrastructure which, if attacked, could produce the most severe consequences. Critical infrastructure includes sites, facilities, systems or system components, or special events that, if it were attacked, would result in:

- ❑ A large number of deaths or injuries – mass gathering events and venues, or
- ❑ Extensive damage to life-sustaining services – Critical Node Targets.

C. Target Inventory:

Critical infrastructure is not, in and of itself, a site that can be targeted. Critical infrastructure relies on a number of highly dependent inter-modal system components that are not usually centrally located in a single site, but may be spread across jurisdictions, across the nation and even across the globe. Identifying specific target sites within a critical infrastructure system is achieved through target system analysis and critical node analysis.

Other potentials target sets are identified as well, including mass-gathering events and sites with symbolic value to the OPFOR.

D. System Analysis:

The target system analysis identifies the critical infrastructure's underlying system. The analysis describes the functions, processes and dependencies of each respective system's components, nodes, and facilities and sets the stage for the *critical node analysis*.

E. Critical Node Analysis:

Nodal analysis assigns numerical scores to a system's components based on each part's functional significance and importance to other components in terms of dependencies. The effort identifies the backbone components – critical nodes – without which the system cannot function. Each system's critical nodes, when associated with a physical site, are identified as a high-value target (HVT).

F. Mass Gathering Events:

Special, high-visibility, high-participation events, regularly scheduled or not, require the least analysis to identify. The broad steps involved here include 1) identifying the venues, 2) reviewing each venue's calendar of scheduled events, and 3) determining what specific targets within the venue would cause the greatest loss of life. The potential target sites within these venues are identified as high value targets (HVT).

G. OPFOR Targets of Interest:

The final set of potential targets includes sites with symbolic significance attractive to an OPFOR. Sites, events, significant dates and personalities that have symbolic value are identified and designated as High-Payoff Targets (HPT).

H. Consequence Assessment:

The consequence assessment activity–also identified *as target forecasting*—combines threat and target factors within the context of an attack scenario. Targets are assessed during risk-assessment to determine potential consequences of a threat or terrorist attack. The assessment determines the impact of an attack in terms of localized deaths and injuries, characterizes the scope and magnitude of a required response, and evaluates the target's criticality to the jurisdiction.

During an actual threat period or attack, the TEW provides consequence projection (forecasting) to identify potential courses of action to the Unified Command Structure. No single local governmental agency has the capability or requisite authority to respond independently and mitigate the consequences of such a threat. The incident may affect a single location or multiple locations, each of which may be a disaster scene, a hazardous scene and/or a crime scene, simultaneously.

The complexity, scope, and potential consequences of a terrorist threat or incident require that there be a rapid and decisive capability to resolve the situation. The resolution to an act of terrorism demands an extraordinary level of coordination of crisis and consequence management functions and technical expertise across all levels of government.

I. Vulnerability Analysis:

During the analysis, a combination of factors is evaluated to determine a site's relative vulnerability, including the site's value to the jurisdiction, its physical characteristics, and its influence on the jurisdiction's moral state.

Physical Vulnerabilities -Aspects of the site and the surrounding environment are evaluated from a physical security perspective. This includes a review and evaluation of factors that define existing security assets, measures and procedures. These factors include the following broad categories:

- ❑ Impact profile and site criticality – loss of life, property and services.
- ❑ Physical characteristics – location, ingress, egress, structures and on-site hazards.
- ❑ Security and Safety Systems – systems that deter, detect, delay, deny and initiate response.

Physical Factors-

- ❑ Site criticality internally and externally
- ❑ Site visibility
- ❑ Access
- ❑ Hazards on-site
- ❑ Population on-site
- ❑ Potential collateral damage
- ❑ Availability of alternative services
- ❑ Security systems

Moral Vulnerabilities - Beyond the measurable impact on life and property, the vulnerability analysis also considers the intangible, but also inevitable, injury to morale, prestige or confidence that could ensue in the aftermath of a successful attack.

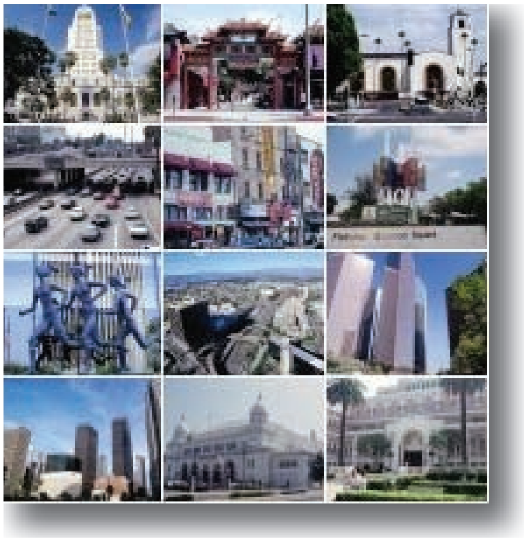
Terrorists endeavor to weaken the resolve of their adversary's people by targeting and attacking assets that are critical to them. Successful attacks further their goals of disrupting the economy, causing large-scale injury and destruction, and damaging national morale, prestige, and confidence. Disrupting or destroying critical infrastructures and key assets would move these goals forward.

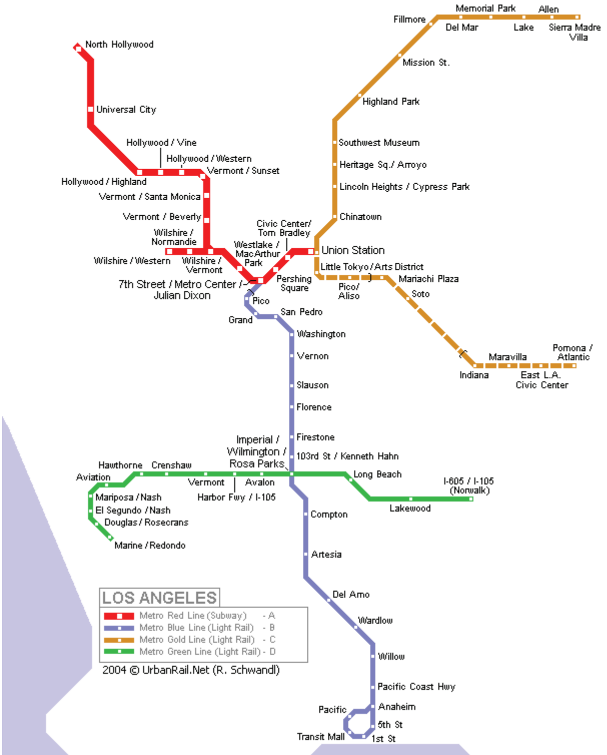
For example, for a period of time after the 9/11 attacks, the public disengaged from activities related to the economy. Such disengagement can be as damaging, if not more detrimental, to the overall health of the country than the immediate physical destruction caused by the attack itself.

This type of tactic relies on economic, social or political conditions of instability, friction or crisis to either exist or be emerging in order to exploit, aggravate or magnify the condition by generating terror, chaos, uncertainty, mistrust, anxiety and alienation. The measure of a successful attack is not exclusively the number of dead and the size of the rubble pile. While these elements are important, the key measure of success is the roar of the crowd after the fact.

Moral Factors-

- ❑ Economic impact of loss
- ❑ Political Impact of loss
- ❑ Social impact of loss
- ❑ Symbolic and propaganda value



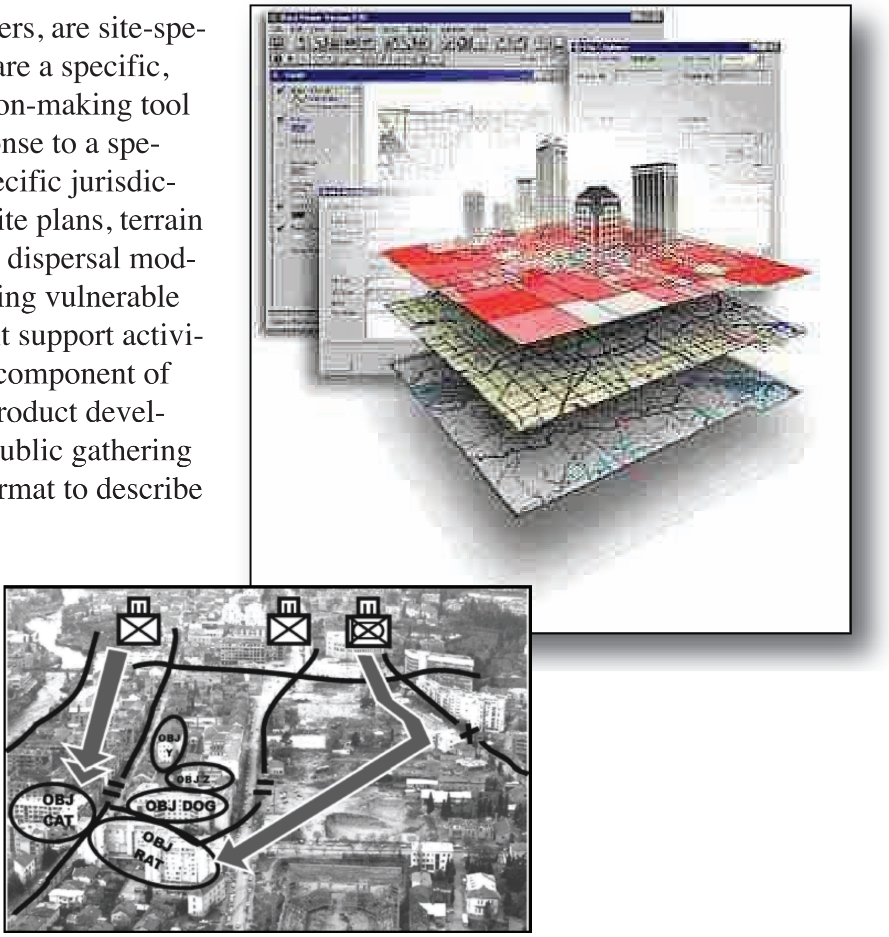


J. Target Hardening:

Target Hardening involves any measures taken to fortify the physical environment of a location or facility so as to deter or mitigate the effects of a criminal or terrorist act against it. It also refers to changing procedures, computer codes, power, and communications links to make it harder to attack. Random Anti-terrorism Measures (RAMS), developed as part of the Operational Net Assessment, are also examples of target hardening.

K. Response Information Folders (RIF):

RIFs, also referred to as Target Folders, are site-specific terrain awareness tools. They are a specific, comprehensive reference and decision-making tool to guide integrated emergency response to a specific, high-profile target within a specific jurisdiction. A target folder could include site plans, terrain analysis, interior and exterior plume dispersal models, and blast analysis. Maps indicating vulnerable points and potential sites for incident support activities could be included. These are a component of geospatial intelligence (GEOINT) product developed for critical infrastructure and public gathering spaces, and utilize a standardized format to describe the characteristics of a venue.



Section 2.5 –
Threat Management Activities

A. Threat Management Overview:

Threat management is made up of four activities: 1) Threat Inventory, 2) Threat Modeling, 3) Threat Integration, and 4) Threat Forecasting. These activities and associated sub-tier activities emphasize identifying complex threat vectors such as CBRNE WMD as well as local threat elements, determining their potential for interacting with global threat actors—such as al-Qaeda cadre—in the execution of an attack on local targets, and further, they emphasize assessing local threat element activities within the context of a globally active kill-chain.

B. Threat Inventory:

The TEW *threat inventory* identifies 1) threat actors and potential threat elements (PTE) within the local area, and 2) complex threat vectors.

Threat Elements Identified - The PTE inventory process endeavors to identify groups or individuals within the jurisdiction whose association with radical, hate and violence-oriented extremists, domestic or otherwise, is known, suspected or considered to be likely in the future. An active threat inventory program, coupled with a *transaction-based* I&W analysis process, is necessary to reduce the likelihood that a previously unknown element will emerge to carry out, or support in any capacity, local attacks.

A sophisticated threat inventory results in a PTE social network map; this map indicates jurisdictional, regional and global connections and transactions between possible threat actors. Within the current threat environment, it is critical that the intelligence effort continue to pursue a better understanding of the global-local-global relationships between threat actors. These relationships provide the OPFOR, among other things, global reach, and the mobilization and participation of supporters, drawn from a wellspring of enthusiastic sympathizers who are already firmly embedded within the local landscape. The analysis of information generated from within the jurisdiction (tactical information), therefore, is always assessed within the context of possible relationships to local PTE activities. Similarly, information related to local PTE activities is also assessed within the context of possible relationships to global developments.

This is particularly important in light of developing trends that indicate the emergence of a collective OPFOR consolidating under the al-Qaeda (AQ) banner and ideology. Disparate terrorist groups, criminal elements and individual sympathizers have united within the context of AQ's fight, particularly the fight against the west, and are actively sharing resources and capabilities.

The threat inventory, therefore, is a process that identifies the local PTE and determining potential local, regional and global relationships and potential connections to the larger OPFOR network.

Complex Threat Vectors Identified - The TEW recognizes that there are classes of threats and terrorist attacks involving highly complex, dynamic and technical characteristics that may or may not also involve rapidly expanding and highly catastrophic consequences.

The threat inventory, therefore, also identifies complex threat possibilities such as the deployment of Chemical, Biological, Radiological, Nuclear, [High]-Explosive (CBRNE) weapons of mass destruction (WMD) and other highly lethal and/or technical threat possibilities. These are called *complex threat vectors*.

C. Threat Model - Overview:

The threat-model process involves developing OPFOR order of battle (OOB) data, and using the OOB data for conducting the Ends-Ways-Means assessment that seeks to reduce the uncertainty in answering the first three of these OPFOR-specific questions:

1. ***(Ends)*** What does the OPFOR "want" to do? – Intentions
2. ***(Ways)*** How has the OPFOR "done" it [conducted operations] before? – Demonstrated TTP
3. ***(Means)*** What "can" the OPFOR do? – Resources and capabilities
4. What will the OPFOR "do?" – Threat Course of Action (COA) hypotheses

The Ends-Ways-Means component of threat modeling includes developing *models* used to describe the OPFOR kill-chain processes for planning, mobilizing and executing attack activities. Threat modeling also facilitates *red-teaming* activities that are often helpful for generating threat COA hypotheses in response to the fourth and final question.

OPFOR activities and other recognizable kill-chain dynamics that are determined to be signature attack precursors are then identified as indicators. Indicators are located within the threat COA, and used as part of the I&W intelligence function to anticipate a developing threat situation. Order of Battle (OOB), Ends-Ways-Means assessments, threat models and threat COA hypotheses are updated regularly in conjunction with developments in the OPFOR situation.

D. Order of Battle Analysis:

The primary means to characterize the OPFOR is to employ Order of Battle (OOB or ORBAT) analysis. OOB is a breakout of key factors that describe the make-up of any fighting force. Even the highly networked, transnational, unconventional forces such as terrorist organizations can be assessed through the OOB process.

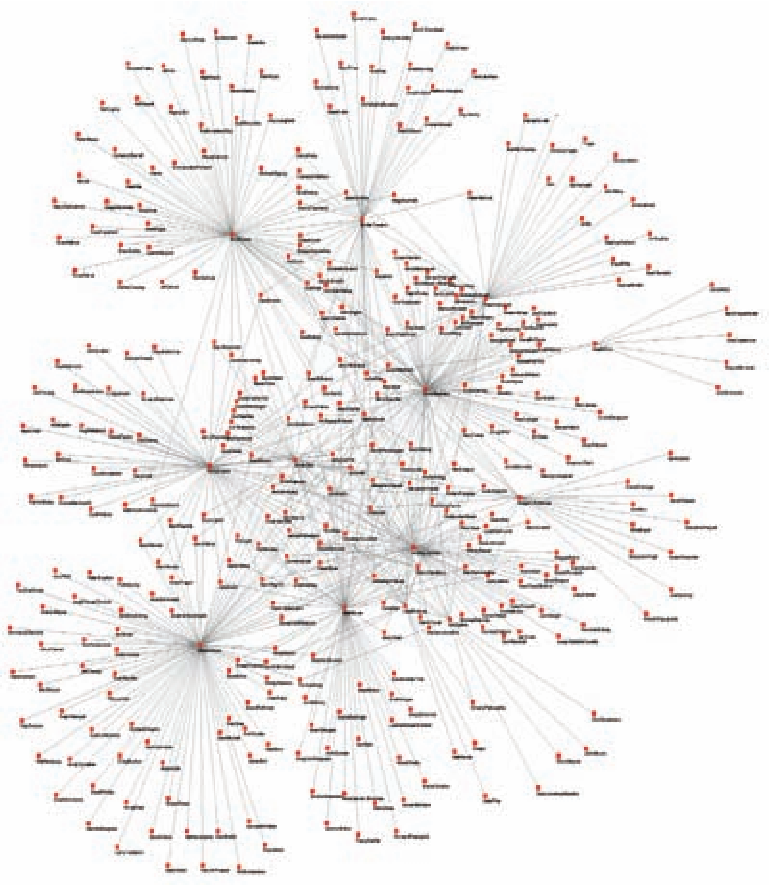
OOB is a methodology for cataloging an adversary's primary war-fighting attributes and establishing an understanding of the kind of war he desires to fight. It is also a means for ascertaining how these attributes contribute to or diminish the force's combat effectiveness. The OOB analysis helps define an adversary's capabilities, strengths, and other advantages while at the same time exposing the adversary's vulnerabilities, weaknesses and disadvantages.

E. The OOB List of Attributes:

Composition - Identification and organization of units and political, religious or ethnic organizations. Unit identification consists of the complete designation of a specific entity by name or number, type, relative size or strength, and subordination.

Disposition - Geographic location of OPFOR elements and how they are deployed, employed or located. Additionally, disposition includes the current, and projected movements or locations of these elements.

Strength - Conventionally described in terms of personnel, weapons and equipment. In counterterrorism operations, strength as a factor is augmented with attack teams, political cadre or cells, and most importantly, popular support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving logistics, or just withholding information.



Tactics - Strategy, methods of procedure, and doctrine. Each refers to the OPFOR accepted principles of organization and employment of forces. Tactics also involve political, military, psychological and economic considerations. OPFOR tactics and operations vary in sophistication according to the level of training the individual or organization has received. OPFOR carefully plan and train for individual and small group operations.

Training - The type and depth of individual and group training that operatives receive is tied to their tactics and operations.

Logistics - The effectiveness of OPFOR operations depends heavily on logistics. This dependency fluctuates horizontally and vertically between the various groups and levels of operation.

Combat Effectiveness - OPFOR receiving healthy flow of support, highly motivated stream of recruits, popular sympathies, fear, intimidation and political power shifts.

Personalities - A critical factor when conducting counterterrorism operations. Attention must be focused on individuals and leaders. OPFOR organizational diagrams can be built through multidimensional link analysis (determining relationships between critical personalities and then their group associations). This applies to virtually any threat represented in counterterrorism operations. Once relationships and the level of contact or knowledge the personalities have are known, many of their activities can be determined.

Culture - Culture is the ideology of a people or region and defines a people's way of life. A people's culture is reflected in their daily manners and customs. Culture outlines the existing systems of practical ethics, defines what constitutes good and evil, articulates the structures and disciplines that direct daily life, and provides direction to establish patterns of thinking and behavior. Cultural issues include, but are not limited to, religion, political and economic beliefs, tribe, clan, ethnicity, regional affiliation, military attitudes, law and justice.

Miscellaneous Data - Includes supporting information needed but not covered by an order of battle factor.

F. Ends – Ways – Means:

OOB factors are used to organize threat information and build the threat knowledgebase. Once in OOB format, threat information is further scrutinized to see how well capabilities line up with intentions as well as if there are any exploitable conditions existing in the ranks. This component of the threat assessment is called the *Ends-Ways-Means* assessment, and refers to identifying the OPFOR's intentions, methods, capabilities and resources.

Assessing Ends - *What does the OPFOR want to do?*

Answering this question involves an assessment of the adversary's strategic, operational and tactical aims and then determining how those aims relate to the execution of past attacks. Past shifts in these aims are also noted, as are any contractions or expansions. For each situation involving a changing objective, the circumstances are noted.

Assessing Ways - *How has the OPFOR conducted operations before?*

The Ways assessment describes the methods the OPFOR uses to achieve the desired end-state or objective, arranged in operational phases, tasks and activities when appropriate.

Past attacks by known groups offer an opportunity to learn how those groups' OOB factors are employed during an operation by examining how each group organizes, recruits, equips, trains and deploys for an attack. *The Ways* assessment reviews past attacks, cataloging the processes, methods, timing and sequencing of activities making up the OPFOR kill-chain. Past attacks can also offer opportunities to understand other patterns, such as target selection, weapon preference, relationships with other terrorists or criminal groups, and dependencies on sponsor nations. The assessment, therefore, also identifies the social networks involved in past attacks in addition to examining the key decisions, decision-makers, and decision processes. Particular attention is given to the target site and weapon selection, assessing the attributes of the target, noting the impact of timing on the resulting effects of the attack, and determining if the attack achieved the OPFOR's intentions.

Threat Framework - The information developed during this assessment is used to generate a threat framework (also, threat database, or threat files) that describe the elements of the OPFOR kill-chain. In fact, a primary product developed here is a graphic illustration depicting the kill-chain as a process flow chart along a timeline. The framework model is used to collect and compile learning points and patterns of behavior discovered after analyzing past attacks.

The threat framework is a tool that is intended to describe how the OPFOR Order of Battle is arranged in time and space, coordinated and supported, and able to surge or swarm when the moment is right. Framework models are improved over time. They are records of what is learned from regularly assessing an evolving threat. Framework models of the ex-Soviet military were developed over fifty years in extraordinary detail, but the process of modeling the current threat has only just begun, leaving plenty of gaps in the intelligence knowledgebase. However, even a rudimentary threat framework model is exceptionally useful as a frame of reference when making inferences or developing a threat picture.

The topics in this table represent the *baseline* set of factors that make up a threat framework.

Organization	**Ends**	**Ways**	**Means**
Weapon Selection	Design	Develop	Delivery
Target Selection	Objectives	Conditions	Effects
Attack	Tactical Organization	Operations	Command & Control
R&S	Assessment	Development	BDA

The development process involves researching past attacks, identifying each of these components and looking for continuity, trends or patterns between the attacks. The information collected in the threat framework and depicted in the kill-chain is next reviewed during the *Means* assessment.

The Kill-Chain Model – A *kill-chain* describes the arrangement and sequence of activities a threat group uses in planning, organizing, mobilizing, training, equipping and staging – resources and operatives. These activities make up the threat group's modus operandi, its attack system. Further, the kill-chain models are used to identify each threat's critical resources, critical capabilities, critical vulnerabilities, and *center of gravity.*

***Assessing Means - ****What can the OPFOR do?*

The *Means* assessment identifies the critical resources and critical capabilities the OPFOR needs in order conduct operations described in the kill-chain. The Means assessment also identifies the OPFOR Center of Gravity and Critical Vulnerabilities.

The Means assessment identifies what the OPFOR is really capable of doing by identifying the mix of core capabilities and resources at their disposal. This includes identifying the key enabling capabilities that are essential to operational success that 1) have been previously demonstrated, or 2) have recently emerged. The assessment reviews the OPFOR kill-chain model and examines demonstrated capabilities from past activities, noting what resources where assembled to enable each core capability. The assessment also identifies newly acquired capabilities or attempts by the OPFOR to acquire new capabilities.

OPFOR core capabilities and resources define the range of threat COA options that are examined when answering the final question, "What will the OPFOR do?" during the red team assessment. Furthermore, activities inherent to core capabilities are typically selected as indicators and used as key tools for anticipating threats and terrorist attacks.

The Means assessment also provides key insights into the underpinnings of the OPFOR's operational capacity that can be useful for interdiction strategies. The availability of core capabilities and resources are examined during the critical vulnerability and center of gravity analysis.

The Means assessment reviews the materials generated through the Ends and Ways assessments, including framework models and kill-chain models in order to isolate and characterize the core capabilities and required resources.

The following capability sets—standard to military action—are provided to guide the assessment:

- ❑ Personnel and staff management – recruit, train, cross border/global insert and extract, embed, document, equip, arm, instruct or direct, sustain and hide.

- ❑ Targeting – target assessment, target selection, target development, recon and surveillance, and deployment.

- ❑ Weapon handling – target-weapon pairing, acquisition (buy, steal, borrow material to design, develop, deliver, or acquired functioning weapon), weapon movement, storage, and demonstrated innovation.

- ❑ Command and control – planning, task-organization, communications, simultaneous coordinated operations, intelligence, counterintelligence and OPSEC, deception, and information operations.

- ❑ Logistics - finance, travel, move things, conduct research and purchase things.

Core capabilities can be assessed in a number of ways, but as a baseline the methodology will include identifying and describing the following elements within each capability:

- ❑ People, knowledge and specialty skills
- ❑ Tactics, techniques, procedures that were defined and understood
- ❑ Organization and structure
- ❑ Equipment
- ❑ Facilities
- ❑ Technology
- ❑ Materials
- ❑ Support

Center of Gravity and Critical Vulnerabilities (Decisive Points) - A center of gravity is a source of moral or physical strength, power, or resistance that is critical to the OPFOR's ability to execute operations. Critical vulnerabilities, also known as decisive points, are components of the OPFOR's operating system—kill-chain—that are both crucial to the functioning of the system and vulnerable to exploitation.

Threat – Target Pairing – Each threat, PTE and terrorist group is assessed in order to establish a *threat-target profile* that is used to pair jurisdictional targets with known OPFOR interests. When these threat-target pairs are identified, an *attack-lane* is said to exist between the two. Information developed during the target assessment and threat management processes provide the tools necessary to develop threat-target profiles, identify the threat-target pairs and conduct the risk-assessment.

Attack-Lanes - An attack-lane conceptually describes the unique relationship between a specific threat element and a particular target. It provides a word-picture for seeing jurisdictional targets at one end of a mobility corridor with an adversary force poised at the other end. There is nothing in between but an empty attack-lane stretching from threat to target.

Mobility classifications for attack-lanes provide base criteria for identifying broad threat-target pair priorities. An OPFOR with capability shortfalls regarding a specific target site is not able to progress along the hypothetical avenue of approach at all.

Attack Lane Conditions - Hypothetical mobility characteristics within the attack-lane are determined by the threat-target factor agreement conditions, for example:

- ❑ ***Go Condition -*** When threat-target factors are in synch, and environmental conditions have cycled to create an opportunity window, then a "*go*" condition exists within that attack-lane.

- ❑ ***Slow-Go Condition -*** When threat-target factors are in synch, but environmental factors are not optimal and, therefore, no opportunity window exists, then a *"slow-go"* condition exists within the attack-lane.

- ❑ ***No-Go Condition -*** When threat-target factors are not aligned, regardless of environmental factors, or opportunity windows, a *"no-go"* condition exists within the attack-lane.

Complex Threat Vectors Assessed - Threat modeling also examines the complex threat vectors identified during the threat inventory, cataloging the range of CBRNE threat potentials, specifically reviewing the characteristics of each type of weapon system, identifying precursor materials, specialized equipment and facility requirements, and requisite subject matter expertise needed to research, design, develop, store and transport the various weapon components. The material components and special apparatus that produce unique, detectable signatures are also identified.

Complex threat vectors also include emerging, innovative, difficult to detect, and highly dangerous threat scenarios that require additional, detailed analysis in order to fully develop prevention and response strategies.

Preventing, deterring or responding to these complex threat classes requires the support of detailed reference protocols that guide the TEW through the technical aspects of threat recognition, outlines critical agency alerting priorities, defines resource requirements and mitigation strategies, and assists the OIC cell determine internal personnel task assignments. The decision-making inherent to situations involving these special classes of threats is most effective when guided by organized references, developed prior to a crisis in a deliberate-planning environment.

Playbooks - The TEW uses reference products called *Playbooks* to provide preplanned general guidance for assessing complex threat situations. The TEW utilizes playbooks as an internal analytical guide. They are organized in standard formats for conducting assessments of actual terrorist threats or attacks. They guide TEW assessment activities before, during and after an attack. They identify common considerations and typical intelligence requirements that decision-makers are likely to need. The TEW has developed playbooks for chemical terrorism, biological terrorism, food surety, water supply surety, suicide bombings, large vehicle bombings, laser threats, radio frequency weapons, and radiological/nuclear terrorism. Additional playbooks will be developed as the need is identified.

G. Threat Integration:

Threat integration is a distinct process within the threat management task that evaluates potential arrangements of threat axis combinations. The effort begins by identifying the range of potential threat combinations—threat axis—including an OPFOR, possibly one or more complex threat vectors, a target preference, and optimal environmental conditions that, taken together, would pose the greatest catastrophic impact to the jurisdiction. These threat alignments are considered the highest impact threat (HIT) scenarios. HIT scenarios are then taken forward into the threat forecasting process.

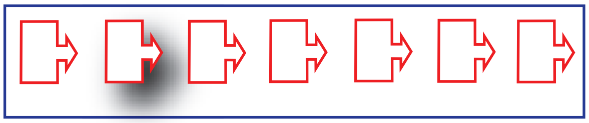
H. Threat Forecasting:

Threat Course of Action (COA) hypotheses - *What will the OPFOR do?*

Threat forecasting uses information developed during the threat inventory, threat modeling and threat integration assessments to develop hypotheses regarding OPFOR course of action (COA) options.

From the HIT scenarios, the threat forecasting effort draws out actual HIT *options*. A scenario is elevated to an option when the OPFOR has the capabilities required to assemble the threat axis and execute the attack. The combinations that are considered the most dangerous are identified as the adversary's most dangerous COA (MD COA) options. Threat combinations that are assessed as *most likely* are then identified as the adversaries ML COA. The result of the threat forecasting is the following three threat axis combinations:

1. Highest Impact Threat (HIT) scenarios.
2. MD Threat COA options.
3. ML Threat COA options.



These threat axis combinations become the basis for subsequent tasks, such as risk-assessment and I&W framework development. Additionally, MD and ML COA options can be further refined through red-teaming to begin formulating hypotheses describing various kill-chain potentials.

Whether a red team is used or not, the central threat forecasting activity involves formulating hypotheses of threat COA options. These COA hypotheses are used as the basis for developing situation-specific kill-chain models that graphically depict OPFOR actions such as planning, target assessment and selection, weapon development, recruitment, and tactical operations along a hypothetical timeline. When complete, the kill-chain model is essentially a graphic forecasting tool, an indicator-mapping tool, and a frame of reference during all-source/all-phase information fusion. When the kill-chain models of an OPFOR are compiled, the result is a comprehensive set of attack plans that include branches and sequels.

The assessment produces graphic attack diagrams to illustrate what the kill-chain would look like if its component parts could actually be seen moving along an attack-lane. This technique allows an analyst to visualize potential timing and sequencing options. The graphic model is not to be confused with factual "ground-truth" but is an analytical tool to help the analyst recognize patterns and relationships between activities. These graphics are called *situation templates*.

One kill-chain model for one attack-lane is developed at a time, allowing for role-playing one OPFOR against one target. During the assessment, however, the red team will identify decisive-points in the kill-chain sequence where branch and sequel options may develop that would shift an OPFOR kill-chain into another attack-lane against a different target. The red team will also identify decisive-points in the kill-chain sequence that help to identify deception options and commitment to a target.

The one-target-at-a-time kill-chain development does not suggest that an OPFOR will not attack along several lanes, against multiple targets with a single kill-chain (attack). The technique uses the one-to-one approach simply to isolate and identify any potential unique indicators that can be used to recognize a particular target is under attack as early as possible. The one-to-one approach also allows the red team to determine environmental conditions that would be optimal for enhancing the effects of the attack and amplifying the impact. When enough of these conditions are present, there is an opportunity window open for attack. Because of this, the I&W effort also tracks environmental factors, looking for indications that an opportunity window might be emerging.

The goal is to have a set of kill-chain models for each MD and ML COA option, as well as for each of the remaining HIT scenarios, illuminating the range of factors that would have to come together for any of these combined complex threat axis to emerge within an attack lane. With this in mind, the red team incorporates gaming techniques in the COA development process that involves scenarios vignettes exploring interaction possibilities between OPFOR cadre and local PTE. These techniques help provide a frame of reference for assessing local activities.

Red Teaming - Red teaming involves examining something from the adversary's perspective. Red teaming activities are used to evaluate physical as well as information security measures. In these situations, a red team or red cell, conducts actual operations against a facility in order to uncover security gaps or other vulnerabilities. Red teams are also useful during exercises to provide a reasoning, scheming adversary that can dynamically interact with the exercise participants.

Analytical red teaming in support of intelligence is a methodology for crafting forecasts from a first person perspective, involving a team of analysts who, by virtue of a simple shift of perspective, are able to comprehend nuances, grasp complexities, and actually get a sense for where an OPFOR may be vulnerable to being exposed, etc.

Section 2.6 – Risk-Assessment

A. Risk Assessment:

Having broadly defined the range of possible threat axis combinations, including the MD and ML COA options, the logical follow-on assessment then, involves identifying the jurisdiction's specific vulnerabilities as illuminated by each HIT scenario or threat COA option, and determining the possible consequences of a successful attack on each respective target.

The emphasis of risk assessment activities is on identifying threat, vulnerability, and criticality factors for jurisdictional targets, understanding the implications of an attack on these targets, and identifying critical response resources within the jurisdiction. Risk assessment includes both vulnerability analysis and consequence assessments. While these activities are identified as part of the target management task, they primarily support risk assessment.

Taken together, these activities provide a *risk assessment* that outlines the threat envelope over each target within each city or jurisdiction. Target reinforcement activities and random anti-terrorism measures (RAMS) then help reduce each target's vulnerability to attack. Additionally, newly identified tactical information on each potential target site is compiled into the Response Information Folder (RIF), developed with the intent to provide an incident commander with immediate site intelligence in the event of an incident. Further, RIFs feed the Operational Net Assessment and Mission Folder development process.

The risk-assessment process, from an intelligence perspective, involves comparing target attributes and limitations (vulnerabilities) with OPFOR capabilities, intentions, and recent attack trends observed globally. Priorities for risk assessment evaluations include threat-target sets within both the Most Dangerous (MD) and Most Likely (ML) threat COA options. Additional threat-target pairs identified as part of the list of HIT scenarios during threat integration are also top candidates for risk assessment.

During risk-assessment, the examination of each threat-target pair provides a more precise understanding of how well threat capabilities align with a specific target site's characteristics, including the site's physical and moral vulnerabilities. Furthermore, the risk-assessment describes the *threat envelope* around each target, and contributes to enhanced security and surveillance.

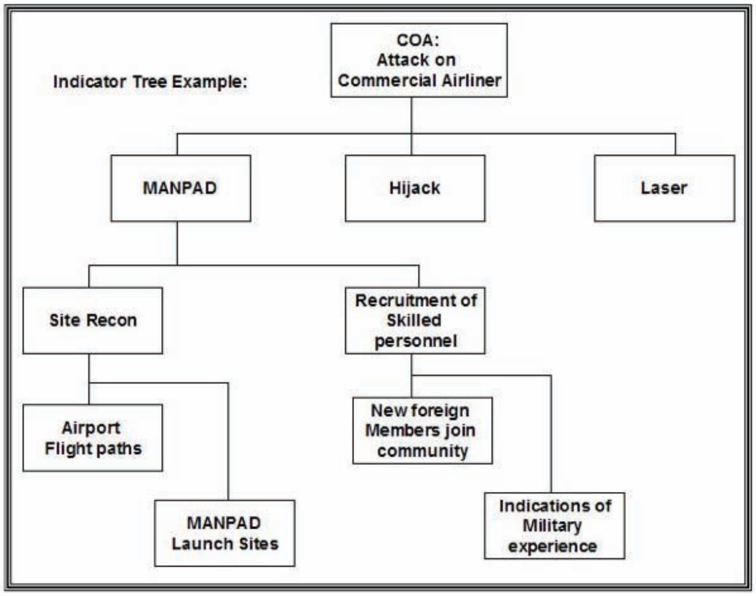
In addition to supporting the target-hardening effort, information developed during risk-assessment is also useful as part of the threat-model. An evaluation of threat-target factor alignments identifies pairs that are fully aligned, pairs that are nearly aligned, and pairs that are significantly out of alignment. When capability shortfalls are identified, the nature and extent of the shortfall is defined and required capabilities are identified. Attempts to acquire these capabilities are integrated into the I&W effort.

Section 2.7 –
Collection Management and Planning

A. Collection Management:

Developing the I&W Framework - The chain of logical activities continues with the development of an I&W framework, supported by an effective collection strategy. The I&W framework is the methodology used within the TEW for anticipating threats or terrorist attacks and involves examining the threat COA options; identifying activities, trends or patterns that signify the threat may be adopting a particular COA; and formulating a collection strategy that is focused on uncovering these signatures—hunting for elements of information that will fill intelligence gaps—when they occur. The framework provides a lens through which the threat environment can be scanned and monitored.

Indicator Trees - Using the threat COA hypotheses kill-chain model as a reference tool, indicators are selected and evaluated to attempt framing them in terms of time and space factors, environmental conditions, key activities, required resources, and other factors as appropriate. These subordinate factors, variables, conditions and activities are broken down further as appropriate to accommodate the constraints of available collection resources. The chain of subordinate variables and relationships associated with each indicator is compiled using a graphic analytical tool called an *indicator-tree*.


Indicator Tree Example:
COA: Attack on Commercial Airliner
MANPAD
Hijack
Laser
Site Recon
Recruitment of Skilled personnel
Airport Flight paths
MANPAD Launch Sites
New foreign Members join community
Indications of Military experience

Using the indicator-tree and kill-chain model, relationships and influences between the various components are evaluated. Special attention is paid to identifying logical event sequences and apparent dependencies or connections between threat elements. The indicator evaluation process results in a deeper understanding of the threat environment's composition and dynamics. This in turn adds focus and precision to the scanning process and adds rigor and context to the analysis and synthesis process.

Collection Strategies - Collecting information is a critical intelligence task involving the formulation of strategies for acquiring information through the employment of available *sensors* or other information resource providers—channels. The sensors could include a citizen's report of suspicious activity to community police, other human collection means, Internet scanning, signal 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 reach-back from multi-sensor arrays or field reconnaissance capabilities (*e.g.*, chemical, biological or radiological sensors or detectors).

During *Collection Planning*, the indicator trees collection characteristics are evaluated in order to match specific information requirements with appropriate information channels. Next, information channels and sources are evaluated in order to pair the specific information requirements with appropriate sources. Collection planning seeks to ensure the most effective and efficient combination of resources can be mapped to the appropriate elements on each indicator tree.

The following represent some basic attributes of an information channel and its source:

- ❑ Delivery –
  - ❍ Information “push” or “pull”
  - ❍ Regularity
  - ❍ Access
  - ❍ Medium – electronic delivery or download, hardcopy, or voice

- ❑ Content –
  - ❍ Scope, depth, accuracy, access and reliability of the source
  - ❍ Finished or raw intelligence
  - ❍ Timeliness of reporting and perishability of the information
  - ❍ Relative value and relevance
  - ❍ Verification, validation, and corroboration techniques or possibilities
  - ❍ Usability – format, controls and classification –easy or difficult to extract

- ❑ Access –
  - ❍ Responsive to *Request For Information* (RFI) or content is dictated by subject matter
  - ❍ Follow-up interaction, protocols and policies

Collection planning also makes sure the information resources are conducive to the “scan” methodology used during I&W. Scanning endeavors to spot key developments in the information stream with minimal false reads. Some resources, therefore, may be identified as first order materials that offer more breadth of coverage and easy parsing, while other materials will be used in second or third order analysis because they offer more depth, but are also more difficult to work through.

Description	Call Sign	Planned Observer Observation	Actual Window of Observation	Window of Target	Remarks
NAI1 (GL634048) Bridge crossing over Brown River.	A12	1600-0700		AB 105	Report any vehicle crossing.
NAI 2 (GL637049) Ford of Brown River.	A13	1600-0700		AB 106	Report any vehicle crossing or Engineer equipment.
NAI 3 (GL700055) Bridge crossing over Brown River.	A14	1600-0700		AB 105	Report number, type, and direction vehicles are moving on Highway 5.

A platoon reconnaissance matrix.

Section 2.8 –
Developing Intelligence

A. Information Processing:

The collection strategy, once executed, results in a content-rich information stream flowing into the TEW. Information processing involves parsing incoming reports and raw information into usable intelligence products. Processing activities include managing the information stream throughout the intelligence development sequence, ensuring information fragments—data—are harvested and organized—information—for the analytical effort. Within this process, incoming reports are triaged, validated and corroborated.

B. Intelligence Analysis:

The information fusion task involves correlating information from multiple sources and, through the intelligence analysis effort, developing a single, comprehensive intelligence picture. The fusion process is facilitated through the use of an intelligence model developed as a pictograph, template or even a text-based format, one that describes the conflict environment's multiple dynamics, providing an increasingly more complete frame of reference for seeing developments in context.

Information synthesized into the model is given deeper and broader context. This context then illuminates relationships between information that might otherwise have appeared unrelated and enhances the analytical activity's ability to extract situational understanding from the aggregated information. Using the intelligence model to support information fusion, develop situational understanding, and formulate increasingly more precise, predictive assessments is referred to as the *analysis/synthesis process*.

The all-source/all-phase information fusion and intelligence analysis tasks, however, are not inherently oriented toward satisfying the requirements of I&W and Operational Net Assessment. These intelligence tasks are the fundamental underpinnings of all intelligence functions, including those not specifically related to the TEW mission. Generating combat assessments, support to offensive targeting, and other intelligence support roles rely on information fusion and intelligence analysis as core capabilities as well. The threat recognition and the consequence assessment tasks bridge this gap, offering an array of activities specifically designed to shape the analysis/synthesis process toward I&W and Operational Net Assessment, respectively.

C. Threat Recognition:

The TEW threat recognition task includes a compliment of activities designed to 1) scan the indicator grid, broadly searching for threat triggers that make up the I&W framework, 2) transition over to *monitoring* when a situation evolves requiring more scrutiny at greater depths, 3) rapidly identify situational developments, non-obvious relationships, and threat indications not previously identified within the I&W framework, and 4) efficiently synthesize new information into the intelligence model and be able to draw out relevant threat signatures, trends and/or patterns that either help uncover OPFOR activities or simply enhance the model.

D. Transaction Analysis Overview:

The Transaction Analysis concept has emerged as one of the key novel intelligence analysis techniques within the TEW. Transaction analysis integrates the knowledge-base within the intelligence model, risk assessment activities and findings, and the daily information processing effort. The *Transaction Analysis*

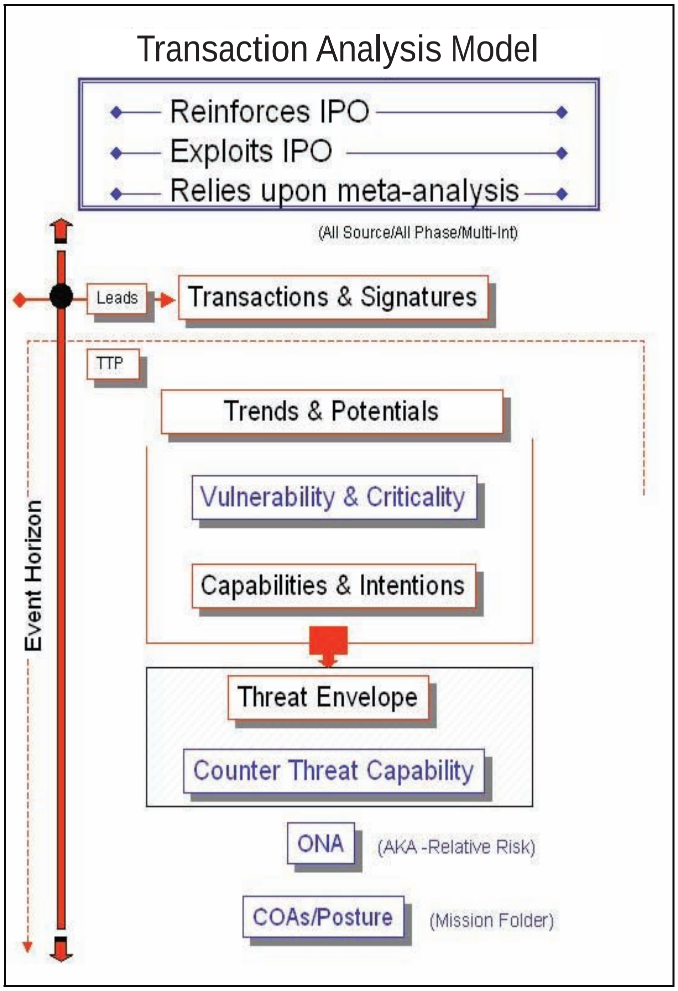
Model is used as an analytical reference guide for illustrating how the various process elements are integrated. It also highlights the critical threat v. friendly dynamics the Analysis/Synthesis effort should be watching for.

The *Transaction Analysis Cycle* illustrates the underlying analytical concept that guides identifying and extracting critical information out of incoming reports. It also illustrates how the cycle's dynamic serves as a pattern generator (like the TEW organization and IPO framework) centered on Analysis/Synthesis. By utilizing this framework, analysts observe activities or transactions conducted by a range of actors looking for indicators or precursors of terrorist or criminal activity of many types.

These activities are bundled together within the *Transaction Analysis Process*. The process involves both the IPO intelligence model serving as a reference, providing context to the analytical effort, and the transaction analysis cycle guiding the information parsing process, helping the analyst rapidly identify the information with intelligence value. Information is then organized and analyzed within the *Transaction Analysis Process* using the intelligence model to identify potential relationships to kill-chain activities, and then, as illustrated by the *Transaction Analysis Model*, to identify evidence of an emerging complex threat axis combination involving: 1) a kill-chain within 2) an attack-lane 3) under 'go' conditions (threat capabilities and intentions matched to target vulnerabilities and criticality in an environment with conditions favoring an attack –existing opportunity window).

The *Transaction Analysis Process*, therefore, is able to facilitate the I&W objective and cull the information stream for indications of an emerging threat. It is a 'threat recognition' process designed to be an effective tool for both scanning for the previously identified *indicators* developed within the I&W framework work-up, as well as for uncovering other *indications* of threat activities by finding signatures buried in the information stream's *noise* and correlating those with alternative kill-chain possibilities.

E. Transaction Analysis Model


Transaction Analysis Model
Reinforces IPO
Exploits IPO
Relies upon meta-analysis
(All Source/All Phase/Multi-Int)
Leads
Transactions & Signatures
TTP
Trends & Potentials
Vulnerability & Criticality
Capabilities & Intentions
Threat Envelope
Counter Threat Capability
ONA
(AKA -Relative Risk)
COAs/Posture
(Mission Folder)
Event Horizon

The Transaction Analysis Model is a tool used to graphically illustrate the relationships between information processing activities guided by the Transaction Analysis Cycle processes and the intelligence model generated through the IPO process. This relationship map helps to guide analysts in the effort to correlate and align various threat related factors identified during threat modeling with potential target-related factors identified during risk assessment.

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

Trends and Potentials: When aggregated, transactions and signatures may form specific trends and potentials (stage two) indicative of terrorist, insurgent or criminal activity.

Vulnerability and Criticality: Absent-specific indicators or information outlining a specific terrorist 'kill chain,' likely target locations can be identified through an assessment of vulnerability and criticality (stage three).

Capabilities and Intentions: These assessments form a hypothesis (or one of multiple competing hypotheses) about the OPFOR's capabilities and intentions (stage four) to be tested through collection and analysis.

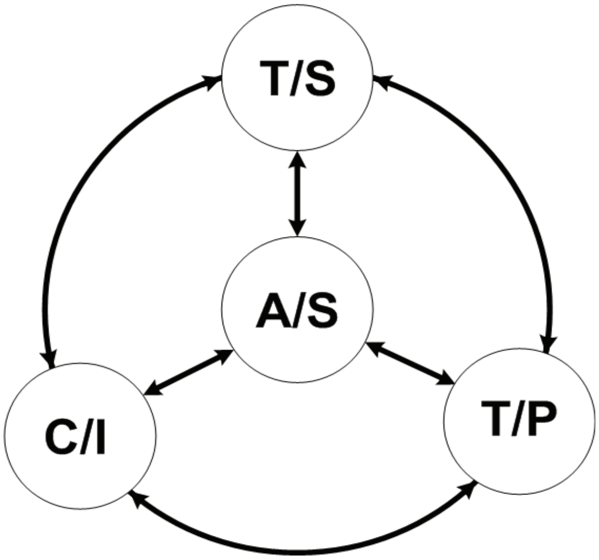
Threat Envelope: The threat envelope is defined by the combination of trends and potentials, vulnerability and criticality, and capabilities and intentions. It represents when terrorists are likely to attack and corresponds roughly to the I&W envelope we are trying to detect via the Transaction Analysis Cycle. An examination of the Transaction Analysis Model, for example, highlights how shifting threat factors that show movement toward aligning with target factors represent an evolving threat envelope.

Counter Threat Capability: Counter threat capability represents the sum total actions that we are able to muster to counter or respond to a given threat. These are our friendly actions.

Net Assessment: An operational or strategic net assessment represents the interaction between threat and friendly capabilities at a given point in time. When friendly capabilities are matched with the threat, the resulting assessment of relative risk can be defined in an operational or strategic net assessment.

Courses of Action/Response Posture: Courses of action (COAs) to respond to and mitigate the risk as well as the posture of friendly security and public safety organizations can be calibrated to the situation described in the net assessment. This information is transmitted through a "Mission Folder," advisories, alerts or warnings and described in IPO Step 4. Discerning the threat components of various transactional data is achieved by using the Transaction Analysis Cycle in combination with the IPO generated intelligence model.

Transaction Analysis Cycle



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

F. Transaction Analysis Cycle

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 TEW's ongoing 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.

Individual transactions (such as acquiring finances, expertise, materials, 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.

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.

G. Transaction Analysis Process:

Pulling all these concepts together and facilitating threat recognition through I&W scanning is the *Transaction Analysis Process*. The process is the interaction between the model and the cycle. It involves analytical activities guided by 1) the Transaction Analysis Cycle and intelligence model to develop intelligence that can be 2) evaluated within the context of an emerging threat using the linear Transaction Analysis Model. The process facilitates:

- □ Parsing through large volumes of information,
- □ Identifying and categorizing threat related activities,
- □ Putting these activities into an organized context,
- □ Recognizing various continuity thread possibilities between activities and
- □ Associating various activity threads to formulate situational hypotheses and evaluate these within the context of I&W.

Using the Transaction Analysis Cycle, the process seeks to identify the transactional aspects of all reported activities. Instead of focusing narrowly on just an activity as the central theme for evaluation, transaction analysis focuses on the characteristics that frame the transactional situation. These characteristics, once they have been identified, examined and developed, are used to identify the range of possible contextual relationships with other transactions. The following is a list of these basic attributes, but the analyst is not constrained from identifying others as well:

- □ A connection
- □ An exchange
- □ A purpose
- □ A place
- □ A time
- □ At least one person
- □ An outcome

These transactions, individually or collectively, may have a signature consistent with criminal or terrorist activity or actors. The key is to recognize that there are many relational "hooks" that allow seemingly unrelated events to be assembled together within a shared context—time, space, or activity—and then scrutinized in the aggregate (*transaction threads*) to explore the possibility that collectively they have a story to tell.

This approach offers multiple dimensions for evaluating the information based on how the transactions related. Each inferred set of connections—transaction thread—however, is assessed to discover evidence that rules out the connections. This process ensures only the viable relationships remain. These "tested" transaction threads are assessed to identify an emerging pattern or signature and are evaluated against other threads to identify if relationships can be made and a trend or signature can be hypothesized. The hypothesis is then subject to testing. Furthermore, the hypothesis is evaluated against the indicator list to identify precursor threat activity or determine if threat actors may be present.

Transaction threads are also evaluated to identify if there are possible relationships with a broader, global context, a known OPFOR for example, with known capabilities and intentions. Scrutinized under these conditions, a trend may represent a deadly potential, if indeed, the connection is valid. Here again, thread connections are reviewed to identify tangible, factual reasons why the relationship could not exist to rule it out. If it cannot be ruled out, the relationship is evaluated to identify linchpins and drivers, evidence that would confirm or deny the thread relationship if it were available.

Further, these possible trends are also viewed within the context of an emerging unknown OPFOR or PTE. Again, where the relationship or the possibility can not be refused based on tangible factors, they are recognized as possible event horizons, the initial signatures of possible hostile actions.

At any one time, the TEW could have numerous possible trends identified out of the transaction threads that can be neither ruled out nor confirmed. Of those open trend possibilities, it is also likely that when viewed in the context of potential associations with an OPFOR, known or unknown, dangerous possibilities exist that can neither be confirmed nor denied. These "open" potentials are never assumed away. Because of the possibilities attached to them, they may be red-teamed to fully develop the range of possibilities.

H. Intelligence Co-Production:

The emerging network of TEWs is a valuable starting point for developing a national network capable of sharing information and intelligence laterally (department to department, TEW to TEW) and vertically (both top-down, from federal agencies, and bottom-up from local agencies and TEWs to state and federal agencies). Essentially, regional TEWs, together with state threat centers, can act as distributed intelligence fusion capabilities that link law enforcement, public safety and intelligence fusion agencies toward prevention of terrorist attacks and better management of response to attacks when they occur.

The TEW 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.

I. Dissemination and Feedback

Dissemination - The heart of information sharing is dissemination of the information. Policies have been established for the types of information that will be disseminated and to whom. Critical to appropriate dissemination of information is understanding which persons have the "right to know" and the "need to know" the information, both within the agency and externally. In some cases, there may need to be multiple versions of one product. For example, an unclassified public version of a report may be created to advise citizens of possible threats. A second version may be "law enforcement sensitive" and provide more detailed information about potential suspects that would be inappropriate to publicize.

When disseminating sensitive material, the TEW imposes a "Third Agency Rule," also known as Originator Control (ORCON). This means that any recipient of intelligence is prohibited from sharing the information with another (i.e., third) agency without permission from the TEW.

J. Information Security/Sensitive but Unclassified Categorizations:

Law Enforcement Sensitive – Intelligence that relates to sensitive investigative or other law enforcement activities. This may only be disseminated to law enforcement agencies with the need-to-know.

Public Safety Sensitive – Threat-related intelligence that can be shared with official public safety agencies. On occasion, these documents may be an appropriately sanitized version of a law enforcement sensitive document that is releasable outside law enforcement channels. This is also disseminated on a need-to-know basis.

Critical Infrastructure Sensitive – This classification restricts dissemination to appropriate public and private parties with right-to-know or need-to-know status and who are not holding an official capacity within law enforcement or public safety agencies.

K. Product Dissemination Criteria:

All TEW product dissemination is subject to the approval of the TEW OIC. TEW developed intelligence and critical information is placed in a report format that maximizes the consumption and use of the information. Each TEW report meets the following criteria:

1. Identifies the targeted consumer of the information (patrol officers, administrators, task force members, others).

2. Conveys the critical information clearly.

3. Identifies time parameters wherein the intelligence is actionable.

4. Provides recommendations for follow-up if appropriate.

TEW dissemination includes regularly produced intelligence reports and products that have a specific format and type of message to convey. They have a specific purpose; are in a consistent, clear, and aesthetic format; and contain all critical information the consumer needs and no superfluous information.

L. Products and Reports:

Monthly OSINTrep – A TEW product that compiles articles of interest or other materials deemed appropriate and relevant. Normally disseminated during the TEW monthly meeting, it includes original text and analysis.

Net-Assessments - The *net-assessment* provides the UCS and emergency managers in the EOC with current situational intelligence, threat course of action forecasts, hazard consequence forecasts, resource availability/requirement profiles and outlines Random Antiterrorism Measures (the net assessment is addressed in more detail in parts four and five).

Mission Folder – This is also an incident-specific intelligence product, combining pre-event intelligence preparation (playbooks and RIFs) with time-sensitive threat information, providing the UCS with a set of friendly force *Course of Action* (COA) recommendations (the mission folder is addressed in more detail in parts four and five).

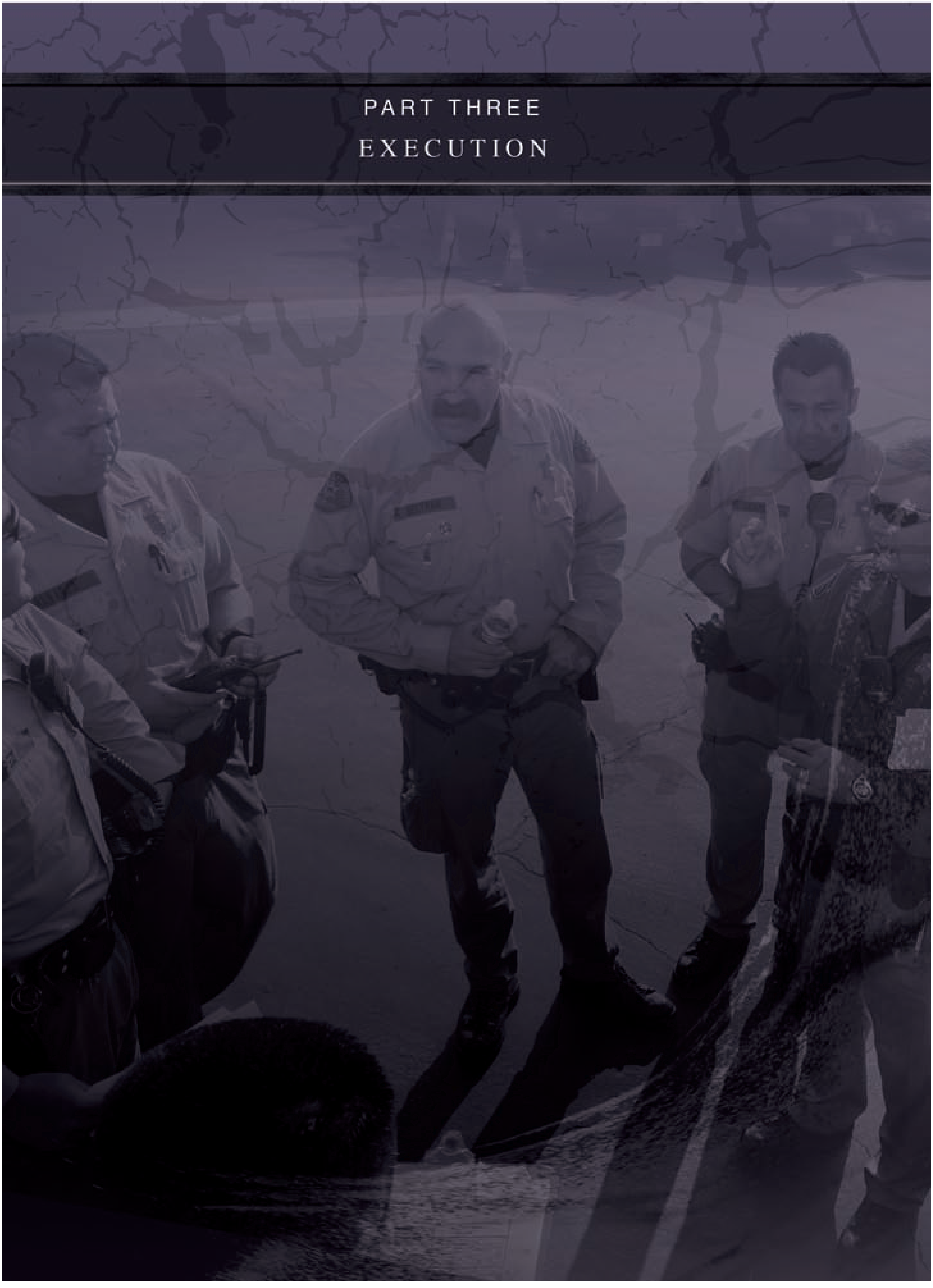
Advisories - A TEW product issued to provide information on potential global or national threats (that are non-specific, low credibility and/or uncorroborated), tactics, techniques and procedures (TTPs) that may be used by terrorists (i.e., modus operandi information), and information on operational security (OPSEC) or officer safety value. Advisories are designed to raise awareness and support training and familiarization objectives. Advisories can be issued during all five national Homeland Security Advisory System (HSAS) levels.

Alerts - A TEW product issued when there is a specific, verified and validated increased threat of terrorism to the United States. These will include potential attacks against US interests abroad or within the United States (particularly locally or adjacent states). Alerts may impact a TEW's operations, but a specific named target within that TEW's area of operations is not known or specified. Alerts will generally be issued during Elevated (Yellow) or High (Orange) HSAS levels.

Warnings - A TEW product issued when there is a credible, verified and validated specific threat to persons or venues (specific sites, events or critical infrastructure) within a TEW's area of operations or an adjacent jurisdiction if local resources are expected to become involved in a mutual aid response. Warnings will always be accompanied by specific response planning steps and recommended course of action options for response. Warnings will be issued during a severe (RED) HSAS level.

PART THREE

EXECUTION



Section 3.1 –
Deliberate Planning IPO:

A. IPO Overview:

IPO produces the TEW intelligence model, blending weather, enemy and terrain (WET) with Urban IPB (Intelligence Preparation of the Battlefield) and a variety of geospatial and geosocial tools to provide context for anticipating and understanding a suite of potential and actual threats.

B. IPO Concept Development:

IPO evolved out of an effort to develop a comprehensive intelligence model, structured to support the tasks associated with conducting counterterrorism intelligence operations emphasizing all-source, all-phase intelligence analysis and synthesis.

The military Intelligence Preparation of the Battlespace (IPB) process, a long standing and proven intelligence operations model, provided the basic template for tailoring the framework of an IPO concept. An IPO working group formed around the tasks of developing the IPO concept, ensuring it was tested, assessed, re-shaped and refined regularly as new issues evolved. The working group composition included personnel with subject matter expertise across a range of relevant disciplines, including law enforcement, public safety and military intelligence.

The IPO process that emerged was designed to be adaptive and scalable. Currently, the dynamics of the operational space environment, the nature and character of the threat, in addition to a host of other relevant information domains that fall within the IPO span of interest, continue to evolve. Dimensions and characteristics of the domestic intelligence arena are still being uncovered and understood. The IPO intelligence model, therefore, should be considered to be constantly evolving and adapting. IPO activities can expand or contract with requirements. IPO has the capacity to assimilate new methodologies and has the flexibility to be configured in a manner appropriate to a jurisdiction's unique characteristics.

The essential IPO framework, however, remains constant. The overarching purpose of IPO is to support domestic intelligence counterterrorism operations. The arrangement of activities, the alignment of steps, the nomenclature, and the embedded analytical conventions make up the essential structure of the IPO process and provide the basis for developing standards of continuity as the network of TEW organizations continues to grow.

C. IPO Attributes:

IPO provides a process for developing the domestic intelligence model required for synchronizing the development of actionable intelligence products with critical operational decisions. Drawn from the military's Intelligence Preparations of the Battlefield (IPB) methodology, the IPO process is built on a logical framework of activities designed to compliment, accommodate and integrate intelligence operations across all phases of the intelligence cycle and all phases of an emergency.

The IPO approach is made up of a collection of interrelated activities with the following attributes:

- ❑ IPO is both cyclic and continuous. It is structured around a progressive four-step process in which the outcomes and products of each step are further developed and refined in subsequent steps.
  - ❍ Step One: Define the Operational Space Environment
  - ❍ Step Two: Describe the Operational Space Environment Effects
  - ❍ Step Three: Evaluate the OPFOR and Threat
  - ❍ Step Four: Determine the OPFOR and Friendly COA
- ❑ IPO is built on the foundation of the traditional intelligence cycle and provides a comprehensive approach for working through each respective phase. Conducting IPO inherently involves the integration of collection, analysis and production activities.
- ❑ IPO helps identify relevant and pertinent jurisdictional issues, provides a framework that focuses the intelligence effort, and helps intelligence managers shape the scope and magnitude of their operations.
- ❑ IPO supports the functions, tasks and activities of domestic intelligence operations and aligns these operations with the characteristics of the operational space, the nature of the threat and the jurisdictional response posture.
- ❑ IPO is flexible and adaptable. It facilitates rapid response, enhances an aggressive optempo, provides continuity during operational transitions, and can scale as needed across the continuum of operational conditions (pre-attack, trans-attack and post-attack concepts addressed in the following section).

The IPO process is designed to consider all aspects of the operational environment in addition to how these aspects influence both friendly as well as adversary –Opposition Forces (OPFOR)—operations. A key principle of IPO is that it is a continuous process characterized by regular reviews, frequent updates and situation-specified refinement. The IPO process works through the four IPO steps and establishes a broad set of IPO products for the operations area.

Another key principle of IPO is the utility of graphic products that provide the intelligence analyst the ability to view issues from multiple perspectives. Very similar to a concept called "Crime Mapping," IPO graphics are tailored to facilitate working through complex analytical issues, enhance pattern recognition and illustrate key intelligence findings. The evolution of Geospatial Information Systems has created an opportunity to significantly enhance the potential for further development of graphic IPO applications.

D. IPO Strategies:

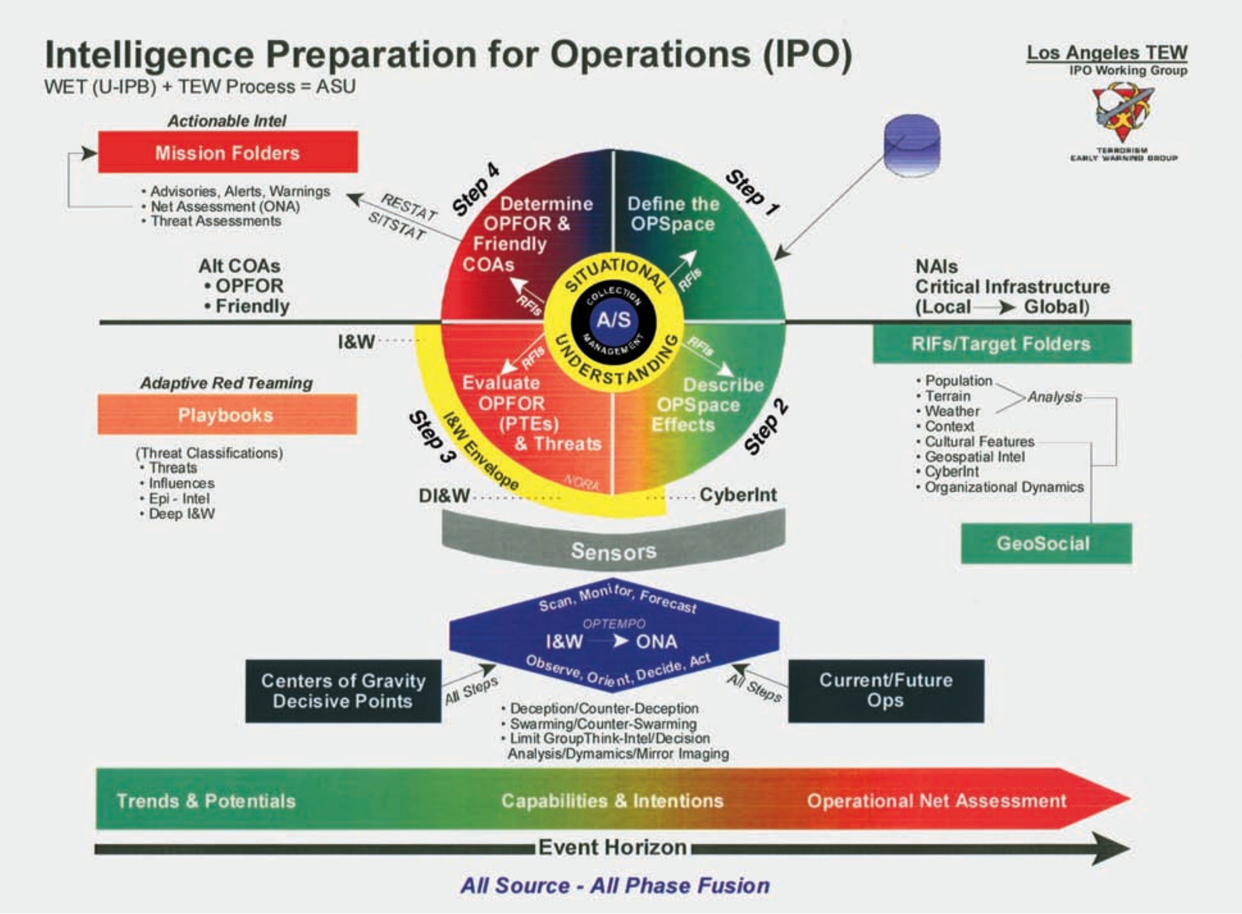
IPO is most effective when conducted within an overarching IPO strategy. While the process is described as four steps conducted sequentially, the initial model "preparation" phase will be one of the few times the entire process is conducted end-to-end. This initial run through will establish baseline support products that are inherent to the IPO approach. Even the initial preparation phase, however, is an enormous undertaking, requiring an iterative, but consistent effort. The IPO process after that will be situation-dependent, driven by circumstances incorporating only the required steps and processes.

E. IPO Process Graphic:

The following information is intended to accompany the IPO Graphic provided below:

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 (NAI) 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 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, weather and cultural features, including cultural intelligence or CULTINT, are also assessed. Geospatial intelligence (GEOINT) including potential infrastructural interactions, 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 is a capability for acquiring or collecting information: sensors. The sensors could include a citizen's report of suspicious activity to community police, other human collection means, Internet scanning, signal 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, and 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.

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.

Putting IPO into Action - IPO provides an ever-maturing intelligence model that serves as the framework for most TEW intelligence tasks. Throughout the CONOP, the emphasis of presentation has been on describing and explaining tasks and activities without regard to sequence or workflow. Beginning with Section 3.2, the presentation emphasis shifts to addressing topics in proper sequence as part of the flow of operations. Further, the information is organized in 'worksheet' formats to be more useable as a reference resource.

As a review, the general sequence of work during circumstances characterized by deliberate planning/operations is:

1. Develop the intelligence model using IPO framework as a guide,
2. Develop Threat COA options,
3. Conduct risk assessment and develop RAMs or target hardening recommendations,
4. Develop I&W framework and collections strategy, and
5. Conduct scanning.

Under circumstances characterized by crisis action planning, the R2P2 intelligence process is initiated with the development of a provisional net assessment. The general sequence of work during R2P2 includes the following:

1. Develop a new, more specific intelligence model;
2. Develop new, more specific threat COA options;
3. Conduct situation-specific risk assessment and develop I&W framework;
4. Prepare decision support products and disseminate; and
5. Conduct monitoring.

The following section provides a more detailed explanation of each of these general steps.

Section 3.2 – The IPO Process –
Developing the Intelligence Model

IPO Step One: Define the Operational Space

Activity	Description	Product
I-I	Ops Space Area Evaluation	Ops Space Orientation
I-II	Identify Critical Infrastructure (Local ↔ Global)	Named Areas of Interest (NAI)

IPO Step Two: Describe the Operational Space Effects

Activity Description	Product	
II-I	Target Inventory	Jurisdiction's Target Contour – Potential Targets Identified
II-II	Target – Response Model	Response Information Folders (RIF)
II-III	Identify Environmental Factors	Environmental Factor Studies
II-IV	Identify Combined Effects	Combined Factors Effect Assessment

IPO Step Three: Evaluate the Threat

Activity	Description	Product
III-I	Threat Inventory	Complex Threat Vectors and PTE
III-II	Threat Model	Threat Framework and Playbooks
III-III	Threat Integration (Complex Threat Combinations)	High Impact Threat (HIT) Scenarios

IPO Step Four: Determine the Threat Course of Action (COA)

Activity	Description	Product
IV-I	Threat Forecasting	Threat COA Options (Alternate, Competing Hypotheses)

A. IPO Step One

IPO Step One: Define the Operational Space

Activity I-I: Ops Space Area Evaluation

Product: Ops Space Orientation

Activity Information

Summary: Identify the defining features of the Operational Space.

Inputs: Available encyclopedic research, current events, mapping tools, and demographic data.

Expected Outcomes: Area orientation.

Overview of Typical Steps:

1. Define the Ops Space “panoramic.”
   - Develop the basic orientation.
   - Define the area’s composition.
   - Define the area’s disposition.
2. Define divergent views.
   - Legacy - place in history, development, contributions, growth factors.
   - Attraction and Draw.
   - Distinctions.
   - Symbolic stature.
3. Define the ‘systems’ view of Ops Space.
   - Identify Local → Global dependencies, and relational linkages of critical input and output.
   - Identify the critical drivers and influence threads of each.
   - Identify the ‘cultural’ systems.
   - Identify critical systems and structures.

Concepts Review

Ops Space Panoramic:

Orientation:
- Location
- Symbolic stature
- Strategic significance
- Organization of jurisdictions
- Area population statistics
- Breakout of key cultural, economic and political sectors

Ops Space Composition:
- Scope and magnitude of area
- Infrastructure
- Geosocial complexion
- Economic and industrial centers
- Jurisdictional systems and authorities

Ops Space Disposition:
- Identify cultural, economic-industrial systems and critical inputs-outputs – influence threads.

Divergent Views:

See the Ops Space through alternative perspectives.

System’s View:

Basic characteristics of Local → Global dependencies:
- Hub –central component with multiple dependents.
- Gateway – pass through or part of a value chain.
- Patron –dependencies on others.

IPO Step One: Define the Operational Space

Activity I-II: Identify Critical Infrastructure (Local → Global)

Product: Named Areas of Interest (NAI)

Activity Information

Summary: During the Area Evaluation, the Ops Space was defined in terms of its critical systems and structures. Additionally, Local → Global dependencies were identified. Within this set of systems, the Ops Space critical infrastructure will be found. The next effort identifies the critical infrastructure systems, defines its features, determines its linkages, and defines its critical input and output. Key nodes and facilities are designated as NAI and may be identified as potential targets in subsequent steps. Critical infrastructure, once identified, is evaluated and prioritized by its relative criticality.

Inputs:
-Jurisdictions critical infrastructure prioritization criteria and scoring convention.

-Area Evaluation data.

Expected Outcomes: Critical Infrastructure identified and prioritized. NAI identified.

Overview of Typical Steps:

1. **Identify Critical Infrastructure.**
   - Identify facilities and services that are critical to the jurisdiction.
   - Identify linkages to global, national or regional critical infrastructure systems.
   - Develop a list of critical infrastructure and determine criticality score.
   - Determine relative priority and ranking order.

Concepts Review

Critical Infrastructure:

The critical infrastructure identification process locates the infrastructure which, if attacked, could produce the most severe consequences. Critical infrastructure include sites, facilities, systems or system components, or special events that, if it were attacked, would result in:

□ A large number of deaths or injuries – Mass Gathering Events & Venues.
□ Extensive damage to life-sustaining services – Critical Node Targets.

The process, therefore, identifies the *services* which, if attacked, could produce the most severe consequences and then defines the key sites, facilities or other features that make up this service.

Additionally, the process assigns a relative value to each service, making it simple to prioritize the jurisdiction's critical infrastructure for subsequent tasks.

Named Areas of Interest (NAI):

NAI are geographical sites or facilities that are functioning as nodes within a critical infrastructure system and are used to define that system's physical profile. NAI may also represent a site or facility upon which a critical infrastructure service is highly dependent. NAI define the critical infrastructure's "target system" features and are assessed in more detail in IPO Step Two, at which time they may be identified as potential targets.

IPO Step One: Define the Operational Space

Activity I-II: Identify Critical Infrastructure (Local → Global)

Product: Named Areas of Interest (Continued)

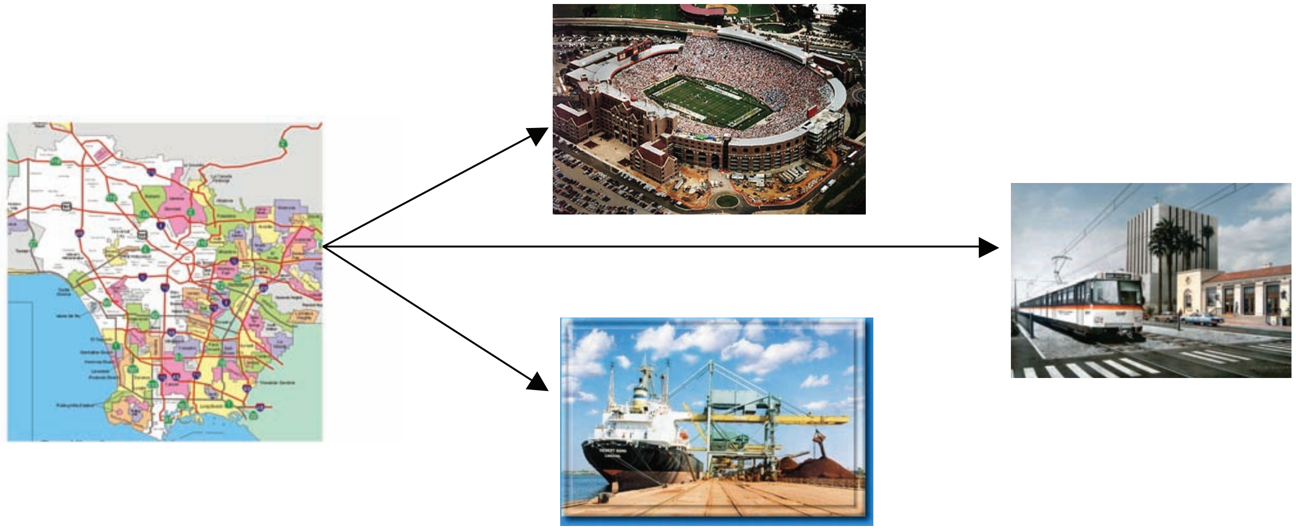
Concepts Review

Essential Goods and Services
Critical infrastructure sectors such as agriculture, food, and water, along with public health and emergency services, provide the essential goods and services that Americans depend on to survive.

Delivery of Essential Goods and Services
Energy, transportation, banking and financial services, chemical manufacturing, postal services, and shipping sustain the nation's economy and make possible and available a continuous array of goods and services.

Interconnectedness and Operability
The information and telecommunications infrastructure connects and increasingly controls the operations of the other critical infrastructures.

Public Safety and Security
Our government institutions guarantee our national security, freedom and key governance, as well as services that make up the nation's public safety net.



B. IPO Step Two

IPO Step Two: Describe the Operational Space Effects

Activity II-I: Target Inventory

Product: Jurisdiction's Target Contour – Potential Targets Identified

Activity Information

Summary: Identifies the Jurisdiction's potential targets by identifying *critical nodes, mass-gathering events* and *venues,* and sites with *symbolic value*. This last set of potential targets are sites that do not necessarily have high value in terms of either critical services or lethality but have a relative value as a target in the eyes an OPFOR.

Inputs: Critical Infrastructure and NAI identified in IPO Step One.

Expected Outcomes: Potential targets identified.

Overview of Typical Steps:

1. **Identify Mass Gathering Events.**
   - Identify events, dates, and venues as potential *High-Value Targets* (HVT).
2. **Conduct Target System Analysis starting at NAI.**
   - Identify critical infrastructure systems and define the system environment.
   - Identify system's functions and processes.
3. **Conduct Critical Node Analysis.**
   - Evaluate system components and determine which are critical to the system.
   - Critical nodes are identified as *High-Value Targets* (HVT).
4. **Identify OPFOR Targets of Interest.**
   - Identify sites or events with potential symbolic significance, identified as High-Payoff Targets (HPT).

Concepts Review

Target Inventory:

Critical infrastructure is not, in and of itself, a site that can be targeted. Critical infrastructure relies on a number of highly dependent inter-modal system components that are not usually centrally located in a single site but may be spread across jurisdictions, across the nation and even across the globe. OPFOR objectives involving the denial, disruption or destruction of vital life-sustaining services will attack the critical infrastructure system by targeting its critical nodes. The target identification process, therefore, defines the *target system* environment and identifies *critical nodes* that could be targeted.

Other potential target sets are identified as well, including mass-gathering events and sites with symbolic value to the OPFOR.

Critical infrastructures consist of critical assets:

Physical plant, systems or functions, and human resources. Some of these critical assets are essential to the availability and reliability of delivery of the vital services that the critical infrastructures provide. Destruction of these critical assets would have such adverse effects on service that they would put at risk the jurisdiction's economic security, public safety and quality of life.

The assets, systems and functions that comprise the critical infrastructures are highly sophisticated and complex. They consist of human assets and physical and cyber systems that work together in processes that are highly interdependent. They are also comprised of key nodes or critical assets that are, in turn, essential to the operation of the critical infrastructures in which they function. Destruction or disruption of these critical assets would cripple the operations of the infrastructures they support.

IPO Step Two: Describe the Operational Space Effects

Activity II-I: Target Inventory

Product: Jurisdiction's Target Contour – Potential Targets Identified (Continued)

Concepts Review

Target Systems:

The target system analysis identifies the critical infrastructure's underlying system. The analysis describes the functions, processes and dependencies of each respective system's components, nodes and facilities, and sets the stage for the *critical node analysis*.

Critical Nodes:

Nodal analysis assigns numerical scores to a system's components based on each part's functional significance and importance to other components in terms of dependencies. The effort identifies the backbone components–critical nodes—without which the system cannot function. Each system's critical nodes, when associated with a physical site, are identified as a HVT.

Mass Gathering Events:

Special, high visibility, high participation events, regularly scheduled or not, require the least analysis to identify. The broad steps involved here include 1) Identifying the venues, 2) reviewing each venue's calendar of scheduled events, and 3) determining what specific targets within the venue would cause the greatest loss of life. The potential target sites within these venues are identified as high value targets (HVT).

OPFOR Targets of Interest:

The OPFOR may assign symbolic value to a particular type of facility, targeting it for that reason alone. Sites, events, significant dates and personalities that have symbolic value are identified and designated as High-Payoff Targets (HPT).

IPO Step Two: Describe the Operational Space Effects

Activity II-II: Target - Response Modeling

Product: Response Information Folder (RIF)

Activity Information

Summary: For each potential HVT or HPT, standardized information packs called Response Information Folders (RIF) are developed.

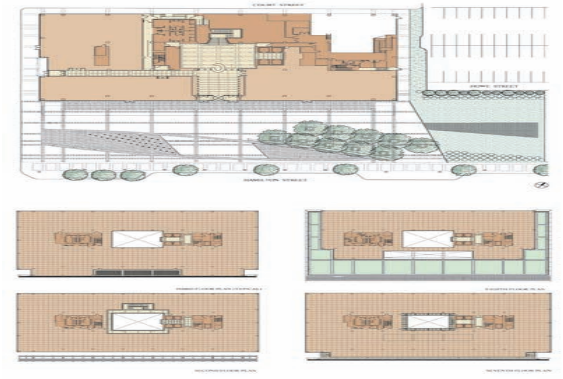
Inputs: Terrain, structural, and other data as identified on potential targets/NAI and sites designated as HVT or HPT.

Information on response resources, hospitals and local community–residence, schools and businesses.

Expected Outcomes: Response Information Folders (RIF) developed for each NAI.

Overview of Typical Steps:

1. Identify information requirements.
2. Assemble required information and materials.
3. Conduct studies and develop information products.
4. Develop RIF.



Concepts Review

Response Information Folders (RIF):

A RIF is a comprehensive, site-specific reference that serves as a decision-making aid to guide an integrated response to a specific NAI (HVT or HPT). The TEW utilizes a standardized template for the development of the RIF. The template defines the fields of information required to complete a RIF. These fields include:

- Site plans
- Terrain analysis
- Weather trends
- Blast analysis
- Interior and exterior plume models
- Maps indicating vulnerable points
- Potential sites for incident activities

A critical component to the RIF is a consequence analysis. Consequence models are developed to aid emergency response personnel in resource and action planning. These models provide a predictive assessment of potential catastrophic incidents associated with vulnerable targets and are significant tools for developing mitigation plans.

Throughout the RIF development process, any information gaps and information requirements should be captured and passed to the collections manager for tasking.

RIFs, also referred to as Target Folders, are site- specific terrain awareness tools. They are a specific, comprehensive reference and decision-making tool to guide integrated emergency response to a specific, high profile target within a specific jurisdiction. A target folder could include site plans, terrain analysis, interior and exterior plume dispersal models, and blast analysis. Maps indicating vulnerable points and potential sites for incident support activities could be included. These are a component of geospatial intelligence (GEOINT) developed for critical infrastructure and public gathering spaces and utilize a standardized format to describe the characteristics of a venue.

IPO Step Two: Describe the Operational Space Effects

Activity II-II: Identify Environmental Factors

Product: Environmental Factor Studies

Activity Information

Summary: Describes environmental aspects and variables within the operational space and determines how these shape conditions and effect friendly and adversary operations.

Inputs: Area Evaluation materials, including critical infrastructure data.

Information from RIF and additional environmental data such as terrain data, weather data, demographic data and calendar items of events adjacent to NAI.

Expected Outcomes: An evaluation of the operational space identifying the key environmental characteristics and effects. A Combined Factors Effects Assessment is produced.

Overview of Typical Steps:

1. Conduct the Terrain Analysis.
2. Conduct the Weather Analysis.
3. Conduct the Geosocial Assessment.
   - Demographics and Culture - Snapshot
     ==> Population
     ==> Age distribution
     ==> Political factors
     ==> Social factors
     ==> General community characterizations
     ==> Education, income and economics
   - Significant Events Calendar.

Concepts Review

Operational Space Environmental Factors:

Terrain and Weather:

The process begins with the *terrain analysis*. The study is best accomplished using aerial imagery that is electronically or manually marked up to highlight the analytical findings.

The tactical terrain studies include, but are not limited to, identifying lines of communication, key terrain, cover, concealment, obstacles and response infrastructure. The weather effects are then identified, primarily noting seasonal patterns and their influences on the jurisdiction. Review page 114 for a more detailed instruction on developing terrain studies.

Geosocial:

The next environmental factor to be assessed is the geosocial aspects of the environment. This includes identifying the demographic and cultural characteristics adjacent to, encompassing, or strategically influencing any NAI. The demographics and cultural analysis includes pulling together recent demographic studies through local census bureaus, community policing programs or other appropriate government agencies in order to identify and understand the most critical and fluid aspect of the environment—the people.

The end-state for demographics and cultural studies is to produce an assessment of the diverse world views and cultural predispositions that exist across the jurisdiction. This “snap-shot” study includes population numbers, age distribution, income groups, socio-economic factors, cultural data and crime data.

Another aspect of the geosocial situation is the *significant* events calendar that identifies important dates, celebrations and memorials that are important to each community.

IPO Step Two: Describe the Operational Space Effects

Activity II-III: Identify Environmental Factors

Product: Environmental Factor Studies (Continued)

Activity Information

`4. Evaluate Global ↔ Local Influences:

- Foreign-national interest threads
- Economic sector threads
- Industry sector threads
- Entertainment sector threads
- Etc…

5. Evaluate *cyber* presence or influences.

6. Examine the *forensic theology* aspect of the communities, identifying and distinguishing belief systems and fundamentals of faith systems.

7. Identify other factors of influence.

Concepts Review

Special events are identified on the calendar, including visits from government officials, foreign dignitaries and other high visibility personalities.

The calendar also includes significant dates that may have attached symbolism considered to be provocative to certain sectors. Finally, the Significant Events Calendar includes all aspects of the environment that follows a regular schedule, such as the annual flu season.

Cultural features including cultural intelligence (CULTINT), as well as theological intelligence (*forensic theology* to discern the authenticity and dissect the semantic content and construction of extremist religious or jihadi communications), are also assessed.

Geospatial intelligence (GEOINT) involves identifying spatial relationships, cultural densities and dispersions, interaction between culture and infrastructure, and recognizing operational opportunities and limitations dictated by the lay of the land on associated features.

Cyber Intelligence (CyberINT) or the exploitation of advanced information systems and social network analysis are then added to the mix. CyberInt is not only intelligence focused on the Internet and information technology but also cyber in that it networks throughout the information environment to fuse and synthesize all aspects of information together. Ultimately, the goal is an understanding of all geospatial and social dynamics, including psychological aspects influencing operations (the combined result being geosocial intelligence).

IPO Step Two: Describe the Operational Space Effects

Activity II-III: Identify Environmental Factors

Product: Environmental Factor Studies (Continued)

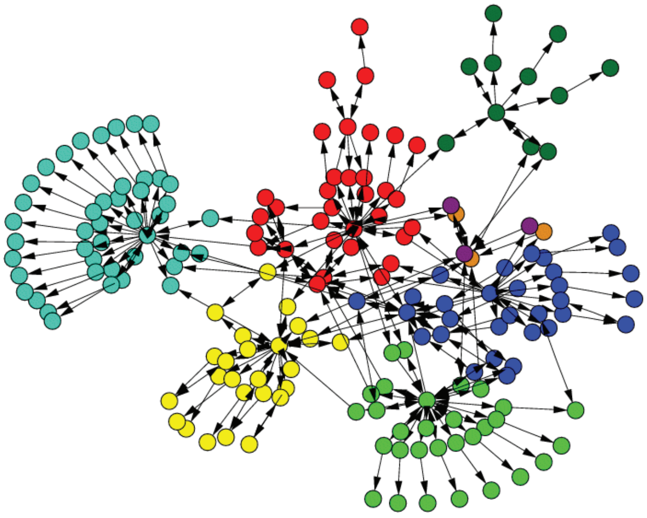
Concepts Review

Global ↔ Local Connections:

Environmental conditions that seemingly would only impact remote corners of the globe can instantly become a driving and influencing element of local conditions as the issues facing foreign communities become manifest in the attitudes and dispositions of a jurisdiction's foreign-national communities.

The jurisdictional demographics study is used to identify sectors of foreign nationals. Countries of origin are noted for each of these sectors, and wedge issues in those countries are evaluated. The evaluation provides a tool for identifying communities where sympathies, grievances or alliances with roots in the home country are still being played out.

The global ↔ local influence assessment continues across as many sectors and sub-sectors as possible, including economic, religious, political and social sectors in order to get a reasonable read on global influences affecting the jurisdiction.



IPO Step Two: Describe the Operational Space Effects

Activity II-III: Identify Environmental Factors

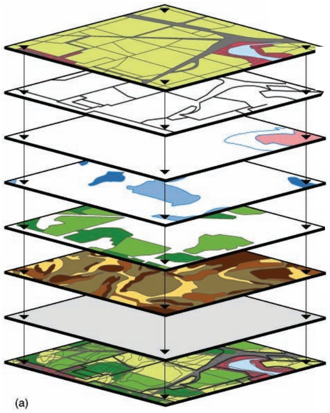
Product: Environmental Factor Studies (Continued)

Concepts Review

Detailed Discussion of Tactical Aspects of Terrain and Weather Study:

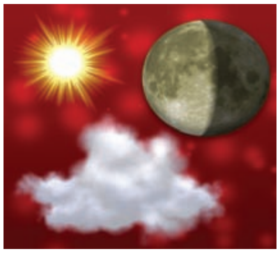
The approach includes a tactical terrain analysis that provides information that could compliment the RIF in the event there was a crisis at one of the NAI. The study is best accomplished using imagery of the area, electronically or manually marked up to highlight the analytical findings. The tactical terrain study includes, but is not limited to, identifying the following aspects of the terrain:

- Lines of communication:
  - o Roads and highways
  - o Inter-structural access and egress
  - o Infiltration avenues – alleys and subterranean passages
  - o Radio dead-space



- Key terrain:
  - o Areas where tactical operations will provide decisive advantage
  - o Cascading access control points (choke points) and associated control sectors
  - o Primary observation points and fields of fire

- Cover or Concealment Obstacles:
  - o Structures, buildings, industrial apparatus



- Response infrastructure:
  - o Fire stations
  - o Police or Sheriff stations
  - o Helicopter Landing Zone study

- Weather:
  - o Climate patterns
  - o Winds
  - o Hazard zones – fire, flooding and slides

The resulting Tactical Aspects of Terrain and Weather includes annotated maps and an assessment of the opportunities and limitations for both friendly forces and threat group activities.

IPO Step Two: Describe the Operational Space Effects

Activity II-IV: Identify Combined Factors Effects

Product: Combined Factors Effects Assessment

Activity Information

Summary: Identifies environmental influences on friendly force and OPFOR activities, as well as on those effecting conditions around NAI.

Identifies existing or approaching economic, political or social conditions of instability, weakness, friction or crisis that an OPFOR could exploit as part of an attack on a physical target.

Inputs: Area Evaluation materials, including Critical Infrastructure data. RIF and all environmental factor studies conducted in the previous activity.

Expected Outcomes: Combined Patterns of Effects and Conditions Study that captures the regularity and frequency of significant environmental factors.

Overview of Typical Steps:

1. Collect previously developed environmental factor products.
2. Evaluate each factor as an isolated variable and identify patterns, frequencies and cycles.
3. Combine all factors and patterns using a matrix format, stacking the patterns of effects on top of one another and spreading the stack across a twelve-month cycle.

   - Evaluate the Combined Factors Matrix and identify high-risk alignments.
   - Record anticipated date windows.
   - Regularly refine and validate the matrix.

Concepts Review

Factors and Effects:

Environmental influences have a significant effect on how events unfold in the Ops Space. Target factors, threat factors and even friendly force response factors are subject to the influences and effects of environmental circumstances.

Environmental factor studies brought forward from the previous activity are combined in order to evaluate the dynamics of these influences and determine what opportunities or limitations may result as these factors combine. When possible, regular cycles or patterns are identified to facilitate forecasting.

The assessment examines how changing conditions combine to influence the character of the Ops Space, for example, how vulnerabilities at potential target sites are impacted, how a terrorist adversary's attack timing and target and weapon selection are influenced, and how friendly force capabilities are impacted. The range of factor combinations examined is not infinite but constrained to reflect the standard ebb and flow of the Ops Space. Typical influences include political events, social attitudes, special dates, weather, seasons, global events, and geosocial issues and their influences.

The assessment produces a *combined factors outlook* that amounts to a snapshot in time of how the factors of environmental effects can come together to alter the threat envelope of certain NAI. This snapshot is reviewed and updated regularly, and impacted NAI are highlighted for closer attention and surveillance measures.

IPO Step Two: Describe the Operational Space Effects

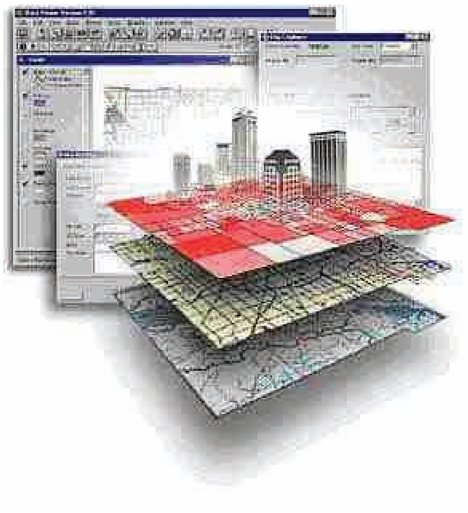
Activity II-IV: Identify Combined Factors Effects

Product: Combined Factors Effects Assessment (Continued)

Activity Information

Overview of Typical Steps (Continued)

4. Using the matrix, develop forecasts of high risk alignments for the next three months.
5. Monitor forecasts, validate or refine the matrix.



Concepts Review

Combined Factor and Effects on Risk:

Risk factors are influenced by environmental conditions that regularly act on them. Population densities shift dramatically over the course of the day, the week, and in accordance with special events. An attack's lethality, then, also shifts during the course of a day or when circumstances create an ad hoc mass-gathering event as witnessed during Hurricane Katrina when tens of thousands of people converged on the football stadium for shelter.

The relationship between terrain and weather conditions is dramatic as well. Depending on soil types, it only takes a little precipitation to completely change the mobility characteristics of the landscape, complicating rescue options if timed appropriately. A HazMat plume, released by a storage facility damaged as a result of an attack on a neighboring site perhaps is affected by wind, rain, temperature and other atmospheric conditions. Properly planned, the HazMat event could be an integral component of a plan seeking to maximize lethality, complicate a response, and further inflame a complex response situation. Assuming the threat actor had the required capabilities to execute this hypothetical attack, the perpetrator only needs to know that the hazard exists, its composition, and what mix of conditions would maximize the material's toxicity or expansion, or both. It is just a matter of selecting the right time and conditions for the attack.

IPO Step Two: Describe the Operational Space Effects

Activity II-III: Identify Combined Factors Effects

Product: Combined Factors Effects Assessment (Continued)

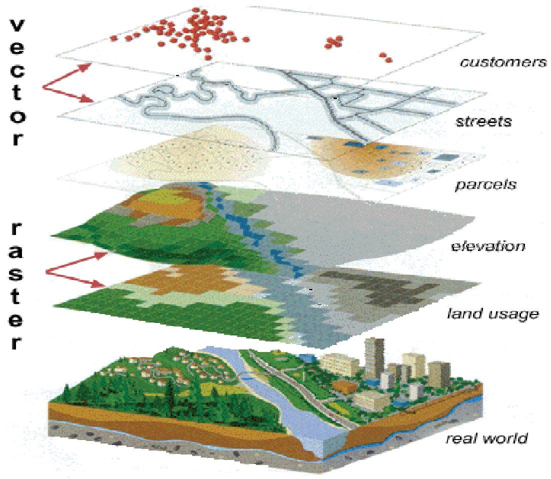
Concepts Review

Combined Factor Effects on Risk (Continued):

Fire season means that area response resources are stretched and the availability of specialty assets may be problematic. Environmental forces can also influence a target's criticality if the appropriate mix of developments occurred, such as a dramatic event in the global market or political landscape resulting in a critical shortage or a loss of a service that people depend on.

For these reasons, a great deal of consideration is given to understanding the influences of environmental factors on each site's risk condition. Consideration is also given to determining optimal environmental circumstances favorable to an attack, determining the pulses and frequency of each contributing factor and estimating convergence cycles.

When the environmental factors offer conditions optimal for achieving amplified attack effects, an *opportunity window* [for attack] exists within the attack-lane. The presence of an opportunity window only means that advantageous conditions are present that could amplify the effects of an attack at that site. An opportunity window available to a threat element with the necessary capabilities to attack the target site is a highly dangerous attack-lane condition.



C. IPO Step Three

IPO Step Three: Evaluate the Threat

Activity III-I: Threat Inventory

Product: Local Potential Threat Elements (PTE) Identified

Activity Information

Summary: Evaluate the Ops Space and determine the local threat elements.

Inputs: Environmental Studies, criminal databases, and current intelligence.

Expected Outcomes: The threat inventory is in a constant state of refinement and improvement.

Overview of Typical Steps:

1. Identify known actors or groups.
2. Identify population densities across the *continuum of relative interest* to identify varying threat density probabilities.
3. Routinely assess global OPFOR activities against developments within local threat densities as part of the Transaction Analysis Process.
4. Identify potential complex threat vectors.

Concepts Review

Threat inventories:

The purpose of the Threat Inventory is to routinely re-assess the threats and OPFOR within the jurisdiction.

The TEW identifies groups and individuals within the region that would pose possible threats. These may include actors with known associations with international terrorist groups, domestic extremists, individuals who have an extreme special interest ideology, or a criminal enterprise.

The threat inventory answers these questions: Who are the people involved? What is their group affiliation, if any, and what do they believe?

The threat inventory also identifies their motives, methods, and targets. With criminal enterprises, the variables are methods, commodities and locations. In either case, understanding how the criminal entity operates and what it seeks to accomplish can provide significant insight into their ability to act.

The TEW threat inventory identifies the potential threat elements (PTE) within the local area. The process endeavors to identify groups or individuals within the jurisdiction whose association with radical, hate and violence-oriented extremists, domestic or otherwise, is known, suspected or considered to be likely in the future. An active threat inventory program, coupled with a *transaction-based* I&W analysis process, is necessary to reduce the likelihood that a previously unknown element will emerge to carry out or support, in any capacity, local attacks. (Continued)

IPO Step Three: Evaluate the Threat

Activity III-I: Threat Inventory

Product: Local Potential Threat Elements (PTE) Identified (Continued)

Concepts Review

Threat Inventory (Continued):

A sophisticated threat inventory results in a PTE social network map indicating jurisdictional, regional, and global connections and transactions between possible threat actors. Within the current threat environment, it is critical that the intelligence effort continue to pursue a better understanding of the global-local-global relationships between threat actors.

These relationships provide the OPFOR, among other things, and its global reach, and facilitates the mobilization and participation of supporters drawn from a wellspring of enthusiastic sympathizers who are already firmly embedded within the local landscape. The analysis of information generated from within the jurisdiction (tactical information), therefore, is always assessed within the context of possible relationships to local PTE activities. Similarly, information related to local PTE activities is also assessed within the context of possible relationships to global developments.

This is particularly important in light of developing trends that indicate the emergence of a collective OPFOR consolidating under the al-Qaeda (AQ) banner and ideology. Disparate terrorist groups, criminal elements and individual sympathizers have united within the context of AQ's fight, particularly their fight against the west, and are actively sharing resources and capabilities.

Complex Threat Vectors Identified:

The TEW recognizes that there are *classes* of threats and terrorist attacks involving highly complex, dynamic, and technical characteristics that may or may not also involve rapidly expanding and highly catastrophic consequences.

The threat inventory, therefore, also identifies complex threat possibilities such as the deployment of Chemical, Biological, Radiological, Nuclear, [High]-Explosive (CBRNE) weapons of mass destruction (WMD) and other highly lethal and/or technical threat possibilities. These are called *complex threat vectors*.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework

Activity Information

Summary: The threat-model process involves developing OPFOR *order of battle* (OOB) data, and using the OOB data for conducting the *Ends-Ways-Means* assessment.

Inputs: Target Inventory, Threat Inventory, Intelligence resources and research.

Expected Outcomes: Threat knowledgebase, OOB files, Threat Framework, Threat-Target Pairs, and Playbooks

Overview of Typical Steps:

1. Develop OPFOR OOB Files.

2. Conduct Ends Assessment.

3. Conduct Ways Assessment:
   - Threat Framework & Kill Chain Models

4. Conduct Means Assessment:
   - Capabilities
   - Critical Vulnerabilities
   - Center of Gravity

5. Conduct Threat-Target Profiling and Pairing.

6. Develop Playbooks.

Concepts Review

Threat Modeling:

Seeks to reduce the uncertainty in answering the first three of these OPFOR-specific questions:

1. (***Ends***) What does the OPFOR "want" to do? – Intentions

2. (***Ways***) How has the OPFOR "done" it [conducted operations] before? – Demonstrated TTP

3. (***Means***) What "can" the OPFOR do? – Resources and capabilities

4. What will the OPFOR "do?" – Threat Course of Action (COA) hypotheses

The Ends-Ways-Means component of threat modeling includes developing *models* used to describe the OPFOR kill-chain processes for planning, mobilizing, and executing attack activities. Threat modeling also facilitates *red-teaming* activities that are often helpful for generating threat COA hypotheses in response to the fourth and final question.

OPFOR activities and other recognizable kill-chain dynamics that are determined to be signature attack precursors are then identified as indicators. Indicators are located within the threat COA and used as part of the I&W intelligence function to anticipate a developing threat situation. OOB, Ends-Ways-Means assessments, threat models and threat COA hypotheses are updated regularly in conjunction with developments in the OPFOR situation.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Order of Battle (OOB) Analysis:

The primary means to characterize the OPFOR is to employ Order of Battle (OOB) analysis. OOB is a breakout of key factors that describe the make-up of any fighting force. Even the highly networked, transnational, unconventional forces such as terrorist organizations can be assessed through the OOB process.

OOB is a methodology for cataloging an adversary's primary war-fighting attributes and establishing an understanding of the kind of war he desires to fight. It is also a means for ascertaining how these attributes contribute to or diminish the force's combat effectiveness. The OOB analysis helps define an adversary's capabilities, strengths and other advantages while at the same time exposing the adversary's vulnerabilities, weaknesses and disadvantages.

OOB Factors:

Composition - Identification and organization of units and political, religious, or ethnic organizations. Unit identification consists of the complete designation of a specific entity by name or number, type, relative size or strength, and subordination.

Disposition - Geographic location of OPFOR elements and how they are deployed, employed, or located. Additionally, disposition includes the recent, current, and projected movements or locations of these elements.

Strength - Conventionally described in terms of personnel, weapons and equipment. In counterterrorism operations, strength as a factor is augmented with attack teams, political cadre or cells, and most importantly, popular support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving logistics, or just withholding information.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

OOB Factors (Continued):

Tactics - Strategy, methods of procedure, and doctrine. Each refers to the OPFOR accepted principles of organization and employment of forces. Tactics also involve political, military, psychological and economic considerations. OPFOR tactics and operations vary in sophistication according to the level of training the individual or organization has received. OPFOR carefully plan and train for individual and small group operations.

Training - The type and depth of individual and group training that operatives receive is tied to their tactics and operations.

Logistics - The effectiveness of OPFOR operations depends heavily on logistics. This dependency fluctuates horizontally and vertically between the various groups and levels of operation.

Combat Effectiveness – OPFOR receiving healthy flow of support, highly motivated stream of recruits, popular sympathies, fear, intimidation, and political power shifts.

Personalities - A critical factor when conducting counterterrorism operations. Attention must be focused on individuals and leaders. OPFOR organizational diagrams can be built through multidimensional link analysis (determining relationships between critical personalities and then their group associations). This applies to virtually any threat represented in counterterrorism operations. Once relationships and the level of contact or knowledge the personalities have are known, many of their activities can be determined.

Culture - Culture is the ideology of a people or region and defines a people's way of life. A people's culture is reflected in their daily manners and customs. Culture outlines the existing systems of practical ethics, defines what constitutes good and evil, articulates the structures and disciplines that direct daily life, and provides direction to establish patterns of thinking and behavior. Cultural issues include, but are not limited to, religion, political and economic beliefs, tribe, clan, ethnicity, regional affiliation, military attitudes, and law and justice.

Miscellaneous Data - Includes supporting information needed but not covered by an order of battle factor.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Ends – Ways – Means Assessment:

The OOB factors are used to organize threat information and build the threat knowledgebase. Once in OOB format, threat information is further scrutinized to see how well capabilities line up with intentions and if there are any exploitable conditions existing in the ranks. This component of threat modeling is called the *Ends-Ways-Means assessment*, and refers to identifying the OPFOR's intentions, methods, capabilities and resources.

Assessing Ends - *What does the OPFOR want to do?*

Answering this question involves an assessment of the adversary's strategic, operational and tactical aims, and then determining how those aims relate to the execution of past attacks. Past shifts in these aims are also noted, as are any contractions or expansions. For each situation involving a changing objective, the circumstances are noted.

Assessing Ways - *How has the OPFOR conducted operations before?*

Describe the methods the OPFOR uses to achieve the desired end-state or objective, arranged in operational phases, tasks and activities when appropriate.

Past attacks by known groups offer an opportunity to learn how those groups' OOB factors are employed during an operation by examining how each group organizes, recruits, equips, trains and deploys for an attack. The *Ways* assessment reviews past attacks, cataloging the processes, methods, timing and sequencing of activities making up the OPFOR kill-chain. Past attacks can also offer opportunities to understand other patterns, such as target selection, weapon preference, relationships with other terrorists or criminal groups, and dependencies on sponsor nations. The assessment, therefore, also identifies the social networks involved in past attacks in addition to examining the key decisions, decision-makers and decision processes. Particular attention is given to the target site and weapon selection, assessing the attributes of the target, noting the impact of timing on the resulting effects of the attack, and determining if the attack achieved the OPFOR's intentions.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Ends – Ways – Means Assessment

Assessing Ways (Continued) -

Threat Framework -The information developed during this assessment is used to generate more depth of understanding of the adversary's operational framework. The threat framework describes the elements of the OPFOR kill-chain. In fact, a primary product developed here is a graphic illustration depicting the kill-chain as a process flow chart along a timeline. The threat framework is used to collect and compile learning points and patterns of behavior discovered after analyzing past attacks.

The framework is a tool that is intended to describe how the OPFOR Order of Battle is arranged in time and space, coordinated and supported, and able to surge or swarm when the moment is right. Threat frameworks are improved over time. They are records of what is learned from regularly assessing an evolving threat. Frameworks of the ex-Soviet military were developed over fifty years in extraordinary detail, but the process of modeling the current threat has only just begun, leaving plenty of gaps in the intelligence knowledgebase. However, even a rudimentary framework model is exceptionally useful when making inferences or developing a threat picture.

The topics in this table represent the *baseline* set of factors that make up a threat framework. Additional framework models are listed in the appendixes.

Organization	Ends	Ways	Means
Weapon Selection	Design	Develop	Delivery
Target Selection	Objectives	Conditions	Effects
Attack	Tactical Organization	Operations	Command and Control
R&S	Assessment	Development	BDA

The development process involves researching past attacks, identifying each of these components and looking for continuity, trends or patterns between the attacks.

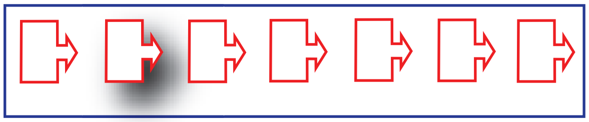
IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Ends – Ways – Means Assessment



Assessing Ways (Continued) -

The Kill-Chain Model – A *kill-chain* describes the arrangement and sequence of activities a threat group uses in planning, organizing, mobilizing, training, equipping and staging – resources and operatives. These activities make up the threat group's modus operandi, its attack system. Further, the kill-chain models are used to identify each threat's critical resources, critical capabilities, critical vulnerabilities, and *center of gravity.*

***Assessing Means** - What can the OPFOR do?*

Identify the critical resources and critical capabilities the OPFOR needs in order to conduct operations described in the kill-chain. The *Means* assessment also identifies the OPFOR Center of Gravity and Critical Vulnerabilities.

The *Means* assessment identifies what the OPFOR is really capable of doing by identifying the mix of core capabilities and resources at their disposal. This includes identifying the key enabling capabilities that are essential to operational success that 1) have been previously demonstrated or 2) have recently emerged. The assessment reviews the OPFOR kill-chain model and examines demonstrated capabilities from past activities, noting what resources where assembled to enable each core capability. The assessment also identifies newly acquired capabilities or attempts by the OPFOR to acquire new capabilities.

OPFOR core capabilities and resources define the range of threat COA options that are examined when answering the final question "What will the OPFOR do?" during the red team assessment. Furthermore, activities inherent to core capabilities are typically selected as indicators and used as key tools for anticipating threats and terrorist attacks.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Ends – Ways – Means Assessment

Assessing Means (Continued) -

The *Means* assessment also provides key insights into the underpinnings of the OPFOR's operational capacity that can be useful for interdiction strategies. The availability of core capabilities and resources are examined during the critical vulnerability and center of gravity analysis.

The Means assessment involves a review of the materials generated through the Ends and Ways assessments, including threat models and kill-chain models in order to isolate and characterize OPFOR core capabilities and required resources.

The following capability sets—standard to military action—provide an initiating guide useful for starting the assessment:

- ❑ Personnel and Staff management – Recruit, train, cross border/global insert and extract, embed, document, equip, arm, instruct or direct, sustain, and hide.

- ❑ Targeting – Target assessment, target selection, target development, recon and surveillance, and deployment.

- ❑ Weapon Handling – Target-weapon pairing, weapon acquisition (buy, steal, borrow weapon or material to design, develop, and deliver a functioning weapon), weapon movement and storage, as well as any noted innovations.

- ❑ Command and Control – Planning, task-organization, communications, simultaneous coordinated operations, intelligence, counterintelligence and OPSEC, deception, and information operations.

- ❑ Logistics - Finance, travel, move things, conduct research, and purchase things.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Ends – Ways – Means Assessment:

Assessing Means –(Continued):

Core capabilities can be assessed in a number of ways, but as a baseline the methodology will include identifying and describing the following elements within each capability:

- ❑ People, knowledge and specialty skills
- ❑ Tactics, techniques, procedures that were defined and understood
- ❑ Organization and structure
- ❑ Equipment
- ❑ Facilities
- ❑ Technology
- ❑ Materials
- ❑ Support

Note: When possible, identify cultural networks and support systems within the support elements.

Center of Gravity and Critical Vulnerabilities - A center of gravity is a source of moral or physical strength, power or resistance that is critical to the OPFOR's ability to execute operations. Critical vulnerabilities are components of the OPFOR's operating system—kill-chain—that are both crucial to the functioning of the system and vulnerable to exploitation.

Following the assessment of core capabilities, the Means assessment then analyzes the total OPFOR picture, the OOB, Ends-Ways-Means, and defines the OPFOR's center of gravity and critical vulnerabilities.

Threat - Target Pairing - Each threat, PTE and terrorist group is assessed in order to establish a *threat-target profile* that is used to pair jurisdictional targets with known OPFOR interests. When these threat-target pairs are identified, an *attack-lane* is said to exist between the two. Information developed during the target assessment and threat management processes provide the tools necessary to develop threat-target profiles, identify the threat-target pairs and conduct the risk-assessment.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Attack-Lanes - An attack-lane, conceptually, describes the unique relationship between a specific threat element and a particular target. It provides a word-picture for seeing jurisdictional targets at one end of a mobility corridor with an adversary force poised at the other end. There is nothing in between but an empty attack-lane stretching from threat to target.

Mobility classifications for attack-lanes provide base criteria for identifying broad threat-target pair priorities. An OPFOR with capability shortfalls regarding a specific target site is not able to progress along the hypothetical avenue of approach at all.

Attack Lane Conditions – Hypothetical mobility characteristics within the attack-lane are determined by the threat-target factor agreement conditions. For example:

- ❑ ***Go Condition -*** When threat-target factors are in synch and environmental conditions have cycled to create an opportunity window, then a "*go*" condition exists within that attack-lane.

- ❑ ***Slow-Go Condition -*** When threat-target factors are in synch but environmental factors are not optimal and, therefore, no opportunity window exists, then a "*slow-go*" condition exists within the attack-lane.

- ❑ ***No-Go Condition -*** When threat-target factors are not aligned, regardless of environmental factors or opportunity windows, a "*no-go*" condition exists within the attack-lane.

Complex Threat Vectors - Threat modeling also examines the complex threat vectors identified during the threat inventory; cataloging the range of CBRNE threat potentials, specifically reviewing the characteristics of each type of weapon system; identifying precursor materials, specialized equipment and facility requirements; and requisite subject matter expertise needed to research, design, develop, store and transport the various weapon components. The material components and special apparatus that produce unique, detectable signatures are also identified.

Complex threat vectors also include emerging, innovative, difficult to detect, and highly dangerous threat scenarios that require additional detailed analysis in order to fully develop prevention and response strategies.

Preventing, deterring or responding to these complex threat classes requires the support of detailed reference protocols that guide the TEW through the technical aspects of threat recognition, outlines critical agency alerting priorities, defines resource requirements and mitigation strategies, and assists the OIC cell determine internal personnel task assignments. The decision-making inherent to situations involving these special classes of threats is most effective when guided by organized references, developed prior to a crisis in a deliberate-planning environment.

IPO Step Three: Evaluate the Threat

Activity III-II: Threat Modeling

Product: Threat Framework (Continued):

Concepts Review

Playbooks - - The TEW uses reference products called *Playbooks* to provide preplanned general guidance for assessing complex threat situations. The TEW utilizes playbooks as an internal analytical guide. They are organized in standard formats for conducting assessments of actual terrorist threats or attacks. They guide TEW assessment activities before, during and after an attack. They identify common considerations and typical intelligence requirements that decision-makers are likely to need. The TEW has developed playbooks for chemical terrorism, biological terrorism, food surety, water supply surety, suicide bombings, large vehicle bombings, laser threats, radio frequency weapons and radiological/nuclear terrorism.

IPO Step Three: Evaluate the Threat

Activity III-III: Threat Integration

Product: Combined Complex Threat Axis and High Impact Threat Scenarios (HIT)

Activity Information

Summary: Combined complex threat arrangements and unique threat axis identified.

Inputs:
Threat model, Threat-Target pairs, Combine Effects Assessment, and Playbooks.

Expected Outcomes: HIT scenarios

Overview of Typical Steps:

1. Identify OPFOR Threat-Target pairs

2. Identify targets most suited for max effects of complex threats – lethality, destructive, disruptive, and impact.

3. Identify complex threat vector targets matching threat-target pairs.

4. Correlate complex threat vectors with OPFOR, targets and conditions, and identify all the possible combinations.

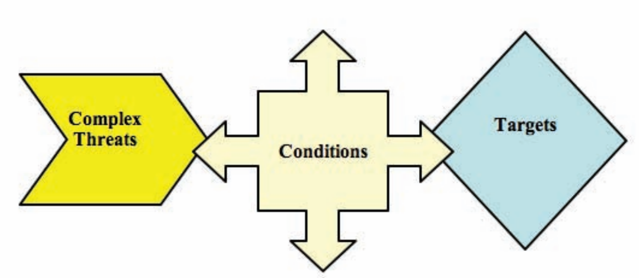
   - First, based on similar targets and conditions.
   - Second, based on similar targets.
   - Finally, based on similar conditions.

Each combined complex threat axis represents a High Impact Threat (HIT) scenario.

Concepts Review

Threat Integration:

Threat integration evaluates potential arrangements of threat axis combinations. The effort begins by identifying the range of potential threat combinations—threat axis—including an OPFOR, possibly one or more complex threat vectors, a target preference, and optimal environmental conditions that, taken together, would pose the greatest catastrophic impact to the jurisdiction. These threat alignments are considered the highest impact threat (HIT) scenarios. HIT scenarios are then taken forward into the threat forecasting process.



D. IPO Step Four

IPO Step Four: Determine Threat Course of Action

Activity IV-I: Threat Forecasting

Product: Threat COA Options (Hypotheses)

Activity Information

Summary: Threat forecasting uses information developed during the threat inventory, threat modeling and threat integration assessments to develop hypotheses regarding OPFOR course of action (COA) options.

Inputs: Threat inventory, Threat modeling, Threat Integration and HIT scenarios.

Expected Outcomes: Most Dangerous and Most likely Threat COA options identified.

Overview of Typical Steps:

1. Identify all possible COA options within HIT scenarios by assessing OPFOR capabilities.

2. Identify, based on available intelligence, which of the COA options are most dangerous and which are most likely.

Note: Evaluating each option's potential lethality and impact assists in determining most dangerous (MD) options, while assessing an option's feasibility assists in determining a most likely (ML) COA option.

Concepts Review

Threat Forecasting:

Threat Course of Action (COA) hypotheses - What will the OPFOR do?

From the HIT scenarios, the threat forecasting effort draws out actual HIT *options*. A scenario is elevated to an option when the OPFOR has the capabilities required to assemble the threat axis and execute the attack. The combinations that are considered the most dangerous are identified as the adversary's most dangerous COA (MD COA) options. Threat combinations that are assessed as *most likely* are then identified as the adversaries ML COA. The result of the threat forecasting is the following three threat axis combinations:

1. Highest Impact Threat (HIT) scenarios.
2. MD Threat COA options.
3. ML Threat COA options.

These threat axis combinations become the basis for subsequent tasks, such as risk-assessment and I&W framework development. Additionally, MD and ML COA options can be further refined through red-teaming to begin formulating hypotheses describing various kill-chain potentials.

IPO Step Four: Determine Threat Course of Action

Activity IV-I: Threat Forecasting

Product: Threat COA Options (Hypotheses)

Concepts Review

Threat Forecasting (Continued):

Whether a red team is used or not, the central threat forecasting activity involves formulating hypotheses of threat COA options. These COA hypotheses are used as the basis for developing situation specific kill-chain models that graphically depict OPFOR actions such as planning, target assessment and selection, weapon development, recruitment and tactical operations along a hypothetical timeline. When complete, the kill-chain model is essentially a graphic forecasting tool, an indicator-mapping tool, and a frame of reference during all-source/all-phase information fusion. When the kill-chain models of an OPFOR are compiled, the result is a comprehensive set of attack plans that include branches and sequels.

The assessment produces graphic attack diagrams to illustrate what the kill-chain would look like if its component parts could actually be seen moving along an attack-lane. This technique allows an analyst to visualize potential timing and sequencing options. The graphic model is not to be confused with factual "ground-truth" but is an analytical tool to help the analyst recognize patterns and relationships between activities. These graphics are called *situation templates*.

A *situation template* normally only depicts a single *kill-chain* along one attack-lane, allowing for an assessment that involves one OPFOR against one target. During the assessment, however, a red-team can be used to identify decisive points in the kill-chain sequence where branch and sequel options may develop, and points where an OPFOR kill-chain may transition into another attack-lane against a different target. The red-team can also identify decisive points in the kill-chain sequence where the OPFOR would employ deception options or where the OPFOR has passed the point of no return.

The one-target-at-a-time kill-chain development does not suggest that an OPFOR will not attack along several lanes, against multiple targets with a single kill-chain (attack). The technique uses the one-to-one approach simply to isolate and identify any potential unique indicators that can be used to recognize a particular target is under attack as early as possible. The one-to-one approach also allows the red team to determine environmental conditions that would be optimal for enhancing the effects of the attack and amplifying the impact. When enough of these conditions are present, there is an opportunity window open for attack. Because of this, the I&W effort also tracks environmental factors, looking for indications that an opportunity window might be emerging.

The goal is to have a set of kill-chain models for each MD and ML COA option, as well as for each of the remaining HIT scenarios, illuminating the range of factors that would have to come together for any of these combined complex threat axis to emerge within an attack lane. With this in mind, the red team incorporates gaming techniques in the COA development process that involve scenarios vignettes exploring interaction possibilities between OPFOR cadre and local PTE. These techniques help provide a frame of reference for assessing local activities.

IPO Step Four: Determine Threat Course of Action

Activity IV-I: Threat Forecasting

Product: Threat COA Options (Hypotheses)

Concepts Review

Red Teaming - Red-teaming involves examining something from the adversary's perspective. Red-teaming activities are used to evaluate physical as well as information security measures. In these situations, a red team or red cell, conducts actual operations against a facility in order to uncover security gaps or other vulnerabilities. Red teams are also useful during exercises to provide a thinking, scheming adversary that can dynamically interact with the exercise participants.

Analytical red-teaming in support of intelligence involves a team of analysts developing attack plans and crafting forecasts from the perspective of the OPFOR. This approach uses role-playing techniques to comprehend nuances, grasp complexities, and actually get a sense for where an OPFOR may be vulnerable to being exposed while conducting hostile actions.

Section 3.3 –
Using the Model

A. Overview:

With the IPO generated intelligence mode—baseline—it is possible to develop a refined appreciation for the true risk to the jurisdiction by using the model within the risk-assessment process and defining the jurisdiction's threat-envelope. It is also possible to develop a refined I&W framework, one that is appropriately postured to detect critical attack precursors.

The threat COA options, the risk assessment, and the I&W framework are all examples of working the intelligence model to generate reason-based tools and together set the stage for the most critical of all the intelligence model uses, the application within the "scanning-transaction analysis-information synthesis-threat recognition" event sequence.

The following section describes using the intelligence model as a tool during risk assessments.

B. Using the Model: Determine the Threat Envelope

Risk Assessment

Identify Target Site Vulnerability and Criticality

Product: Random Anti-Terrorism Measures (RAM), Target Hardening Recommendations

Activity Information

Summary: Risk assessment is a process that determines a target's threat envelope, that is, its relative vulnerability to a specific combined threat axis as well as its relative criticality to the jurisdiction.

Inputs: Threat Forecast: MD & ML Threat COA options and remaining HIT scenario combined threat axis.

Expected Outcomes: Vulnerability assessments, along with RAM/target hardening recommendations and consequence assessments determining a site's criticality, impact and hazard consequences, defines required response resources and determines resource availability.

Overview of Typical Steps:

1. Identify priority target sites, beginning with those within MD Threat COA options and continue through ML Threat COA options until there is an established assessment order.
2. Conduct vulnerability assessment in accordance with local SOP.
   - Analyze results and capture friendly and OPFOR relevant insights.
   - Synthesize new information into the intelligence model.

*Recommend RAMs and target hardening.

Concepts Review

Risk Assessment:

The risk assessment process involves comparing OPFOR capabilities, intentions and patterns of recent attacks (target profile defined during threat modeling) against a potential target to determine the target's vulnerabilities and criticality, and to identify the target's relative threat envelope.

Target Integration -Vulnerability Assessment:

A key component of terrorists' attack planning is the target assessment and selection process. Part of that process involves assessing a potential target site's vulnerabilities and then weighing the risk of failing versus the gains of successfully executing an attack. The goal for the local jurisdiction is to identify the vulnerabilities of potential targets and sufficiently harden them and employ RAMs. The main activities of the vulnerability analysis achieve these ends.

Risk Assessment

Identify Target Site Vulnerability and Criticality (Continued)

Product: Random Anti-Terrorism Measures (RAM), Target Hardening Recommendations

Activity Information

Overview of Typical Steps (Continued):

3. Conduct consequence assessment in accordance with local SOP.
   - Analyze results and capture friendly and OPFOR relevant insights.
   - Synthesize new information into the intelligence model.
   - Develop appropriate recommendations.

Concepts Review

Target Forecasting Consequence Assessment:

Targets are assessed during risk assessment to determine potential consequences of a threat or terrorist attack. The assessment determines the impact of an attack in terms of localized deaths and injuries, characterizes the scope and magnitude of a required response, and evaluates the target's criticality to the jurisdiction.

C. Using the Model: Develop the I&W Framework - Collection Mapping

I&W Framework - Collection Mapping

Indicators and Warning

Product: Indicator List

Activity Information

Summary: Kill-chain models are used to identify events, conditions or activities that represent alerting triggers to significant developments that may include an emerging threat situation.

Inputs: Kill-chain models for MD and ML Threat COA options and risk-assessment related indictors.

Expected Outcomes: List of indicators that correspond with MD and ML Threat COA options.

Overview of Typical Steps:

1. Assess each kill-chain for signature events, conditions or activities.
2. Identify indicators by order of magnitude on the Indicator list (relative value of the indicator) using whatever convention is appropriate.
3. Example of one method:
    - High level indicator – high probability of attack.
    - Med level indicator – attack scenario is one of many possibilities, but several appearing raise threshold.
    - Low level indicator – highly inconclusive, but serves as a trigger to develop close watch on events.
4. Identify confirmation or validation events, conditions or activities for each indicator.

Concepts Review

Indications and Warning (I&W):

I&W is defined by a rigorous analysis process that includes both threat modeling and red-teaming potential threat elements against likely target sites. The results of the analysis yield a set of potential threat forecasts. Forecasts are then broken down into likely indicators that can be tracked through an analysis and synthesis process. The I&W process is made up of three component tasks: 1) identifying the activities, signals, signs, queues and triggers that make up the indicators and warning set; 2) matching the I&W to information resources; and 3) routinely scanning the information stream for I&W.

I&W is developed to provide pre-planned alerting triggers for the following general conditions:

- Environmental factors and threat group capabilities and intentions are aligned or moving in that direction, indicating a threat opportunity has emerged or may soon emerge. *(Attack Lane I&W)*
- Threat group activities appear to be consistent with one or more elements of an attack effort (planning, resource mobilization, recruiting, etc), indicating an attack may be coming together. *(Kill-Chain I&W)*
- Threat group activities that suggest a growing interest or direct efforts to acquire the materials, facilities, equipment or expertise associated with a WM, indicating an attempt to acquire, design or develop a WMD. *(WMD I&W)*

I&W Framework - Collection Mapping

Indicators and Warning (Continued)

Product: Indicator List

Activity Information

Overview of Typical Steps (Continued):

5. Evaluate each indicator for "micro-elements."
   - Activities, conditions, developments, and/or events that make up each indicator.
   - Drill down even further to identify the types and categories of transactions that would make up a signature of each respective component activities, conditions, developments and/or events.
6. Develop the indicator-tree for each indicator.
7. Compile indicators in a matrix for easy reference during scanning.

Concepts Review

Activities, mannerisms, appearances, and identifiable signatures of people, equipment or weapons that public safety official at a potential target site can look for to detect a possible attack *(Last chance I&W)*.

The kill-chains developed in the previous task are used to identify *indications and warnings*. . Attack variables–activities and environmental conditions—identified during the red-teaming are evaluated to identify component factors that can be monitored. These are trigger events or developments that help develop the threat picture as they offer patterns useable for making reliable inferences.

Indicator-Trees:
As the indicators are identified, an indicator list is developed that catalogs these precursors and makes particular note of any indicators that can be tied to a particular target-site. Indicator lists are then broken out into *indicator-trees* that drill down into each indicator to identify sets of factors, activities, conditions or events that are the component parts of the original indicator. These "micro" elements are the basis for constructing collection strategies. Indicator trees list the activities–*transactions and signatures*—that are tracked during a scanning and *monitoring* process.

The process is continued for each target. With kill-chain models and indicators for each attack lane on the list of targets, the analysts have prepared a hypothetical map of potential avenues of approach that one or more threats may use to descend upon a jurisdiction. .

The critical aspect of this effort is not identifying every option, but being able to recognize key configurations and alignments of activities, conditions and events and being able to negotiate the OPFOR options faster than the OPFOR can develop them.

D. Using the Model: Collection Planning

Collection Planning

Collection Strategy

Product: Information Resource List

Activity Information

Summary: The Collection Strategy is developed through a process that correlates information requirements to information resources.

Inputs: Indicator list and information resources inventory.

Expected Outcomes: Information channel identified that facilitates scanning for indicators.

Overview of Typical Steps:

1. Identify all available information resources.
2. Identify the defining features of each in terms of:

   - Delivery
   - Content
   - Access.

3. Identify the first, second and third order information channels and sources for each information element.

Concepts Review

The Collection Strategy:

After the indicator list is developed, cataloging the potential precursors for an attack at a particular site and then broken out into indicator-trees, the collection strategy can be developed. The collection strategy aims to identify multiple potential information channels for each indicator's "*micro-elements*" listed on its indicator tree.

The strategy development begins by identifying all *available* information resources that TEW analysts have access to, including Open Source Intelligence (OSINT) as well as information channels tied to classified resources, investigations, field units, and the flow of "leads" reported into the TEW on a daily basis.

The collection strategy then looks at each information channel and source and determines its characteristics. The following represent some basic attributes of an information channel and its source:

Delivery –

- Information "push" or "pull"
- Regularity
- Access
- Medium – electronic delivery or download, hardcopy, or voice.

Collection Planning

Collection Strategy

Product: Information Resource List

Concepts Review

Content

- Scope, depth, accuracy, access and reliability of the source.
- Finished or raw intelligence.
- Timeliness of reporting and perishability of the information.
- Relative value and relevance.
- Verification, validation, and corroboration techniques or possibilities.
- Usability –format, controls and classification–easy or difficult to extract.

Access

- Responsive to *Request For Information* (RFI) or content is dictated by subject matter.
- Follow-up interaction, protocols and policies.

By identifying each of these variables, the most effective and efficient combination of resources can be mapped to the appropriate elements on each indicator tree.

For example:

The strategy needs to support the “scan” methodology for tracking I&W that relies on being able to spot key developments in the information stream with minimal false reads. Some resources, therefore, may be identified as first order materials that offer more breadth of coverage and easy parsing, while other materials will be used in second or third order analysis because they offer more depth but are also more difficult to work through.

A collection strategy that has been developed using the IPO methodology is more difficult to construct up-front, but the process results in a focused and precise I&W effort in which critical intelligence is *mined* out of the information flow.

E. Using the Model: Scanning-Transaction Analysis

Scanning - Threat Recognition

Transaction Analysis

Product: NA

Activity Information

Summary: Information reporting materials are scanned to identify and characterize transaction elements. These transactions are then evaluated for possible threads of continuity possibilities with other transactions in order to identify signatures of a trend or potential.

Inputs: Indicator List and Intelligence Model.

Expected Outcomes: Threat signatures identified.

Overview of Typical Steps:

1. Scan information resource in accordance with the developed colletion strategy.
2. Identify transactions reported across a broad range of source materials.
3. On the reports, circle the transaction and provide it with appropriate attributes (These represent the transaction's "hooks").
4. Where an attribute is unknown, identify it as such, naming that attribute just what it is: a name, a time, a place, etc.
5. List the array of transactions together and identify relationships based on like hooks.
6. Identify transaction threads that form a recognizable signature of a trend (after developing numerous kill-chains, this task will not be difficult).
7. List these threads, even if some transactions are part of multiple competing threads.

Concepts Review

Transaction Analysis-Scanning

The scanning methodology is based on a process called *transaction analysis* that extracts from the information stream the component activities identified on the indicator tree that make up the elements of an indicator.

This process includes aggregating transactions into *transaction-threads* and identifying in those threads possible *signature* activities that suggest an identifiable trend. A trend may take the shape of a pre-identified indicator or it may represent the emergence of unforeseen potentials.

The process seeks to identify the transactional aspect of all activities. A transaction in its most basic form is an event involving multiple key attributes: 1) a connection, 2) an exchange, 3) a purpose, 4) a place, 5) a time, 6) at least one person, and an outcome. Because of these attributes, the transaction view of scanning provides a framework from which analysts can evaluate varying contextual relationships between reports by identifying transactions, keying in on as many of these attributes as possible and then investigating possible relationships to other transactions, identifying possible *transaction-threads* and assessing possible trends within each of the threads.

The key aspect of this analysis technique is that it prompts the analyst to disqualify or modify all previously developed hypotheses in the face of alternate potentials.

Scanning - Threat Recognition

Transaction Analysis

Product: NA

Activity Information

Overview of Typical Steps:

8. Identify tangible reasons to deny each of the threads.
9. List the threads that survive.
10. Revaluate the transaction connections by assessing them in different formats such as complimentary activities, timelines, etc., instead of only assessing like attributes.
11. Repeat the process for identifying threads and ruling them out.
12. Identify any other pattern or phenomena within the transactions.
13. Classify the remaining transaction threads in terms of likely trends.
14. Identify any distinct relationship between the attributes of the trend and any known OPFOR or target-site.
15. If relationships are recognized, identify any tangible reasons to deny the relationship.
16. If the trend survives and the relationship is possible, a potential even horizon has been identified.
17. If no relationship can be found and no reason to deny one can be found either, then this represents an open potential and remains a consideration until proven false.

Concepts Review

The process seeks to identify the transactional aspect of all activities. A transaction in its most basic form is an event involving multiple key attributes: 1) a connection, 2) an exchange, 3) a purpose, 4) a place, 5) a time, 6) at least one person, and an outcome. Because of these attributes, the transaction view of scanning provides a framework from which analysts can evaluate varying contextual relationships between reports by identifying transactions, keying in on as many of these attributes as possible and then investigating possible relationships to other transactions, identifying possible *transaction-threads* and assessing possible trends within each of the threads.

The key aspect of this analysis technique is that it prompts the analyst to disqualify or modify all previously developed hypotheses in the face of alternate potentials.

Regardless of whether the developments observed in the transaction threads were forecasted or not, if the emerging trend and potential points to identifiable threat factors–i.e. known capabilities and intentions of known OPFOR–and these are in line with, or lining up with known target factors–vulnerabilities and impact–it would indicate that a kill-chain is likely advancing down an attack-lane. The analytical effort at this point shifts to identify the range of possibilities, including the possibility of deception.

When an appropriate number of indicators are identified suggesting the emergence of a kill-chain along one or more attack lanes, the scanning effort shifts into monitoring mode.

F. Using the Model: Crisis Action Planning

Rapid Response Planning Process (R2P2)

Situation Specific Intelligence Operations

Product: Threat Development and Warning

Activity Information

Summary: Monitoring activity requires a shift from scanning to a more detailed, focused assessment of the threat situation and occurs when indications extracted from information resources suggest an event horizon for a gathering attack has been recognized, or credible intelligence provided directly into the TEW suggests similar possibilities.

Inputs: Relevant RIF, Playbook, kill-chain, threat model, threat COA option work-up.

Expected Outcomes: Preliminary Net Assessment, situation-specific intelligence model, situation-specific MD and ML Threat COA options, situation specific threat envelope and I&W framework driving information monitoring – transaction analysis, and appropriate warning reports.

Overview of Typical Steps:

1. Develop/disseminate preliminary net assessment.
2. Develop new intelligence model using four IPO steps and pre-packaged 'bridges' RIF, Playbooks, and threat model.
3. Generate MD/ML Threat COA options.
4. Identify threat envelope for relevant targets, noting new insights.
5. Develop situation specific I&W framework.
6. Develop collection plan (include tactical R&S).
7. Monitor information stream for new developments.
8. Disseminate warning as appropriate.

Concepts Review

Monitoring:
During monitoring, the possible attack-lanes and kill-chains are reassessed, Threat COA options are updated, and the collection plan is refined to increase resolution on the potential developments. Hypotheses are inferences and forecasts that classify the range of potential OPFOR options and are the basis for initiating the planning for prevention and deterrence actions.

Advisories:
A TEW product issued to provide information on potential global or national threats (that are non-specific, low credibility and/or uncorroborated), tactics, techniques and procedures (TTPs) that may be used by terrorists (i.e., modus operandi information), and information on operational security (OPSEC) or officer safety value. Advisories are designed to raise awareness and support training and familiarization objectives. Advisories can be issued during all five national Homeland Security Advisory System (HSAS) levels.

Alerts:
A TEW product issued when there is a specific, verified and validated increased threat of terrorism to the United States. These will include potential attacks against US interests abroad or within the United States (particularly locally or adjacent states). Alerts may impact a TEW's operations, but a specific named target within that TEW's area of operations is not known or specified. Alerts will generally be issued during Elevated (Yellow) or High (Orange) HSAS levels.

Warnings:
A TEW product issued when there is a credible verified and validated specific threat to persons or venues (specific sites, events or critical infrastructure) within a TEW's area of operations or an adjacent jurisdiction if local resources are expected to become involved in a mutual aid response. Warnings will always be accompanied by specific response planning steps and recommended course of action options for response. Warnings will be issued during a Severe (Red) HSAS level.

G. Using the Model: Decision Support

R2P2 – Decision Support

Develop Decision Support Intelligence

Product: Net Assessment and Mission Folders

Activity Information

Summary: Develop the net-assessment to provide comprehensive situation intelligence to key jurisdictional decision makers. Develop Mission Folders to provide resource inventories and COA recommendations.

Inputs: New Intelligence Model, Current situation, RIF, Playbook, Threat Model, New MD/ML Threat COA options, new threat envelope.

Expected Outcomes: Timely, accurate, and relevant Net Assessment and Mission Folder.

Overview of Typical Steps:
The net-assessment is prepared in accordance with the current template. The following elements of information are examples of what would typically be included:

1. Develop threat and incident situation information.
2. Categorize threat and OPFOR attack hypothesis if attack has not occurred.
3. Describe attack and consequence possibilities if attack has occurred.
4. Develop comprehensive description of chain of events.
5. Develop assessment of event scope and magnitude.

Concepts Review

NetAssessment:

The *net assessment* provides the UCS and Emergency Managers in the EOC with situational intelligence, threat course of action forecasts, hazard consequence forecasts, resource availability/requirement profiles and outlines Random Antiterrorism Measures (RAMs).

The net assessment process is focused on describing the scope, magnitude and potential impact of an event and is a critical resource for *consequence mitigation*. Feeding off critical site information drawn from the site's RIF, net-assessments provide a description of the current threat envelope and becomes a decision support resource for both emergency responders and emergency managers.

R2P2 – Decision Support

Develop Decision Support Intelligence

Product: Net Assessment and Mission Folders

Activity Information

Overview of Typical Steps (Continued):

Develop Mission Folder in accordance with current template.

1. **A completed Mission Folder includes the following elements:**
   - Written situation brief.
   - Clear, concise mission statement.
   - Clearly worded (recommended) commander's desired end state.
   - Rules of engagement (ROE), restraints, constraints and assumptions.
   - Resource availability/capability matrices.
   - Complete intelligence annex.
   - Collection plan worksheet.
   - RIF/Target Folder (if available, otherwise developing a "spontaneous" target folder (or folders) from the template).
   - Archival/technical information,
   - Maps, schematics, photos, and IPO templates.
   - Investigatory status.
   - Intelligence estimate (for the next operational period), including Intelligence summaries/situation reports to date.
   - Detailed potential courses of action (OPFOR and friendly).
2. **Ensure proper and immediate dissemination.**

Concepts Review

Mission Folder:

The Mission Folder is incident-specific, combining pre-incident intelligence preparation (playbooks and response information/target folders) with time sensitive threat information. A "Mission Folder" is designed to provide the Unified Command Structure (UCS), field Incident Commanders (IC), staff at Operation Centers, and commanders of follow-up resources with the detailed intelligence information. This includes situation and resource status, scene/location information, and a general concept/COAs for making decisions that will resolve a complex incident.

Section 3.4 - Operational Conditions (Phases of Emergency)

A. Pre-Attack Operations:

During pre-attack conditions, Target Assessment and Threat Management preparations are early priorities that transition to an emphasis on the I&W as local critical infrastructure assessments are completed, targets are identified and reinforced, and an understanding of the local threat envelope matures.

Terrorism depends on surprise. With it, a terrorist attack has the potential to do massive damage to an unwitting and unprepared target. Without it, the terrorists stand a good chance of being thwarted by authorities, and even if they are not, the damage from their attacks is likely to be less severe.

Reducing uncertainty in pre-attack conditions relies on eight interrelated but distinct categories of intelligence analysis and production.

Tactical Threat Analysis - Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their current and potential activities allow the government to take immediate and near-term action to disrupt and prevent terrorist acts and to provide useful warning to specific targets, security and public safety professionals, or the general population.

Strategic Threat Analysis - Developing a deep understanding of the organizations that may conduct terrorist attacks against the United States is also essential. Knowing the identities, financial and political sources of support, motivation, goals, current and future capabilities, and vulnerabilities of these organizations will assist in preventing and preempting future attacks, and in taking long-term actions that can weaken support for organizations that seek to damage local interests. Intelligence can support the long-term strategies to defeat terrorism by understanding the roots of terrorism overseas.

Vulnerability Assessments - Vulnerability assessments must be an integral part of the intelligence cycle for homeland security issues. They allow planners to project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government. These projections allow authorities to strengthen defenses against different threats. Such assessments are informed by the use of tools such as computer modeling and analysis.

Risk Assessments - Mapping terrorist threats and capabilities—both current and future— against specific facility vulnerabilities will allow authorities to determine which organizations pose the greatest threats and which facilities and sectors are most at risk. It will also allow planners to develop thresholds for preemptive or protective action.

Tactical Preventive Actions - Analysis can, and must, be turned into action that prevents terrorists from carrying out their plots. This analysis and assessment will help support and enable the actions taken by local law enforcement to prevent terrorism.

Warning and Protective Action - Inclusive and comprehensive analysis allows the local government to take protective action and to warn appropriate sectors and the public. Defensive action will reduce the potential effectiveness of an attack by prompting relevant sectors to implement security and incident management plans. In addition, defensive action works as a deterrent to terrorists weighing the potential effectiveness of their plans. Warnings allow entities and citizens to take appropriate actions to meet the threat, including upgrading security levels in any affected sectors, activating emergency plans, dispatching state and local law enforcement patrols, and increasing citizen awareness of certain activities.

Utilize Dual-Use Analysis to Prevent Attacks - Terrorists use equipment and materials to carry out their criminal acts. Such equipment and material can include items such as fermenters, aerosol generators, protective gear, antibiotics, and disease-causing agents. Many of these items are "dual-use" items—they have not just terrorist applications, but also legitimate commercial applications, and can often be bought in the open market.

If suspect dual-use acquisitions are identified, cross-referenced with intelligence and law enforcement databases, and mapped against threat analyses, the local government's ability to detect terrorist activities at the preparation stage will be enhanced.

Employ "Red Team" Techniques - The TEW, working with the intelligence community, utilizes "red team" techniques to improve and focus defenses against terrorism. Applying intelligence and information, the TEW has personnel responsible for viewing the Operational Area from the perspective of the terrorists, seeking to discern and predict the methods, means and targets of the terrorists. Today's enemies do not think and act in the same manner as yesterdays. The red team uses its capabilities and analysis to learn how they think in order to set priorities for long-term protective action and "target hardening." Employing "red team" tactics, the TEW seeks to uncover weaknesses in the security measures at local critical infrastructure sectors during government-sponsored exercises.

B. Trans-attack Operations:

During a Trans-attack condition, Threat I&W activities continue, but the Operational Net Assessment objective becomes the main effort as critical intelligence is developed to support field commanders and emergency managers. Threat I&W activities continue by looking forward to the next several operational periods to identify indications of future attacks.

Additionally, as in all incidents, WMD incidents may involve mass casualties and damage to buildings or other types of property. However, there are several factors surrounding WMD incidents that are unlike any other type of incidents that must be taken into consideration when planning a response.

First responders' ability to identify aspects of the incident (e.g., signs and symptoms exhibited by victims) and report them accurately will be key to maximizing the use of critical local resources and for triggering a Federal response.

1. The situation may not be recognizable until there are multiple casualties. Most chemical and biological agents are not detectable by methods used for explosives and firearms. Most agents can be carried in containers that look like ordinary items.

2. There may be multiple events (e.g., one event in an attempt to influence another event's outcome).

3. Responders are placed at a higher risk of becoming casualties. Because agents are not readily identifiable, responders may become contaminated before recognizing the agent involved. First responders may, in addition, be targets for secondary releases or explosions.

4. The location of the incident will be treated as a crime scene. As such, preservation and collection

of evidence is critical. Therefore, it is important to ensure that actions on scene are coordinated between response organizations to minimize any conflicts between law enforcement authorities, who view the incident as a crime scene, and other responders, who view it as a hazardous materials or disaster scene.

5. Contamination of critical facilities and large geographic areas may result. Victims may carry an agent unknowingly to public transportation facilities, businesses, residences, doctors' offices, walk-in medical clinics, or emergency rooms because they do not realize that they are contaminated. First responders may carry the agent to fire or precinct houses, hospitals, or to the locations of subsequent calls.

6. The scope of the incident may expand geometrically and may affect mutual aid jurisdictions. Airborne agents flow with the air current and may disseminate via ventilation systems, carrying the agents far from the initial source.

7. There will be a stronger reaction from the public than with other types of incidents. The thought of exposure to a chemical or biological agent or radiation evokes terror in most people. The fear of the unknown also makes the public's response more severe.

8. Time is working against responding elements. The incident can expand geometrically and very quickly. In addition, the effects of some chemicals and biological agents worsen over time.

9. Support facilities, such as utility stations and 911 centers, along with critical infrastructures, are at risk as targets.

10. Specialized state and local response capabilities may be overwhelmed.

The TEW’s role in response situations is to ensure the Unified Commander and the OA EOC receives critical situational and resource related information, as well processed intelligence, both of which are intended to facilitate emergency response, ensuring the parameters of on-site hazards are identified and protective measures recognized.

This role is accomplished through the development of several interrelated information and intelligence products.

The Response Information (Target) Folder (RIF) - An information package produced for each potential target identified during the target assessment process and prepared prior to an incident. The RIF is a package of information materials that provide critical intelligence about the site. The RIF lists each site’s organic hazards, provides pre-developed contingency planning aids such as consequence models and resource guides. The RIF is a critical tool for helping responders rapidly develop situational awareness. (The RIF is addressed in more detail in parts four and five.)

Net Assessments - The *net assessment* provides the UCS and Emergency Managers in the EOC with current situational intelligence, threat course of action forecasts, hazard consequence forecasts, resource availability/requirement profiles and outlines Random Antiterrorism Measures (the net assessment is addressed in more detail in parts four and five).

Mission Folder – This is also an incident specific intelligence product, combining pre-event intelligence preparation (playbooks and RIFs) with time sensitive threat information, providing the UCS with a set of friendly force *Course of Action* (COA) recommendations (the mission folder is addressed in more detail in parts four and five).

C. Post-attack Operations:

Following a terrorist attack, as the emergency moves into the recovery phase, the TEW continues the net assessment effort, but the emphasis returns to I&W activities.

D. THREAT LEVELS:

Additionally, underlying the continuum of operations is a threat level hierarchy meant to trigger specific activities characterized by heightened vigilance, increased security and enhanced preparedness based on threat I&W derived from national, state or local sources that suggest such activities are required.

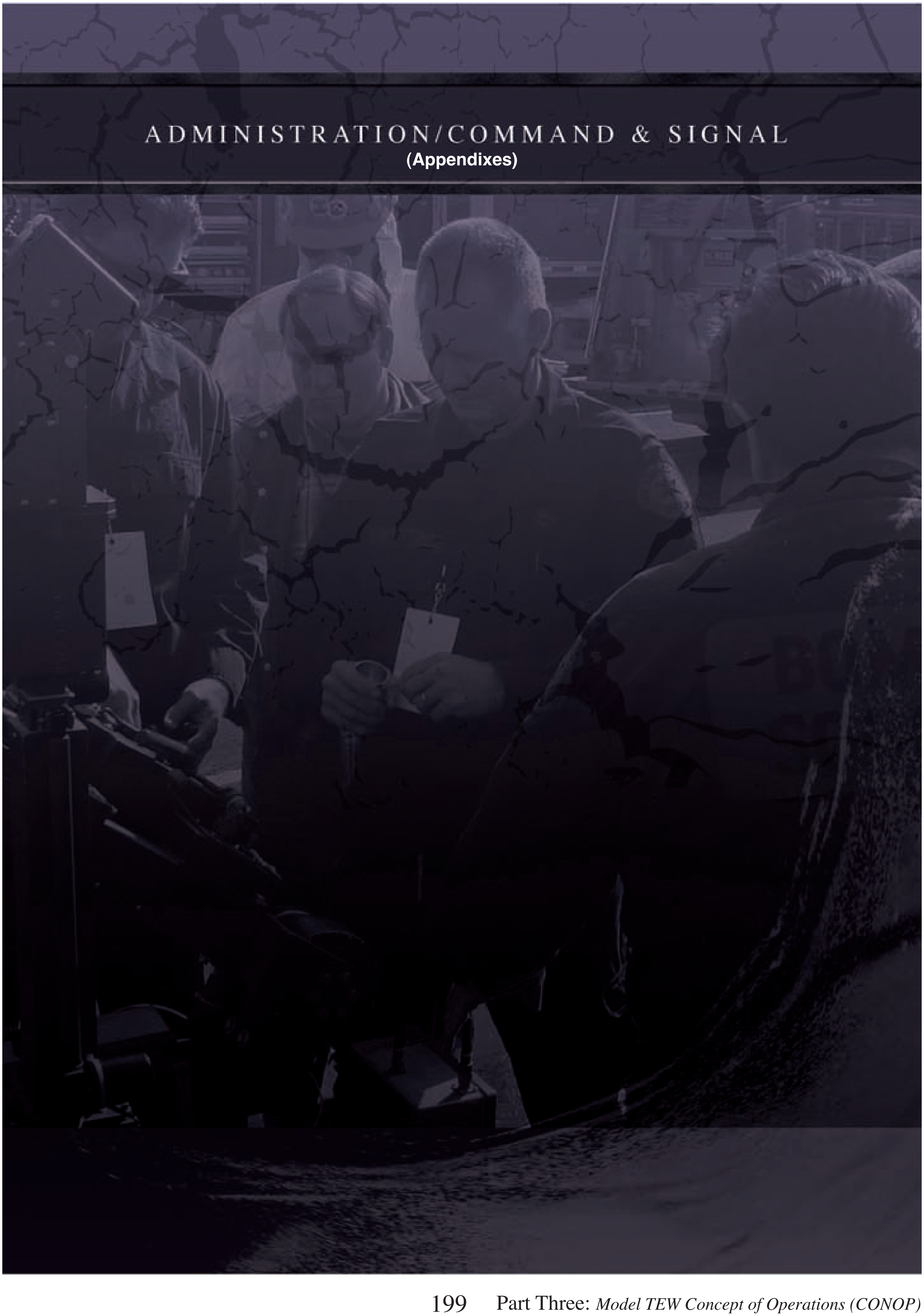
Threat levels are tied to the Homeland Security Advisory System (HSAS). A HSAS threat level increase can be issued to a specific population sector, infrastructure type, region or more broadly applied to the entire nation based on the National Command Authority's assessment of the relevant intelligence. Additionally, a threat level increase can be tied to intelligence developed locally that describes a shift in the local threat environment.

The threat picture underpinning the threat level increase will dictate which activities take priority in the TEW. As a general rule, under circumstances where there is an increase in the threat level, the TEW will work in collaboration with other TEW organizations, regional threat intelligence centers and federal agencies to develop an assessment of the threat and identify the implications/impact to the local area. Such activities include the following:

- ❑ Net Assessment to identify threat type and group
- ❑ Review Playbooks
- ❑ Develop initial threat forecasts
- ❑ Identify potential target sets
- ❑ Update RIFs
- ❑ Pre-format Mission Folders
- ❑ Conduct updated risk assessments
- ❑ Recommend target-hardening strategies and Random Anti-terrorism Measures (RAMS)
- ❑ Identify response resource shortfalls
- ❑ Refine threat forecasts
- ❑ Adjust the I&W –develop collections strategy—to match the emerging threat picture
- ❑ Maintain situational awareness.

ADMINISTRATION/COMMAND & SIGNAL

(Appendixes)



Appendix A –

SUMMARY OF KEY LAW ENFORCEMENT PHASES/WMD Actions

PRE-INCIDENT PHASE	TRANS-INCIDENT PHASE	POST-INCIDENT PHASE
INTELLIGENCE Through national asset identify real and potential international, national and local threat organizations and/or individuals. ***PLANNING*** FBI Nuclear Incident Contingency Plan. FBI Chemical/Biological Incident Contingency Plan. ***PREPAREDNESS*** NBC Training. Interagency coordination and organizational interface. ***THREAT ASSESSMENTS*** Installations/sites/facilities. Nuclear Assessment Program. Critical/Incident Response Group (CIRG). Communicated Threat Assessment. Technical Description Assessment. Operational Capability. Behavioral Threat Assessment. ***DETER*** Through public information and other means make the know price for terrorist activity too high to pay. ***CREDIBLE THREAT RESPONSE*** **FBI Crisis Management** (Readiness Levels 5 through 1) Coordination with President, NBC, applicable federal, state, & local officials. DOJ (FBI) as lead LFA, directs appropriate response and deployment of required federal response assets. ***DETECT*** Conduce surveillance, search, and other LLEA activities using national specialized teams & equipment. ***INTERDICT*** Apprehend & arrest perpetrators and recover, safeguard, & analyze NBC weapons or related materials taken from the perpetrators, if possible. ***PREVENT*** Where possible, prevent detonation or release of NBC or related materials.	***RESPONSE (In the event of NBC release) NBC Incident*** Time of incident, with or without witness observation (actual or estimated). ***Discovery & Notification*** Time of discovery, if incident was not observed. Time of notifications to IRF or CNN News Break. ***INITIAL RESPONSE*** (IRF/Local First Responders) (See the Emergency Management Summary for Details Pertaining to Initial Response.) Preserve & protect the incident site for investigators, when possible. Perform witness interviews. Upon arrival, coordinate access & entry to site for forensic investigators. Establish a database of information for developing SITREPs, Media Briefings, & After-Action Reports. ***FOLLOW-ON RESPONSE*** (Under FBI as LFA) ***FEMA Consequence Management*** Arrival & interface, receive formal briefing from IRF. Formally assume responsibility from IRF. Establish & operate a JOC. Establish & operate a JIC. Perform Hazards Assessment activities (FRMAC). Perform administrative & support functions. ***PERFORM NBC MITIGATION ACTIVITIES*** Employ specialized detection, monitoring, medical, decontamination and other teams. Weapon recovery, if applicable. (See the Emergency Management Summary for Details Pertaining to Emergency Response Deactivation). When incident scene is stabilized and contaminated areas are identified and marked, consider transition. ***INITIATE INVESTIGATION & ACTIONS TO APPREHEND PERPETRATOR***	***INVESTIGATE, APPREHEND & PROSECUTE*** Review evidence, follow-up on leads, and investigate suspect individuals and organizations. Upon apprehension of perpetrators, pursue legal/judicial activities, and prosecute through conviction sentencing and appropriate punishment. ***RECOVERY & SITE RESTORATION*** Near-Term Activities Formally convene the SRWG. Establish a recovery organization. Work contamination fixing & resuspension issues, if appropriate. Transition the JOC to the DFO. Develop a database for long-term monitoring. Develop onsite & offsite Characterization Plans. Implement and document planned activities. Continue to provide progress reports to the media and participating and concerned organizations. Address the transfer of the FRMAC from DOE to EPA. Work the funding & legal issues. ***Long-Term Activities (Site Monitoring)*** Develop a Site Monitoring Plan after site restoration is completed. Monitor onsite & offsite locations in accordance with the Site Monitoring Plan. Continue monitoring until federal, state, & local authorities agree to terminate monitoring. Prepare & maintain formal documents (EPA & state, as required). LFA and/or state must continue budget requests in annual submissions for funding. **NOTE:** This table addresses key (major) activities only. Activities may occur concurrently or in any order. The alignment of activities under the Pre-, Trans- & Post-phases is for planning purposes and may change based on the requirements of actual emergency response.

Appendix B –

SUMMARY OF KEY EMERGENCY MANAGEMENT PHASES/WMD Actions

PRE-INCIDENT PHASE	TRANS-INCIDENT PHASE	POST-INCIDENT PHASE
PLANNING ***Emergency MGT. Program Planning*** Policy & Guidance (Requirements Identified). Hazard Assessment (Credible Threats). Emergency Plan development & processing. Coordination with tasked organizations. Logistics Planning (including Facilities / Equipment / Supplies / Vehicles, etc.). Administrative Planning (inclu. Budget). Quality Assurance Planning. ***Emergency Response Procedures / Checklists*** Develop & processed through approval. User friendly job aides (used as mind tweakers). Updated & maintained. Immediately available. ***PREPAREDNESS Emergency Facilities*** EOC, team & equipment facilities, vehicles, etc. ***Logistics*** Establish requirements for & maintain emergency equipment (including communications), supplies & vehicles in operable status. Inventory & Resupply. ***Training (Knowledge, Hands-on & Performance)*** Formal, plan based, & formally documented. General & Responder (Indiv. & Team) oriented. ***Drills*** Training function to prepare ERO in specific tasks. ***Exercise*** Evaluating function to document demonstrated ERO emergency response capability. ***Assessment / Evaluation*** Self-evaluation and assistance visits. Provides appraisal of the emergency management program to complement evaluation of the ERO. Together, the program appraisal & the ERO emergency response exercise evaluation, determine the total emergency response capability.	***RESPONSE Incident*** Time of incident, with or without witness observation. ***Discovery & Notification*** Time of discovery, if incident was not observed. Time of notifications to Initial Response Force (IRF) or CNN News Break. ***INITIAL RESPONSE*** ***IRF & Initial Crisis Management*** Notify Initial Responders (Fire, Medical, Security, etc.) Assess the hazards, use appropriate PPE, & perform rescue & life saving operations. Establish command, control & communications. Establish a security cordon & NSA/NDA, if needed. Assess the situation, perform consequence assessment, direct Protective Actions (PAs) onsite, & recommend PARs off site. (Preplanned default of JHEC calculated.) Mitigate the emergency situation. Make formal notifications (off site & up channel). Activation& deployment of Federal Response Assets. Preserve & protect the incident site for investigators, when possible. Establish a database of information for developing SITREPs, Media Briefings, & After Action Reports. ***FOLLOW-ON RESPONSE*** (FBI is LFA) ***Crisis Management & Initial Consequence Management*** Arrival & interface, receive formal briefing from IRF. Formally assume responsibility from IRF. Establish & operate a JOC. Establish & operate a JIC. Establish a Joint Legal/Claims Office (JLCO). Perform hazards analysis activities (FRMAC). Perform administrative & support functions. ***Weapons Recovery*** Perform EOC/ARG reentry. Weapons Recovery Plan & safety operations. Weapon Packaging & Transportation Plans. Formal transfer of custody & transport. ***Emergency Response Deactivation*** Develop emergency response termination criteria through SRWG. Prepare a Recovery Turnover Plan/Agreement. Formal transfer from LFA to Federal Coordinating Officer (FCO). Notification of transfer to all involved authorities. Reports prepared, released, & returned to home station.	***RECOVERY & SITE RESTORATION (CONSEQUENCE MANAGEMENT)*** **Near-Term Activities** Formally convene the SRWG. Establish a recovery organization. Work contamination fixing & resuspension issues, if appropriate. Transition the JOC to the Disaster Field Office (DFO). Develop a database for long-term monitoring. Develop onsite & offsite Characterization Plans. Implement and document planned activities. Continue to provide progress reports to the media and participating and concerned organizations. Address the transfer of the FRMAC to EPA. Work the funding & legal issues. ***Long-Term Activities (Site Monitoring)*** Develop a Site Monitoring Plan after site restoration is completed. Monitor onsite & offsite locations in accordance with the Site Monitoring Plan. Continue monitoring until federal, state, & local authorities agree to terminate monitoring. Prepare & maintain formal documents (EPA & state, as required). LFA and/or state must continue budget requests in annual submissions for funding. **NOTE:** This table addresses key (major) activities only. Activities may occur concurrently or in any order. The alignment of activities under the Pre , Trans & Post phases is for planning purposes & may change based on the requirements of actual emergency response.

Appendix C – glossary

A

Advisories: A TEW product issued to provide information on potential global or national threats (that are non-specific, low credibility and/or uncorroborated), tactics, techniques and procedures (TTPs) that may be used by terrorists (i.e., modus operandi information), and information on operational security (OPSEC) or officer safety value. Advisories are designed to raise awareness and support training and familiarization objectives. Advisories can be issued during all five national Homeland Security Advisory System (HSAS) levels.

Agro terrorism: Agro terrorism is the malicious use of plant or animal pathogens to cause devastating disease in the agricultural sector. It may also take the form of hoaxes and threats intended to create public fear of such events.

Alerts: A TEW product issued when there is a specific, verified and validated increased threat of terrorism to the United States. These will include potential attacks against US interests abroad or within the United States (particularly locally or adjacent states). Alerts may impact a TEW's operations, but a specific named target within that TEW's area of operations is not known or specified. Alerts will generally be issued during Elevated (Yellow) or High (Orange) HSAS levels.

Anarchist: Anarchist terrorists are opposed to all forms of government. Anarchists are often allied with Leftist groups.

Anti-Abortion: Anti-abortion terrorists commit acts of terrorism against abortion providers and supporters of the "pro-choice" movement. Typically motivated by religion in their opposition to abortion, these terrorists frequently target abortion clinics and doctors.

Anti-Globalization: Anti-globalization terrorists oppose the increasing integration of the world into a single free market. They believe that the impact of global capitalism on both the average individual and national culture is negative. Anti-globalization terrorists most often attack corporate and U.S. targets.

B

Bioterrorism: Bioterrorism is the intentional use of microorganisms or toxins derived from living organisms to produce death or disease in humans, animals, or plants.

C

Cadre: A cell of trained personnel around which a larger organization can be built, or a member of such a group, the term cadre is often used to refer to an armed member of a militant or terrorist organization.

Capabilities and Intentions: The portion of the indication and warning cycle which deals with the specific operational capacity (capabilities) and objectives (intentions) of a terrorist group to conduct an attack. This portion of the cycle includes criminal intelligence.

Chemical Agents: Chemical agents are poisonous gases, liquids, or solids that have toxic effects on people, animals, or plants. Severity of injury depends on the type and amount of the chemical agent used and the duration of exposure. Chemical weapons include nerve agents, blister agents, blood agents, choking agents, incapacitating agents or any toxic industrial chemical (TIC) utilized as a weapon.

Civil Support Team (CST): On March 17, 1998, Secretary Cohen announced the creation of 10 Rapid Assessment and Initial Detection (RAID) units to enhance the Defense Department's ability to respond to domestic incidents involving weapons of mass destruction. The WMD program began with the creation of 10 Civil Support Teams (CSTs) - formerly called Military Support Detachment (MSD) Rapid Assessment Initial Detection (RAID) teams. The unit's mission is to support civil authorities at a domestic CBRNE incident site by identifying CBRNE agents/substances, assessing current and projected consequences, advising on response measures, and assisting with appropriate requests for additional support.

Consequence Management: Consequence management is predominantly an emergency management function, and it includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. Consequence management is also used in natural disasters, man made disasters, civil unrest, etc. It isn't limited to terrorism.

Counterterrorism: Any political, military, social, economic, psychological, or law enforcement efforts to neutralize, deter, or prevent terrorism. Counter-terrorism can emphasize military defeat of terrorists by thwarting attacks or physically eliminating groups or their ability to attack. Counter-terrorism can also emphasize removing motivations that commonly convince people to become terrorists.

Crime Prevention Through Environmental Design (CPTED): CPTED is a strategy for lowering the incidence of criminal or terrorist activity through proper design and effective use of a particular physical environment.

D

Domestic Terrorism: Incidents perpetrated by local nationals against a purely domestic target.

E

Emergency Operations Center (EOC): An emergency operations center (EOC) is the site from which civil government officials (municipal, county, state, and federal) exercise direction and control in an emergency.

Event Horizon: The event horizon is the foreseeable future within a crisis or emergency incident. The impact of the event and its consequences can be interpreted as the event horizon based upon an understanding of what occurred, the resources available to manage the event, the potential actions of an adversary, and the impact of response and mitigation actions during the course of response activities.

H

Hazardous Materials: Hazardous materials are any substance or combination of substances that cause or contribute to in increase in mortality, irreversible or incapacitating illness, or pose a present or potential hazard to health safety, or the environment. These include chemical, biological and nuclear agents.

Homeland Security Exercise and Evaluation Program (HSEEP): The Homeland Security Exercise and Evaluation Program (HSEEP) is designed to provide financial and direct support to assist state and local governments with the development and implementation of a state exercise and evaluation program to assess and enhance domestic preparedness. Well designed and executed exercises are the most effective means of testing policies, plans, and procedures; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement.

I

Improvised Explosive Device (IED): A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals, designed to destroy, disfigure, distract or harass. They may incorporate military stores, but are normally devised from non-military components. IEDs are similar to land mines, but are generally home-made and of varying explosive force. The term IED came to public use during the violent insurgency that followed the 2003 U.S. led invasion of Iraq.

International Terrorism: Incidents in which terrorists go abroad to strike their targets, select domestic targets associated with a foreign state, or create an international incident by attacking airline passengers, personnel or equipment.

J

Joint Information Center (JIC): The Joint Information Center (JIC) is established to coordinate the federal public information activities at an emergency site. It is the central point of contact for all news media at the scene of the incident. Public information officials from all participating federal, state, and local agencies should gather at the JIC.

Joint Operations Center (JOC): The Joint Operations Center (JOC) is established by the lead federal agency (LFA) under the operational control of the federal coordinating officer (FCO), as the focal point for management and direction of on-site activities, coordination and establishment of state requirements and priorities, and coordination of the overall federal response.

M

Mission Folder: A mission Folder is incident-specific, combining pre-incident intelligence preparation (playbooks and response information/target folders) with time sensitive threat information. A "Mission Folder" is designed to provide the Unified Command Structure (UCS), field Incident Commanders (IC), staffs at Operation Centers, and commanders of follow-on resources with the detailed intelligence information. This includes situation and resource status, scene/location information, and a general concept/COAs for making decisions that will resolve a complex incident.

O

Open Source Intelligence: Open source intelligence (known as OSINT) is information gathered from non-classified sources such as the news media, the Internet, and databases which when properly analyzed can provide decision-makers with timely and pertinent information on which to base decisions. OSINT can be utilized to provide context and to discern trends and potentials, and to prioritize other intelligence activities

P

Playbook: Playbooks provide preplanned general guidance for assessing a complex situation. The TEW utilizes them as an internal analytical tool. They are organized in standard formats for conducting assessments of actual terrorist threats or attacks. They guide TEW assessment activities before, during and after an attack. They identify common considerations and typical intelligence requirements that decision-makers are likely to need. Playbooks are developed for classes of threat. The LA TEW has developed playbooks for chemical terrorism, biological terrorism, food surety, water supply surety, suicide bombings, large vehicle bombings, laser threats, radio frequency weapons, and radiological/nuclear terrorism

R

Radiological Weapons: Radiological weapons include radiological dispersal devices which are any explosive device used to spread radioactive material; or a simple radiological dispersal device which is any act or container designed to release radiological material as a weapon without an explosion.

Resource Typing: Resource typing is the process of categorizing and describing resources that are commonly exchanged in disasters via mutual aid, by capacity and/or capability. Through resource typing, responder disciplines examine and identify the capabilities of a resource's components (i.e., personnel, equipment, and training).

Response Information Folders (RIFs): RIFs also referred to as Target Folders, are site- specific terrain awareness tools. They are a specific, comprehensive reference and decision-making tool to guide integrated emergency response to a specific, high-profile target within a specific jurisdiction. A target folder could include site plans, terrain analysis, interior and exterior plume dispersal models, and blast analysis. Maps indicating vulnerable points and potential sites for incident support activities could be included. These are a component of geospatial intelligence (GEOINT) developed for critical infrastructure and public gathering spaces, and utilize a standardized format to describe the characteristics of a venue.

T

Tactic: The classification of terrorist-incident tactics is maintained by RAND Corporation. The current list of tactics is detailed below.
Armed Attack, Arson, Assassination, Barricade/Hostage, Bombing, Hijacking, Kidnapping, Other, Unconventional Attack, Unknown, Unspecified

Target: The classification of terrorist targets is maintained by RAND Corporation. The current list of targets is detailed below. Abortion Related, Airports & Airlines, Business, Diplomatic, Educational Institutions, Food or Water Supply, Government, Journalists & Media, Maritime, Military, NGO, Other, Police, Private Citizens & Property, Religious Figures/Institutions, Telecommunication, Terrorists, Tourists, Transportation, Unknown, Utilities

Target Hardening: Target Hardening is defined as any measures taken to fortify the physical environment of a location or facility so as to deter or mitigate the effects of a criminal or terrorist act against it. It also refers to changing procedures, computer codes, power, and communications links to make it harder to attack.

Terrorism: Terrorism is violence, or the threat of violence, calculated to create an atmosphere of fear and alarm. These acts are designed to coerce others into actions they would not otherwise undertake, or refrain from actions they desired to take. All terrorist acts are crimes. Many would also be violation of the rules of war if a state of war existed. This violence or threat of violence is generally directed against civilian targets. The motives of all terrorists are political, and terrorist actions are generally carried out in a way that will achieve maximum publicity. Unlike other criminal acts, terrorists often claim credit for their acts. Finally, terrorist acts are intended to produce effects beyond the immediate physical damage of the cause, having long-term psychological repercussions on a particular target audience. The fear created by terrorists may be intended to cause people to exaggerate the strengths of the terrorist and the importance of the cause, to provoke governmental overreaction, to discourage dissent, or simply to intimidate and thereby enforce compliance with their demands.

Terrorist Group: A collection of individuals belonging to an autonomous non-state or subnational revolutionary or anti-governmental movement who are dedicated to the use of violence to achieve their objectives. Such an entity is seen as having at least some structural and command and control apparatus that, no matter how loose or flexible, nonetheless provides an overall organizational framework and general strategic direction. This definition is meant to include contemporary religion-motivated and apocalyptic groups and other movements that seek theological justification or divine sanction for their acts of violence.

Terrorism Early Warning Group (TEW): The Terrorism Early Warning Group (TEW) is an anti-terrorism intelligence and assessment team. The TEW incorporates multiple disciplines (fire, EMS, HazMat, law enforcement, public health, and emergency management) into a single team dedicated to preventing, preparing for, and responding to incidents of terrorism. The first TEW was created in Los Angeles County and has since become a model counterterrorism program used by jurisdictions throughout the country.

Trends and Potentials: The portion of the indications and warning cycle that considers patterns of attack, and the potential selection of targets and tactics by terrorists (trends) and their likely impact on the provision of emergency services (potentials).

U

U.S. State Dept. FTO Foreign Terrorist Organizations [FTOs] are foreign organizations that are designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended. FTO designations play a critical role in our fight against terrorism and are an effective means of curtailing support for terrorist activities and pressuring groups to get out of the terrorism business.
Legal Criteria for Designation [of an FTO] (Reflecting Amendments to Section 219 of the INA in the USA PATRIOT Act of 2001):
It must be a foreign organization.
The organization must engage in terrorist activity, as defined in section 212 (a)(3)(B) of the INA (8 U.S.C. § 1182(a)(3)(B)),* or terrorism, as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C. § 2656f(d)(2)),** or retain the capability and intent to engage in terrorist activity or terrorism.
The organization's terrorist activity or terrorism must threaten the security of U.S. nationals or the national security (national defense, foreign relations, or the economic interests) of the United States
The U.S. State Department publishes a list of designated Foreign Terrorist Organizations, which the *Terrorism Knowledge Base* lists as "Designated Groups." In addition, the department compiles a secondary list of "other terrorist groups." The other groups are listed in the *Terrorism Knowledge Base* as "Watched Groups." The Terrorism Knowledge Base contains FTO information from 1997-Present. 1997 was the initial year in which the U.S. State Department published two lists of terrorist organizations, designated and other.

U.S. Terrorist Exclusion List: Section 411 of the USA PATRIOT ACT of 2001 (8 U.S.C. § 1182) authorized the Secretary of State, in consultation with or upon the request of the Attorney General, to designate terrorist organizations for immigration purposes. This authority is known as the "Terrorist Exclusion List (TEL) " authority. A TEL designation bolsters homeland security efforts by facilitating the USG's ability to exclude aliens associated with entities on the TEL from entering the United States.
An organization can be placed on the TEL if the Secretary of State finds that the organization:
Commits or insights to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity;
Prepares or plans a terrorist activity;

Gathers information on potential targets for terrorist activity; or
Provides material support to further terrorist activity.

W

Warnings: A TEW product issued when there is a credible, verified and validated specific threat to persons or venues (specific sites, events or critical infrastructure) within a TEW's area of operations or an adjacent jurisdiction if local resources are expected to become involved in a mutual aid response. Warnings will always be accompanied by specific response planning steps and recommended course of action options for response. Warnings will be issued during a Severe (RED) HSAS level.

Weaponization: The deliberate processing, preparation, packaging, or synthesis of any substance for use as a weapon or munitions. "Weaponized Agents" are those agents or substances prepared for dissemination through any explosive, thermal, pneumatic, or mechanical means

Weapons of Mass Destruction (WMD): Weapons of mass destruction are generally referred to as chemical, biological, radiological/nuclear, or large explosive (CBRNE) weapons. A weapon of mass destruction (WMD) is any device, material, or substance used in a manner, in a quantity or type, or under circumstances evidencing intent to cause death or serious injury to persons, or significant damage to property.

Appendix D – References

Background Sources

Arquilla, John, and Ronfeldt, David F., "Netwar Revisited: The Fight for the Future Continues," in Robert J. Bunker (ED.), *Networks, Terrorism and Global Insurgency*. London: Routledge, 2005, pp.8-19.

Bodnar, John. "Making Sense of Massive Data by Hypothesis Testing." Presentation materials, MacLean, VA: SAIC. Retrieved in 2005, from https://analysis.mitre.org/proceedings/Final_Papers_Files/124_Camera_Ready_Paper.pdf.

Bunker, Robert J., and Begert, Matt, "Operational Combat Analysis of the Al Qaeda Network," in Robert J. Bunker (ED.), *Networks, Terrorism and Global Insurgency,* London: Routledge, 2005, pp.146-168.

Campbell, Lisa J., "Applying Order of Battle to Al Qaeda Operations," in Robert J. Bunker (ED.), *Networks, Terrorism and Global Insurgency,* London: Routledge, 2005, pp.183-197.

Carter, David L., "*Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*," for the U.S. Department of Justice, Office of Community Oriented Policing Services. Michigan State University, 2004.

FM 5-33. *Terrain Analysis*. July 1990.

FM 5-170. *Engineer Reconnaissance*. March 1992.

FM 6-20-10. *Tactical, Techniques, and Procedures for the Targeting Process*. March 1990.

FM 34-1. *Intelligence and Electronic Warfare Operations*. July 1987.

FM 34-2. *Collection Management and Synchronization Planning*. January 1994.

FM 34-3. *Intelligence Analysis*. March 1990.

FM 34-7. *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations*. May 1993.

FM 34-60. *Counterintelligence*. February 1990.

FM 34-81-1. *Battlefield Weather Effects*. December 1992.

FM 34-130. *Intelligence Preparation of the Battlefield (IPB) Manual*. July 1996.

FM 90-10. *Military Operations on Urbanized Terrain (MOUT)*. August 1979.

Glaese, Edward L., and Shapiro, Jesse M., "Cities and Warfare: The Impact of Terrorism on Urban Form," in the *Hazard Institute of Economic Research* (Discussion Paper Number 1942). Cambridge, Massachusetts: Harvard University, December 2001. Retrieved from http://post.economics.harvard.edu/hier/2001papers/2001list.html.

Glen, Russell, W., *Heavy Matter: Urban Operations' Density of Challenges*. MR-1239, Santa Monica, CA: RAND, 2000.

Guidelines for Establishing and Operating Fusion Centers *at the Local, State, Tribal and Federal Level: Law Enforcement Intelligence Component,* in *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World (Version 1.0)* Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with Global Justice Information Sharing Initiative, 2005.

Guidelines for Homeland Security: Terrorism Prevention and Deterrence *(Version 2.0)*. U.S. Deparment of Homeland Security, Office for State and Local Government Coordination and Preparedness, Office for Domestic Preparedness, March 2005.

Hollywood, John, Snyder, Diane, McKay, Kenneth, and Boon, John, *Out of the Ordinary; Finding Hidden Threats by Analyzing Unusual Behavior*. Santa Monica, CA: RAND, 2004.

Mani, Inderjeet and Klein, Gary, L., *Evaluating Intelligence Analysis Arguments in Open-ended Situations*. Georgetown University, Washington, DC: The Mitre Corporation, 2005.

MCDP-1. Warfighting. June 1997.

MCDP–2. Intelligence. June 1997.

MCWP 3-33.5. Counterinsurgency Operations. August 2004

Medby, Jamison Jo and Glenn, Russell W., *Street Smart: Intelligence Preparation of the Battlefield for Urban Operations*. MR-1287, Santa Monica, CA: RAND, 2002.

Sullivan, John P., "A Cooperative Vehicle for Threat Assessment: L.A. County Terrorism Early Warning (TEW) Group." *Annual Report*, The Interagency Board for Equipment Standardization and InterOperability, 2000, pp. 45-51.

Sullivan, John P., "Intelligence Co-production and Transaction Analysis for Counterterrorism and Counter-Netwar," paper presented to *International Studies Association, ISA Annual Conference*. Panel on Intelligence and Operational Issues for Counterterrorism and Counterinsurgency, San Diego, CA 24 March 2006.

Sullivan John P., "Networked All-Source Fusion For Intelligence and Law Enforcement Counterterrorism Response," paper presented to Intelligence Studies Section of the *International Studies Association (ISA)*, 2004 ISA Annual Convention, Montreal Quebec, Canada, 18 March 2004.

Sullivan, John P., "Networked Force Structure and C4I,“ in Robert J. Bunker (Ed.), *Non-State Threats and Future Wars*, London: Frank Cass, 2003, pp. 144-155.

Sullivan, John P., "Terrorism, Crime and Private Armies," in Robert J. Bunker (ED.), *Networks, Terrorism and Global Insurgency*, London: Routledge, 2005, pp.69-83.

Sullivan, John P., "Terrorism Early Warning and Co-Production of Counterterrorism Intelligence," Presented to Canadian Association for Security and Intelligence Studies *CASIS 20th Anniversary*

International Conference, Panel 5: In Pursuit of the Analytical Holy Grail: Part 1 Innovation in Analysis, Warning and Prediction (October 21, 2005), Montreal, Quebec, Canada.

Sullivan, John P., *TEW Resource Book One: Introduction to the Terrorism Early Warning Group,* for the Terrorism Early Warning (TEW) Expansion Program, National TEW Resource Center, 2005.

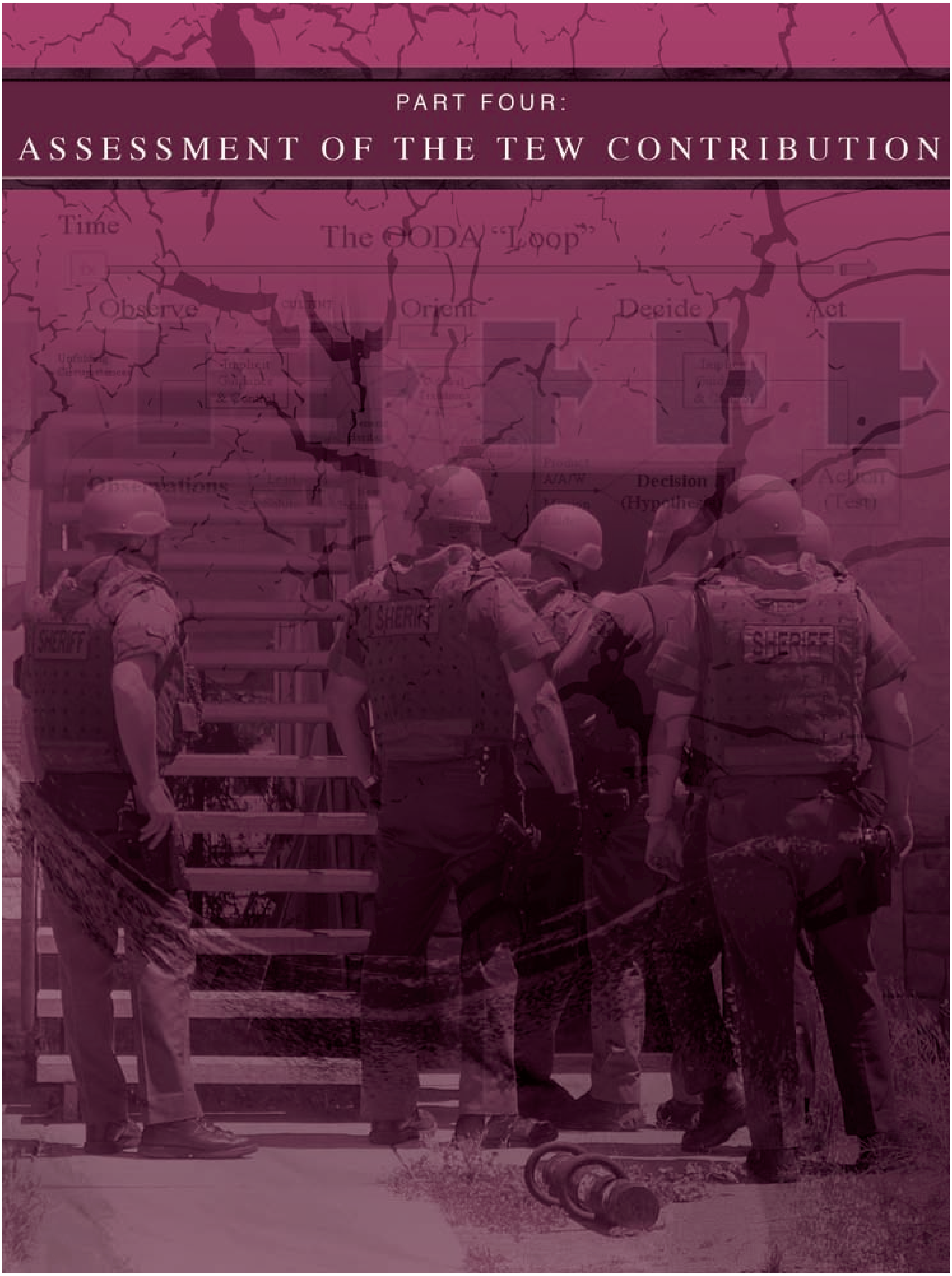
Sullivan, John P. and Bunker Robert J., "Multilateral Counter-Insurgency Networks," in Robert J. Bunker (ED.), *Networks, Terrorism and Global Insurgency*, London: Routledge, 2005, pp.183-198.

Sullivan, John P., Kempfer, Hal, and Medby, Jamison Jo, "Understanding Consequences in Urban Operations: Intelligence Preparation for Operations", *OnPoint: A Counterterrorism Journal for Military and Law Enforcement Professionals,* 2005, Retrieved from http://www.uscav.com/uscavonpoint.

The National Criminal Intelligence Sharing Plan: *Solutions and Approaches for a Cohesive Plan to Improve out nation's Ability to Develop and Share Criminal Intelligence,* Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with Global Justice Information Sharing Initiative (October 2003).

PART FOUR:

ASSESSMENT OF THE TEW CONTRIBUTION



The Terrorism Early Warning Group's Contribution to the Counterterrorist Intelligence Process

By Brian Michael Jenkins

Early warning has become more crucial as terrorists have escalated their violence. The traditional law enforcement approach of reacting only to crimes committed does not adequately protect the public when terrorists are determined to kill scores, hundreds, or, as on 9/11, thousands of people. And there is little justice to be done when the perpetrators themselves are willing to die in the attacks. Understandably, there is pressure on all authorities to intervene before the carnage occurs. This requires good intelligence, not only to deter or disrupt terrorist attacks, but also to avoid panic-driven overreactions if attacks do occur.

If we were dealing exclusively with centrally directed organizations taking their orders from leaders ensconced in some remote corner of the world, early warning would depend primarily on communications intercepts, the monitoring of border crossings and money movements, and liaison with foreign intelligence services, the kinds of things national intelligence services do. The 9/11 plot provided some of those clues, although the national intelligence community failed to put them together.

There is an erroneous impression, though one still extant in the clearance process and other controls on information, that all intelligence flows downward and outward from the federal government. That may have been true during the Cold War, when information about Soviet intentions and capabilities came almost exclusively through the highly compartmentalized collection efforts of the national intelligence agencies, which had very little need to share their findings. As we have learned, this model doesn't work very well now.

Instead of being organized in disciplined hierarchies, today's terrorists (like much of today's organized crime) operate in networks that link operatives but are not necessarily centrally directed. A central command may plan strategic operations, it may provide approved projects with financial or technical assistance, or it may merely exhort local followers to take action. Inspired by the message, local operatives may initiate action with little outside guidance. They may have little or no direct contact with the center, although they may link up with other operatives at the local level, or they may carry out attacks entirely on their own.

The unprecedented unanimity of focus among the world's intelligence services and law enforcement organizations following 9/11 has forced the al-Qaeda–inspired terrorist enterprise to operate in an increasingly hostile environment, and as a result, al-Qaeda's operations have become more decentralized. There was in early 2008 still some debate among analysts about how deeply involved al-Qaeda central has been in the major terrorist attacks since 9/11. Some see al-Qaeda's hand in every major terrorist attack, while others are worried more about homegrown terrorism. Central direction and local initiative are both there. But whether or not the recent jihadist operations have been directly linked in every case to a central command, most seem to have had a higher local content. That means we may not be able to depend as much on the information obtained through national intelligence efforts.

Local police, through community policing, routine criminal investigations, or dedicated intelligence efforts, are just as likely to pick up hints and warnings of attacks as any national intelligence organization. This suggests that local intelligence capabilities, for both collection and analysis, should be enhanced. It is the local cops, or the local fire investigators, or local hospitals, or local industries who may be best positioned to "connect the dots."

Domestic intelligence collection will always be controversial and subject to constraints in a democracy. Local police have certain advantages here. They are intimately familiar with their territory, the local social geography, the diverse local communities. Locally recruited, they are better able to reflect the communities in which they operate. And they report to locally elected officials, which make them more acceptable to the community.

Local law enforcement also has disadvantages. With state and local governments strapped for funds, the resources available to local police will always be limited, especially resources devoted to the invisible work of intelligence. Unless, as in New York, there is a continuing sense of clear and present danger, it is hard to justify diverting any resources from combating ordinary crime. Besides having limited resources, local police, confined to city limits, have much smaller operational horizons.

These shortcomings can be overcome by obtaining federal assistance, by developing relationships with federal authorities that ensure the flow of information both up and down, and by networking with adjacent communities to guarantee the lateral flow of information. Sharing is not merely a virtue, it is critical to success. But it doesn't always work that way.

Putting together intelligence about terrorism might be compared to doing a jigsaw puzzle, but with artificial handicaps imposed. As in a jigsaw puzzle, there are lots of pieces of information. The objective is to fit the pieces together to eventually reveal a picture of what is going on, but how they all fit together is not immediately apparent.

In real-life intelligence, the task of assembling the puzzle is made more difficult by the absence of the cover of the box, which illustrates the completed puzzle. Intelligence analysts have no box covers to guide them—they have no idea what the final picture will look like. In fact, the picture the analysts are looking for may itself be changing during their analysis. Moreover, the real-life intelligence puzzle has no straight edges or other obvious clues that assist people in solving a jigsaw puzzle.

In addition, some pieces of the puzzle will be missing. Even more confusing, pieces from other puzzles will be mixed in. Analysts have to decide which pieces fit and which are irrelevant, while avoiding the creation of a false picture with erroneously combined pieces.

The task is further complicated by dividing the pieces into separate, unequal piles and distributing these to different analysts at different agencies. Everyone may have some relevant pieces. No one has the whole picture.

The ideal solution would be for all of the analysts to get together to combine all of their pieces, but in real life, that is not easily done. Legal and bureaucratic barriers restrict what can be shared and with whom. Not everyone can talk with everyone else. The "intelligence community" is not so much a community as a collection of walled towns.

Sharing information among intelligence services is an unnatural act. National commissions can exhort information sharing, legislators can mandate it, committees inside government can develop elaborate wiring diagrams and negotiate memoranda of understanding, but none of this guarantees that information, in fact, will be shared within a single cabinet department, among federal government agencies, or with state and local authorities or actors who are not part of the traditional intelligence community—for example, health authorities—let alone with the private sector.

Sharing intelligence is still difficult to do, even after 9/11. In the intelligence environment that existed in the late 1990s, it was even more difficult. The mechanisms hardly existed. It is in this context that we must view the creation of the Los Angeles Terrorism Early Warning Group (TEW). The TEW is a unique organization. Although it is a group project, it reflects the vision and driving energy of one man in particular, Lieutenant John Sullivan. And it has benefited from the continuing support of Sheriff Lee Baca, who has demonstrated that he is not averse to unorthodox views and unconventional approaches to law enforcement.

At the same time, the TEW draws upon California's tradition of cross-jurisdictional planning and mutual assistance in dealing with the recurring disasters that affect the state. Wildfires, mudslides, earthquakes, and other major events can easily overwhelm the capacity of local fire departments, emergency services, and law enforcement. Los Angeles County is a sprawling piece of geography that ranges from cityscapes to rugged mountains. Its 10 million inhabitants are divided into 88 separate cities, most of which are served by their own police and fire departments. The county's two largest police departments, the Los Angeles Police Department and the Los Angeles Sheriff's Department, have less than half the manpower of the New York Police Department, which serves roughly the same number of people. The requirement for mutual assistance comes with the territory.

Mutual assistance, in turn, requires protocols, standardized operating procedures, and interoperability of equipment and communications to produce a seamless expanding response to a large-scale emergency. The state of California has taken the lead in this area. Its Incident Command System (ICS) and Standardized Emergency Management System (SEMS) provided the model for the National Incident Management System, which the Department of Homeland Security has made a requirement for local authorities across the nation. In many respects, the TEW is the intelligence component of these earlier collaborative efforts. The Los Angeles Sheriff's Department was in a unique position to develop these relationships, since it provides police services or major-crimes investigative support to a number of the county's smaller communities. By necessity, the Los Angeles Sheriff's Department is a leader in cooperative ventures.

The TEW, however, reaches beyond cooperation among law enforcement organizations. It defines security broadly to include not only the law enforcement response to crime, but also a spectrum of activities from basic knowledge of the adversary, intelligence collection and analysis, countersurveillance, deterrence, prevention, detection, and defense to emergency response, evacuation, mitigation of consequences, maintenance of vital services, and restoration of normal conditions.

Obviously, these are functions that transcend the mandate of the Sheriff's Department. They involve numerous local actors—police, fire departments, public health, hospitals, transportation—as well as state and federal authorities, including the Department of Homeland Security and the Department of Defense. With much of the county's vital infrastructure privately owned, the private sector must also be represented.

All of these organizations are likely to be involved in a major disaster, either natural or man-made. The response cannot depend on entirely state or federal authorities to arrive at the scene, conduct an assessment, and formulate plans. In order to operate effectively, all will require detailed local intelligence, not only about possible villains, but about the attributes of their potential targets, the potential effects of attacks, and the consequences of destruction or failure.

Threat assessments, target folders, contingency plans, tabletop and field exercises to test responses and reveal problem areas all must be prepared and conducted in advance. To operate seamlessly also requires knowledge of and confidence in counterparts, the kind of personal relationships that are built up by working together over a period of years. The TEW provides a forum for these discussions, a center for planning, a catalyst for participating agencies to ensure their own preparedness.

We tend to view counterterrorism in dramatic terms of undercover agents, secret informants, the uncovering of diabolical plots, and arrests in the nick of time. Sometimes it is that, but the reality is usually different. It is a bureaucratic task of systematic approaches to threat analysis, the protocols for information sharing, and the detailed operational plans that are described earlier in this volume. This is how government works.

Yet these same structures can sometimes get in the way. Process can defeat mission achievement. The TEW has, in its twelve years of existence, developed systematic approaches and a frankly, sometimes daunting, array of charts and acronyms. Yet its very success depends on its origins as an autonomous self-organizing enterprise, attracting to itself those with similar concerns and responsibilities. Cooperation requires organization that cannot be allowed to kill cooperation. The TEW has functioned well, not because anybody ordered its creation or demanded participation, but because it fulfilled a need. The TEW transcended organizational lines and jurisdictional boundaries, breached bureaucratic barriers, operated "outside" the system, external to positions and politics. It became the one place where once-unthinkable threats and the community's ability or inability to respond could be addressed freely.

How do we assess the success of the TEW? Not by the standards of television drama. Prevention of terrorist attacks is just one goal, important but hard to measure—how do you count things that do not occur? And preventive measures don't always connect to specific plots. Terrorists may be deterred by alert guards trained to report possible instances of surveillance. A nascent terrorist cell may be disrupted by the timely arrest on other charges of one of its members. The presence of a patrol car can persuade terrorists that they are being watched. Good security, always a deterrent, depends on knowledge about how terrorists might exploit the vulnerabilities of a particular target. Police investigators have to be trained in what to look for—e.g., when is what looks like a meth lab, in fact, a bomb factory? There has to be a mechanism for rapidly transmitting information when something looks suspicious.

Not all of the intelligence effort is devoted to apprehension or disruption. It is also important to know quickly whether stealth attacks are taking place—e.g., pathogens being released. Here, the early warning may come from emergency rooms or hospital admissions. Rapid diagnosis of a threat can lead to public warnings that save lives, just as erroneous information can lead to public panic.

Good intelligence on suspected terrorist cells can assist an investigation in the event of an attack. Target folders for every likely terrorist target inform first responders and help city officials make evacuation decisions. The TEW is not solely concerned with law enforcement, it touches upon all of these areas. It is the intelligence back-up to the Emergency Operations Center, where responses to disasters are managed. In sum, it is not the number of villains arrested, but the community's degree of engagement and level of preparedness that counts.

The work of the Los Angeles County's TEW has been incorporated into the Los Angeles Joint Regional Intelligence Center (JRIC), a larger fusion center. Now physically collocated with federal, state, and local authorities, it carries on its work, devoting itself to more fundamental strategic assessments—the TEW became the JRIC's think tank.

At the same time, the TEW has become a model of organization for cooperation that is being replicated by other local governments across the nation. The nation is too diverse for one model to fit all, but the spread of TEWs, JRICs, and Joint Terrorism Task Forces (JTTFs) is gradually creating a national network of intelligence defined broadly—a virtual national intelligence service, but one that is primarily locally owned and operated, which seems typically American. The federal government should act to enable rather than attempt to control the process. And the network or network of networks must guard against over-bureaucratizing itself. The Los Angeles TEW deserves credit for pioneering this positive development.

PART FIVE:
APPENDICES

RECOVERY & SITE RESTORATION
(CONSEQUENCE MANAGEMENT)
Near-Term Activities
Formally convene the SRWG.
Establish a recovery organization.
Work contamination fixing & resuspension issues, if appropriate.
Transition the JOC to the Disaster Field Office (DFO).
Develop a database for long-term monitoring.
Develop onsite & offsite Characterization Plans.
Implement and document planned activities.
Continue to provide progress reports to the media and participating and concerned organizations.
Address the transfer of the FRMAC to EPA.
Work the funding & legal issues.
Long-Term Activities (Site Monitoring)
Develop a Site Monitoring Plan after site restoration is completed.
Monitor onsite & offsite locations in accordance with the Site Monitoring Plan.
Continue monitoring until federal, state, & local authorities agree to terminate monitoring.
Prepare & maintain formal documents (EPA & state, as required).
LFA and/or state must continue budget requests in annual submissions for funding.
CALIFORNIA REP

The following appendices recount significant TEW events, including monthly TEW meetings, conferences and workshops.

I. TEW Speakers and Presentation History

Once a month, law enforcement, intelligence, medical, business, academic, and military professionals gather for the Terrorism Early Warning Group plenary session. Though the primary mission of the TEW is to develop an understanding of potential threats and develop the analytical tradecraft required to conduct counterterrorism intelligence analysis and response, the TEW also serves the purpose of increasing law enforcement and public safety knowledge of new developments in terrorism, security, international relations, and technology. A host of speakers have presented before the TEW, sometimes reprising academic papers presented at conferences or published in scholarly journals. A list is provided below of significant speakers and presentations since 1996.

1996

November

Mr. Maury Eisentein, The RAND Corporation. "The RAND Perspective on Terrorism and its Local Impact."

December

Dr. Robert Bunker, National Security Studies Program, CalState San Bernardino. "Future War and Terrorism."

Mr. Charles Chase, Program Manager, Imperial Valley Law Enforcement Coordination Center. "Cross Border Potentials."

1997

February

Dr. Robert Bunker, National Security Studies Program, CalState San Bernandino. "Advanced Terrorism Concepts and the Non-State Soldier."

March

Dr. John Celentano, L.A. County Department of Health Services. "Chemical and Biological Warfare and Terror Agents."

April

Dr. Bob Anderson, The RAND Corporation. "Cyberspace Security and Safety."

Mr. William Swansinger, Sandia Labs. "NBC Mitigation Technology."

Dr. Annete Sobel, Sandia Labs. "Technology and Medical Counterterrorism."

Mr. Mike Skroch, Sandia Labs. "Technology for Addressing Cyberterrorism."

June

Lt. Col. Matt Begart, United States Marine Corps. “Developing Playbooks: Vulnerability Assessment, Target Sets & Folders.”

July

Ms. Michelle Amador, GTE. “Critical Infrastructure Issues—Telecom.”

Mr. Maury Eisenstein, The RAND Corporation. “Airbase Defense Implications for Civil Aviation.”

Messrs. Thomas McGrann and Dennis Imbro, Lawrence Livermore National Laboratory. “Counterterrorist (NBC+1) Technology Issues.”

August

Mr. Eric Nelson, G-TWO-I (G2I). “Open Source Intelligence Analysis: G2I.”

Detective Rubin Holguin, LAPD Anti-Terrorist Division. “Hamas Briefing.”

September

Dr. Robert Bunker, NSSP/CSUSB. “Advanced Less-Lethal Weapons: Projected Terrorist Employment.”

Mr. Ray Jackson, NSSP/CSUSB. “Models of Home-made EMP Devices.”

Mr. John Dering, SARA Labs. “Radio Frequency Weapons: A Technical Introduction and Their Potential for Terrorist use.”

Mr. Clark Staten, Emergency Response Research Institute. “Perspectives on CB Terrorism Prepareness,”

October

LTC Arthur Corbett, United States Marine Corps. “Chemical Biological Incident Response Force Overview.”

CPT Laurie Belajurchik, United States Navy. “Medical Support to the CBIRF.”

Annette Sobel, M.D., Sandia National Laboratory. “Counterterrorism Technology Developments.”

November

Special Agent Kevin Miles, Federal Bureau of Investigation “Conventional Bombing Incidents and Concerns.”

Mr. Mike Tobin, Lawrence Livermore National Laboratory. “Nuclear Detection: Wide Area Tracking System Overview.”

December

Mr. Charles Chase, Imperial Valley Counterdrug Coalition. “Cross Border Potentials.”

1998

January

Shirley Fanin, M.D., Director of Disease Control Programs, LAC DHS. "Problem-Solving With Biological Agents: An Overview and Examples."

February

Dennis Imbro, Ph.D, Lawrence Livermore National Laboratory. "WMD Exercises: 911 Bio Lessons Learned."

Deputy Larry Richards, LASD EOB. "Case Study: Phineas Priests."

Mr. T.J. Lyden, Simon Wiesenthal Center. "Skinhead Perspectives."

March

Mr. Nick Catrantzos, Metropolitan Water District. "An Overview Threat and Vulnerability Analysis for Water Systems."

Special Agent Robin Salvador, FBI, Las Vegas Office. "Case Study: Henderson 'Anthrax' Incident."

April

Scott Layne, M.D., School of Public Health, UCLA. "Bioterrorism: Laboratory Firepower for Threat Reduction."

David Ronfeldt, Senior Social Scientist, RAND Corporation. "Looking Ahead: Preparing for Information Age Conflict."

June

Lt. Col. Matt Begert, USMC; Dr. Robert Bunker, CSUSB; CPT Dan Lindsay, ONT FD. "Laser Employment Against Civil Aviation and Law Enforcement: Overview, Recent Incidents, Scenarios, and Response Measures."

November

International Terrorism Squad, FBI, Los Angeles Field Office. "Hizbollah: An Overview."

1999

January

Deputy Larry Richards, LASD EOB. "Anthrax Threat Protocols."

February

Sergeant Ron Waltman, LASD, Detective Resource Information Center (DIRC). "LASD DIRC Overview."

March

Captain Dan Lindsay, ONT Airport. “Laser Incident Update.”

April

Mr. Jason Pate, Research Associate, Center for Nonproliferation, Monterey Institute of International Studies. “Chemical, Biological, Nuclear and Radiological Threat Database.”

May

Mr. Brian Jenkins, RAND Corporation. “Will Terrorists Use Weapons of Mass Destruction—An Assessment of the Threat.”

June

Benjamin C. Garett, PhD, Chief Scientist, CW/BW Defense, Battelle. “The Biological Weapons Threat: Nightmare vs. Reality.”

Mr. Chuck Crawford, Soldier & Biological Chemical Command. “A Proposed Response to a BW Incident.”

July

Javed Ali, J.D., M.A., Research Planning International, Inc. “BW Proliferation—A Threat Assessment.”

Special Agent Brendan Finn, FBI, Los Angeles Division. “Lessons Learned from Canadian WMD Response.”

August

Mr. Richard Hunt, NAWC Imageering Lab. “Emerging C4ISR Technology.”

Lieutenant Joe Eddy, LAPD, Devonshire Division. “Granada Hills Daycare Shooting.”

September

Western States Council, Anti-Defamation League. “Trends in Hate Groups.”

Scott Lewis, California Department of Health Services. “State DHS Capabilities for WMD Events.”

October

Special Agent Trent Teyema, FBI, Los Angeles Division. “Cyberthreat Update & Infragard Overview.”

Sergeant Shiela Sanchez, LASD EOB. “Operational Area NY2000 Event Matrix.”

November

Jonathan Schachter, Doctoral Fellow, RAND Graduate School. “Israeli Approaches to WMD Terrorism.”

2000

January

Mr. Mike Schuk, Director, Precision Guided Weapons Countermeasures Test and Evaluation Directorate, Office of the Secretary of Defense. "Surface-to-Air Missiles: Technology and Threat."

February

Brian Houghton, Doctoral Fellow, RAND Graduate School. "Overview of Bioterrorism Homeland Defense Symposium."

Ernest Lorelli, SPARTA, Inc. "WMD/IED Recognition Training."

April

Maj. Adrian Bogart, US Army, COMPIO. "Overview of Interagency Board for Equipment Standardization and Interoperability for Terrorism Response."

Commander Vic Thies, Irvine Police Department. "Overview of Irvine 'Bio-Fem' WMD Incident."

Col. John Alexander, USA (ret). author Future War. "Future Conflict."

Dr. Robert Bunker "WebBase Overview."

May

Col. G.I Wilson, Special Intelligence Project Officer, I MEF. "Emerging Threats for Consequence Management."

Investigator Steve Reyes, California Highway Patrol. "Briefing on the Downing of a CHP Helicopter by Gunfire."

June

Kathleen Kaufman, LAC DHS, Radiation Management. "Overview of LAC Radiological Mgt. Programs."

July

Todd Brethauer, Consultant to TSWG. "Overview of TSWG CT Technology Programs."

James Llewellen & Michael Krogh, Honeywall. "Briefing on Laser Protection."

August

LTC Ralph Peters, USA (ret). "Insights into Future Conflict."

September

James Llewellen & Michael Krogh, Honeywall. "Update on Laser Protection Options."

October

Rudolph V. Matalucci, Ph.D., P.E., Distinguished Member of Technical Staff, Sandia National Laboratories. “Infrastructural & Architectural Surety.”

John M. Kaysak, Nuclear Program Manager, FBI Laboratory, Investigative Response Section. “The FBI’s Response to a Nuclear Threat.”

November

Sean J.A. Edwards, RAND Corporation. “Swarming and Future Conflict.”

2001

February

Deputy Larry Richards, LASD. “Intelligence Concepts.”

February

Maj. Hal Kempfer, Director, Joint Reserve Intelligence Center. “Creating Intelligence.”

Larry B. Barnes, Senior Analyst, Kapos Associates, Inc. “Briefing on the Camp Pendleton Anti-Terrorism Exercise.”

March

Scott P. Layne, M.D., Associate Professor, School of Public Health, UCLA. “Epidemiologic Investigations of Bioattacks.”

April

Dr. Russell Glenn, RAND, Arroyo Center. “Density in Urban Operations (Urban Ops/Density Challenge).”

Col. Pete Dotto, USMC, Retired. “Non-Lethal Weapons/Force Protection.”

May

Dr. Fadi Essmaeel, Office of Representative Dan Rohrabacher. “Terrorism, Politics, and First Responders.”

June

LTC Ken Luikart, 165th Airlift Wing, Air National Guard, Savannah, GA., “Intelligence Analysis”

LTC Hal Kempfer, USMCR, OIC, Camp Pendleton Joint Reserve Intelligence Center (JRIC). “Intelligence: Indications and Warning.”

July

Jamison Jo Medby, RAND Corporation. “Intelligence Preparation of the Battlefield (IPB).”

Deputy Larry Richards, EOB. “Recent Networked Anti-Globalization & Anti-GMO Events.”

August

John A. Nolan III, President, Society of Competitive Intelligence Professionals. “Human Intelligence Operations and Terrorism.”

September

Deputy Larry Richards, EOB. “Recent Terrorist Attack in NYC and Washington.”

Sergeant John Sullivan. “Terrorism Early Warning Group Activated Immediately.”

October

Scott Gerwehr, RAND Corporation. “Deception and Terrorism.”

CPT Mike Thompson, California National Guard 9th Weapons of Mass Destruction Civil Support Team. “Mission Planning.”

November

Dan Paradis, Royal Canadian Mounted Police. “Canadian Response to Terrorism Post-9/11.”

December

Scott P. Layne, M.D. Associate Professor, School of Public Health, UCLA. “VADAR—Virtually Assured Detection and Response.”

2002

January

Ken Englehard, Security Services, The Boeing Company. “A Private Sector Perspective—Terrorism Early Warning.”

February

Captain Jason Whalen, USMC/JRIC. “Deployment Rapid Deployment (R2P2) Planning.”

Mr. Matt Begert, NLECTC-West. “WTC Overhead Imagery for CM Planning.”

March

Col. G.I. Wilson USMCR. “Indications & Warning: Deep I&W and TEW Interface.”

April

Susan Everingham, Director of Forces and Resources Policy Center, National Defense Research Institute, RAND. “Gilmore Commission Update.”

Brian M. Jenkins, RAND. “Terrorism Trends: Impact of Islamist Extremism.”

June

Sergeant Heidi Clark, LASD Arson/Explosives Detail. “Suicide Bombings in Israel: LA Study Team, Lesson Learned.”

July

Jamison Medby, RAND. “Security and Safety in Los Angeles High-Rise Buildings After 9/11.”

Frank Lepage, US DOJ, Office of Domestic Preparedness. “Prepositioned Equipment Program.”

August

Mr. Hakim Hazim. “Radical Jihad: An Overview.”

LTC Matt Begert, USMC (ret). “Principles of Special Operations,” “Fabens, TX Border Lasing Incident.”

September

LTC Hal Kempfer, USMCR. “Consequence Management Intelligence.”

October

Matt Devost, Terrorism Research Center, Inc. “Cyberterrorism: Identifying and Responding to Emerging Threats.”

November

Dr. Dave Warner, Mindtel, Inc. “Information Visualization and Toroids.”

Mr. James Higgens, USMC. “15th MEU Afghan Conflict.”

2003

January

Dr. Jessica Jones, LACO DHS. “LA County Smallpox Preparedness Vaccination Program.”

Richard Hunt and Richard Busse, Naval Air Warfare Center. “Emerging Threats: MANPADS.”

Maria Reta, Chief, Foreign Services Branch, Center for Countermeasures, White Sands Missile Range, New Mexico. “Manportable Surface to Air Missiles.”

February

Captain Phil Cater, USAR. “Emerging Terrorism Law.”

Battalion Chief Jeff Marcus, Los Angeles City Fire Department, Terrorism Early Warning Group. “Briefing on the TEW Consequence Management Cell.”

March

Dr. Robert J. Bunker, NLECTC-West. “Hamas Suicide Bombings: Overview and Threats.”

April

Hakim Hazim. “Militant Cults and the Emergence of the Lone Wolf.”

LTC Hal Kempfer, USMCR. “Marine Emergency Preparedness Liaison Officer Program.”

May

John Miller, Chief, Homeland Security Group, Los Angeles Police Department. “Briefing on Terrorism and LAPD response.”

Dr. Pete Katona, University of California, Los Angeles, School of Public Health. “SARS and Lessons for Bioterrorism Response.”

June

Sergeant Heidi Clark, Los Angeles County Sheriff’s Arson/Explosives Detail. “Large Vehicle Improvised Explosive Devices.”

Arson Investigator Glen Lucero, Los Angeles Fire Department. “House of Worship Arson Task Force.”

July

Major Matthew Castro, United States Marine Corps Reserve, Joint Task Force Civil Support. “Briefing on JTF Civil Support.”

Don McMullin and Kerry Williams, Booz Allen Hamilton. “Asymmetric Threat Implications & Warning for Critical Infrastructure Protection.”

Dr. Robert Bamban, Adjunct Professor, Pepperdine University. “Conditional Confusion.”

George Ake, CAPTWIN Project. “Briefing on the CAPWIN Project.”

August

Rich Mesic, D.A.G.S., RAND Corporation. “Scenario Development for Homeland Security.”

Todd Brethauer, Technical Support Working Group. “Technical Support Working Group CBRNC Project Group.”

William Rosenau, Ph.D. and Peter Chalk, Ph,D, RAND Corporation. “Security Intelligence, the Police, and Counter-terrorism: What Can We Learn from Other Democratic Nations?

September

Steve Emerson, Terrorism Analyst and Author: American Jihad: The Terrorists Living Among Us. “Jihad in America.”

Peter Katona, M.D., UCLA School of Public Health, "Agroterrorism Overview.”

October

David C. Rapoport, Professor of Political Science, UCLA and Editor, Terrorism and Political Violence. “The Four Waves of Modern Terror: A Generational Analysis.”

Andy Wehrle, BAE Systems and Joe Langvin, Tracrer Round. “Terrorist Strategy and Tactics.”

Robert J. Bunker, Counter-OPFOR Program, NLECTC-West. “Suicide Bombing WebBase Update.”

November

LTC Kempfer, USMCR, Region IX MEPLO. “Indications and Warning (I&W) for Terrorism Response.”

2004

January

Mr. John Short, Detective Chief Superintendent, Royal Ulster Constabulary/Northern Ireland Police Service (Ret). and Mr. Bill Lowry, Superintendent, RUC/NIPs (ret). “Comparative Intelligence: The Fight Against Terrorism! You are the Key.”

February

RADM Brenda J. Holman, Director, US FDA Regional Food & Drug Pacific Region and Mr. Tom Sidebottom, Special Assistant for Science, US FDA Pacific Region. “Food Emergency Response Network (FERN) Concept.”

Dr. Robert J. Bunker, NLECTC-West. “RMPA and the Future Threat Environment.”

March

Captain Lisa Campbell, California Air National Guard. “Applying Order of Battle Analysis to Al Qaeda.”

Chief John Penido, LA Area Fire Chiefs Association. “LARTCS: True Radio Interoperability Today.”

April

Scott Gerwehr, RAND Corporation. “Understanding, Shaping, and Defeating Terrorist Reconnaissance: In Progress Project Briefing.”

Andrew MacPherson, Institute for Security Studies, Dartmouth College. “Cyber Capabilities of Islamic Terrorist Groups.”

May

David R. Franz, DVM, PhD, Chief Biological Scientist, Midwest Research Institute & Director, National Agricultural Biosecurity Center. “Bioterrorism Scenarios and Threats.”

Dave Warner, MD, Mindtel. “Desert Bloom: Shadow Operation for DARPA Grand Challenge.”

June

Matt Begert, National Law Enforcement and Corrections Technology Center-West. “Principles of Special Operations.”

Analyst working for Supervisory Intelligence Analyst Katy Taylor, LA Field Intelligence Group, FBI-LA. “International Terrorism Intelligence Requirements.”

July

Peter Jahring, PhD, Senior Research Scientist, USAMRIID, “Smallpox and Related Pox Virus Threats.”

Jay Rosenthal, Certified Consulting Meteorologist, Geophysics Branch, Battelle. “Important Weather Considerations for Response to CBRNE Attacks and Toxic Clouds.”

Kim Guevara, SRA International, Inc. “*Operation Talavera*: TEW Exercise Summary.”

August

Dr. Abraham R. Wagner, Hicks & Associates, Inc. “Terrorism and the Internet: Uses and Abuses.”

Raphael Malki, former head of General Security Service, Operations and Logistics Division. “Current Threat to Transport and Critical Infrastructure: An Israeli Perspective.”

September

Colonel G.I. Wilson, USMCR, (ret). “Operational Perspectives on Terrorism.”

Amy H. Kaji, M.D., Disaster Medical Research Fellow, Harbor-UCLA Medical Center. “Hospital Disaster Preparedness in LA County.”

October

Brigadier General Annette L. Sobel, New Mexico Director of Homeland Security and J-2 National Guard Bureau. “Overview of the New Mexico Threat and Vulnerability Assessment Process.”

Mike Gobitz, Director of Intelligence, New Mexico Office of Homeland Security. “The Integrated Security Analysis System for Application in Early Warning.”

November

Dr. Theodore Karasik, Political Scientist, International Policy and Security Group, RAND Corporation. "The Spread of Chechen Tactics, Techniques and Procedures."

Mr. Scott Gerwehr, Associate Policy Analyst, RAND Corporation. "Al-Qaeda Recruitment."

2005

January

Dr. Theodore Karasik, Political Scientist, International Policy and Security Group, RAND Corporation. "Hezbollah in North America."

Mr. Chris Baush, SRA Inc. "*Operation Talavera*: The Year in Review."

February

Mr. Todd Brethauer, Technical Support Working Group. "Briefing on TSWG Counterterrorism Technology Update."

Dr. Robert J. Bunker, NLETC-West. "Laser Strikes Against Aircraft."

Dr. Peter Katona, Associate Professor, UCLA School of Medicine, "Influenza Update: Threat and Pandemic Potentials."

March

Rabbi Arthur Zuckerman, Emergency Response Foundation and Mr. Dan Papp, Emergency Preparedness Coordinator, City of Carlsbad. "Report on Knesset Mock Disaster Scenario."

Mr. Philip Carter, Esq, McKenna, Long, and Aldridge LLP. "Update on Legal Issues from the War on Terrorism."

Jim Morrisson, LA TEW Epi-Intel Team Leader, Larissa Mohamadi, MPH, Bioterrorism and Emergency Preparedness Coordinator, Pasadena Public Health, John Holguin, MPH, Epidemiologist Supervisor, Long Beach Dept. of Health and Human Services, and Dickson Diamond, MD, Director, Psychological Programs for Bioterrorism, LA County Public Health. "LA TEW Epi-Intel Update."

April

Dr. Boaz Ganor, Executive Director, The International Policy Institute for Counter-Terrorism (ICT). "Dealing with Counter-Terrorism Dilemmas Based On The Israeli Experience."

Philip Carter, McKenna, Long & Aldridge. "Legal Update: Current Issues."

May

Michael Callahan, MD, DTM&H, MSPH, Center for the Integration of Medicine and Innovative Technology (www.cimit.org) and Massachusetts General Hospital. “Bioterrorism: Case Scenarios.”

Mr. Duane Clarridge and Ms. Monique Aschkenasy, DAX and Associates. “Lessons Learned: The Formation of the CIA’s Counter-Terrorism Center.”

June

Peter Katona, MD, UCLA School of Medicine. “Bioterrorism: Differential Diagnosis Tutorial.”

Mr. Hal Kempfer KIPP. “Intelligence Requirements to Indicator Trees: Tools for Making ‘Intelligence’ Actionable, Relevant, and Real.”

September

Mr. Frank Stopa, Central Intelligence Agency, retired. “Human Intelligence Networking and Terrorism Early Warning.”

Mr. Jim Petroni. California Specialized Training Institute. “Consequence Assessment for Terrorism.”

Messrs. Alex Mintz and Marshall Toplansky. “Overcoming Biases in Homeland Security Decision Making Through Computer Simulation.”

October

BG Annette L. Sobel. “National Guard Information Sharing.”

Ms. Lisa Sokol, General Dynamics, Knowledge Management Center of Excellence. “Information Management Environment for Early Warning Centers.”

Lt. Col Hal Kempfer, USMCR, Region IX MEPLO. “Defense Support to Civil Authorities.”

November

Mr. Jay Kurtz, KappaWest. “Military & Business Intelligence Insights.”

Mr. Len Hayes. “Border Issues.”

Dep. Rick Byrum, LASD, LA TEW. “Inter-Faith Liaison Issues: Lessons From The UK.”

2006

March

Ms. Lauren Armisted, Deputy Director, HSAC Region I. “Introduction to Homeland Security Advisory Council.”

MSgt Brandall Horney, CA Air National Guard. “Cartoon War: Overview of Cultural Impact of ‘Muslim’ Cartoons.”

Mr. James E. (Ed) Beakley, Center for Asymmetric Warfare. “Adaptability: Project White Horse.”

May

Mr. Mark Chris Bausch, Red Team Intelligence, LLC. “Intel Tradecraft: 1-1: Intelligence Fundamentals Overview.”

June

Mr. Alain Bauer, Criminologist at the Sorbonne University. “New Criminal Threats: A Good Look to the Enemy.”

Mr. Greg O’Hayon, Criminal Intelligence Analyst, CISC. “Early Warning for Organized & Serious Crime.”

Mr. Mark Jackson, Chief Meteorologist, National Weather Service. “National Weather Service & Support to Homeland Security.”

July

Mr. Ernie Lorelli, Penro Group. “Global IED Trends.”

GySgt Peter Archer, USMC. “IED Trends from Iraq Theater.”

Mr. Mark Chris Bausch, Red Team Intelligence, LLC. “Bomb (IED) Intel Concepts.”

August

Dr. Abraham R. Wagner, Colombia University. “Electronic Surveillance: Understanding the Context,”

Major John Persano, USMCR. “Intelligence Oversight Issues for DoD in CONUS.”

September

James D. Ballard, PhD, California State University Northridge. “Nuclear Power Protection.”

Bennett Ramberg, PhD, JD, Author: Nuclear Power Plants as Weapons for the Enemy (University of California Press). “The Politics of Preventing Terrorist Sabotage at Reactors.”

October

Frederick M. Wehrey, International Policy Analyst, RAND Corporation. “Muslim Apocalyptic Movements.”

SMSgt Ramon Barboa, Outreach Coordinator, California OHS. “CBRNE Training Opportunities.”

November

Mr. William Schnied, Director Special Operations, Global Projects LTD. "Cross-Border Insurgency Potentials."

Dr. Robert J. Bunker, Counter-OPFOR Corp. "Body Cavity Suicide Bomber Potentials."

2007

January

Maj. Lisa Campbell, CANG. "Cross-Border Violence Potentials: Beheadings in Mexico."

Dr. Jeffrey Upperman, Associate Professor of Surgery, Children's Hospital LA, Keck Medical School, USC. "Pediatric Disaster Preparedness."

February

Col. G.I Wilson, USMCR, ret., "Gangs, Terrorism, Netwar and Fourth Generation Warfare."

April

Peter Katona, MD, UCLA School of Medicine. "Epi-Surveillance."

Kevin Cresswell, VP Security and International Operations, Sayres and Associates. "Maritime Terrorism Overview."

May

Dr. Robert J. Bunker, Counter-OPFOR Corp. et al. "MS-13 and Improvised Online Communication Networks."

June

Mr. Jim Barnes, The Boeing Company. "Radiological and Nuclear Threats and Counter-Measures."

Mr. Hal Kempfer, KIPP Inc. "Terrorism Intelligence: Anticipating the Threat."

July

Gregory F. Treverton, RAND Corp. "The State of Domestic Intelligence: A Progress Report."

Matt Begert, NLETC. "Special Operations Theory and Counter-Terrorism."

August

Mr. Tomer Benito, Consultant. "Security Technology."

Mssrs Jeff Slivacka & Ken Post, ASI. "Concept for Integrated Sensing-Alerting-Warning System."

Lt. John Sullivan. “Proposed TEW-CAW Red Team Exercise.”

September

Professor Michael D. Intriligator, UCLA. “Globalization, Global Business, and Global Terrorism.”

Mr. Hakim Hazim, Consultant. “Revolt: The State Versus A State of Mind.”

October

Assoc. Prof. Amy Zegart, School of Public Affairs, UCLA. “Spying Blind: The CIA, the FBI, and the Origins of 9/11.”

Mr. Hal Kempfer, Knowledge and Intelligence Program Professionals. “Business Intelligence & Risk.”

November

Issac Maya, Director of Research, CREATE. “Risk and Economics Research at the USC CREATE Homeland Security Center.”

Peter Katona, MD, UCLA. “Vulnerability of Health Care Infrastructure.”

II. References

Criminal Intelligence Service of Canada (CISC). 2007. *Strategic Early Warning for Criminal Intelligence: Theoretical Framework and Sentinel Methodology*. This unclassified CISC paper details the processes used for strategic early warning for serious crime and demonstrates the utility of early warning approaches. It can be downloaded on line at:
http://www.cisc.gc.ca/products_services/sentinel/document/early_warning_methodology_e.pdf.

Gleghorn, Todd E. 2003. *Exposing the Seams: The Impetus For Reforming U.S. Counterintelligence*. Master's Thesis, Naval Postgraduate School. Gleghorn argues in favor of "devolving" U.S. counter-intelligence by centralizing it under a single agency with the authority to conduct foreign and domestic CI operations, with an analytical service to support it. Gleghorn also argues for the creation of regional fusion centers (with private sector support and involvement) to carry out the agency's mission. Gleghorn uses the Los Angeles Terrorism Early Warning Group as a model of local law enforcement intelligence operating within his proposed CI agency.

Grossman, Michael. 2005. *Perception Or Fact: Measuring The Effectiveness of the Los Angeles Terrorism Early Warning (TEW) Group*. Master's Thesis, Naval Postgraduate School. Grossman empirically evaluates the effectiveness of the Los Angeles Terrorism Early Warning Group (TEW), focusing on the TEW structure instead of its output. Grossman's examination leads him to the conclusion that the TEW is a model of collaborative network intelligence that can and should be replicated nationwide.

Jenkins, Brian Michael. 2003. "Connect the Cops to Connect the Dots." *San Diego Union Tribune*. June 1. RAND. <https://www.rand.org/commentary/060103SDUT.html> (accessed January 9, 2008). Jenkins evaluates new trends in counter-terrorism intelligence sharing and praises the Los Angeles Terrorism Early Warning Group (TEW) for its successes in overcoming interagency frictions.

Lanier, Cathy L. 2005. *Preventing Terror Attacks In The Homeland: A New Mission For State and Local Police*. Master's Thesis, Naval Postgraduate School. Lanier advocates the creation of a national law enforcement intelligence network, uniting municipal, state, federal, and tribal agencies into a common intelligence-sharing framework. Lanier's aim is to ensure that "every police officer" understands their role in preventing terrorist attacks. Lanier praises Los Angeles Terrorism Early Warning Group (TEW) as a model for regional preparedness.

Morrissey, James F. 2007. *Strategies for the Integration Of Medical and Health Representation Within Law Enforcement Intelligence Fusion Centers*. Master's Thesis, Naval Postgraduate School. Morissey argues for increased medical and health community representation in intelligence fusion operations. Morissey examines Terrorism Early Warning Group (TEW) epi-intelligence operations nationwide, including the Los Angeles TEW.

Rust, Sunchlar M. 2006. *Collaborative Network Evolution: The Los Angeles Terrorism Early Warning Group*. Master's Thesis, Naval Postgraduate School. Rust uses organizational social network theory to chart and analyze the Los Angeles Terrorism Early Warning Group (TEW) evolution to a regional counter-terrorism intelligence network. Rust praises the TEW for its consensus, problem solving skills, and mission-based structure while criticizing more traditional top-down organizations.

Sullivan, John P. *Book One: TEW Concept and Overview*: *National TEW Resource Center Resource Guide*, National TEW Resource Center, March 2006 (primary author).

Sullivan, John P. “Terrorism Early Warning and Co-Production of Counterterrorism Intelligence.” *INTSUM Magazine*. Marine Corps Intelligence Association, Volume XVII, Issue 8, Spring 2006.

Sullivan, John P. “Terrorism Early Warning Groups: Regional Intelligence to Combat Terrorism.” *Homeland Security and Terrorism: Readings and Interpretations*. Russell Howard, James Forrest, and Joane Moore (Eds). New York: McGraw-Hill. 2005.

Sullivan, John P. “The Terrorism Early Warning (TEW) Group: Multilateral Intelligence Fusion and Information Sharing.” *Protecting Your Community From Terrorism: The Strategies for Local Law Enforcement Series: Vol 4: The Production and Sharing of Intelligence*. Stephen A. Loyka, Donald A. Faggiani, and Cliff Karchmer (Eds), Police Research Forum, 2005.

Sullivan, John P. “Networked Force Structure and C41.” *Small Wars and Insurgencies*. Vol. 13, No. 2. Summer 2002. Reprinted in *Non-State Threats and Future Wars*, Robert J. Bunker (Ed), London: Frank Cass, 2003.

Sullivan, John P. “A Cooperative Vehicle for Threat Assessment, A Case Study: Los Angeles County Terrorism Early Warning (TEW) Group. *The Interagency Board for Equipment Standardization and Inter-Operability, 2000 Annual Report*. April 2001.

Sullivan, John P. “Intelligence Preparation for Operations: Developing Tools to Support Decision Making in Specific Incidents.” *The Interagency Board for Equipment Standardization and Interoperability, 2000 Annual Report*. April 2001.

Sullivan, John P. “ICIS Future Vision: Linking Emergency Responders Through a C4ISR Platform.” *The Interagency Board for Equipment Standardization and Interoperability, 2000 Annual Report*. April 2001.

Sullivan, John P. and Robert J. Bunker. “Multilateral Counterinsurgency Networks.” *Small Wars & Insurgencies*. Vol. 13, No.2 Summer) 2002. Reprinted in *Networks, Terrorism, and Global Insurgency*, Robert J. Bunker (Ed), London: Frank Cass, 2005.

Sullivan, John P., 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. Republished online as “Understanding Consequences in Urban Operations” at *OnPoint: A CounterTerrorism Journal, US Cavalry*.
<http://www.uscav.com/uscavonpoint/Feature.aspx?id=150>

Sullivan, John P., and James J. Wirtz. “Terrorism Early Warning and Counterterrorism Intelligence.” *International Journal of Intelligence and Counterintelligence*. Volume 21, Number 1, March 2008.

Welch, Alicia L. 2006. *Terrorism Awareness and Education As A Prevention Strategy For First Responders*. Master’s Thesis, Naval Postgraduate School. Welch argues that terrorism education and awareness is essential for first responders such as law enforcement and emergency operations personnel. She analyzes the Los Angeles Fire Department, as well as interagency cooperation. Welch praises the Los Angeles Terrorism Early Warning Group (TEW) for its information-sharing practices.

III. TEW Workshops and Conferences

The TEW's intellectual collaboration has not been limited to just threat level analysis meetings. Over the years, many military, law enforcement, academic, and private sector figures who have briefed the TEW have debated in conferences open to the public. This section lists the two "Terrorism, Security, and the Law," conferences held to date, as well as workshops on narrower subjects such as shoulder-fired missiles and cyberterrorism.

Terrorism, Security, and the Law

The first LA TEW *Terrorism, Global Security and the Law* Conference brought together leading specialists in the legal, military, law enforcement, intelligence, medical, and civil liberties communities to discuss global terrorism. As counterterrorism, as many have said, is now increasingly a law enforcement activity, there is much uncertainty over how to deal with civil liberties concerns in an era where the battlefield and home front are quickly blurring together. Public security professionals must contend with questions of legality, civil liberties, privacy, technical access, rules of evidence, and humanitarian concerns that their predecessors did not. The overriding theme of the conference was change. New definitions of "war," "combatant," and "enemy," are needed to accompany changing realities. New relationships and cooperation between civilians and public security personnel are needed to combat terrorism and global crime. And new legal structures are needed to continue to safeguard both American lives and civil liberties.

The second *Terrorism, Global Security, and the Law* Conference was held on 19-20 October 2006. It continued the themes discussed in the first event. Both Conferences were held at the RAND Corporation in Santa Monica. Both conferences included speakers and participants from across the United States and abroad.

Topical Workshops

A key element of the TEW experience has been the development of subject matter awareness and expertise for emerging threats. In order to inform analysts and decision-makers of the dynamics of the evolving threat environment, the TEW periodically holds topical workshops on issues that responders may face. Examples of these forums include a Suicide Bombing Workshop held on 21 November 2002, a MANPADS Workshop was held on 18 June 2003, and a Cyberterrorism Workshop was held on 17 October 2003.

TERRORISM
EARLY WARNING GROUP

Los Angeles Terrorism Early Warning Group
Conference June 1-2, 2005.
Terrorism, Global Security, and the Law

Day One

0730 – 0815 Registration and Coffee

0815 – 0830 Introduction

0830 – 0915 Plenary Session 1: Issues for Counterterrorism and Homeland Security
Dean Elizabeth Rindskopf – Parker, Mc George School of Law

0915 – 1000 Plenary Session 2: Evolving National Security and Homeland Security Issues
Honorable Gary Hart, former Senator, and former co-hair, Hart-Rudman Commission

1000 – 1015 Break

1015 – 1200 Breakout Session 1

1A: Detention and Trial of Terrorist Suspects Under U.S. and International Law
Professor Paul Finkelman, University of Tulsa School of Law
Professor Susan N. Herman, Brooklyn Law School.
Professor Katharina von Knop, University of Innsbruck
Ms. Renee C. Redman, International Institute of Connecticut
1B: Forensic Epidemiology: U.S. Issues
Dr. Jonathan Fielding, Los Angeles County Department of Health Services
Dr. Michael Allswede, Department of Emergency Medicine, University of Pittsburgh
Dr. Richard A. Goodman, CDC
1C: Operational Intelligence for Counterterrorism:
Ms. Sally Thomas, Los Angeles County District Attorney's Office
Ms. Beverly Reid O' Connell, U.S. Attorney's Office, Los Angeles
Mr. Michael Wermuth, RAND Corporation

1200 – 1330 Lunch and Luncheon Topic: Racial Profiling
Dr. Jack Riley, RAND Corporation

1330 – 1410 Plenary Session 3: Constitutional and Civil Rights,Privacy and Counterterrorism
Professor Susan N. Herman, Brooklyn Law School

1410 – 1415 Break

1415 – 1530 Breakout Session 2

2A: Trial of Terrorists in Civilian Courts and Military Tribunals

Mr. Philip Carter, McKenna Long & Alridge LLP
Mr. Philip Sundel, Law Offices of David P. Sheldon
Ms. Diane Marie Amann, UCLA Law School

2B: Quarantine and Isolation: Global Issues
Dr. Peter Katona, UCLA Medical School
Dr. Robert Kim-Farley, Los Angeles County Department of Health Services
Dr. Robert DeBell, The Titan Corporation

2C: Operational Intelligence for Counterterrorism: Global Perspectives
Detective Chief Superintendent Keith Weston, Metropolitan Police, United Kingdom
Detective Chief Inspector Paul Swallow, Metropolitan Police Special Branch, United Kingdom
Staff Sergeant Robert Taylor, Royal Canadian Mounted Police (RCMP)
Assistant Chief Bruce L. Cooke, U.S. Department of Homeland Security (USDHS), Office of Border Patrol

1530 – 1545 Break

1545 – 1715 Breakout Session 3

3A: Legal Access and New Technologies
Mr. Neal Pollard, Terrorism Research Center, Inc.
Rear Admiral (Ret). Alex Miller, the Titan Corporation
Professor David Koepsell, State University of New York (SUNY) Buffalo, School of Law and the Center for Inquiry, Amherst, New York

3B: Rendition, Detention, and Interrogation of Terrorist Suspects
Mr. Steven Watt, American Civil Liberties Union (ACLU)
Professor George Harris, McGeorge Law School

3C: Trends in Terrorism 1: Dealing with Suicide Bombers and Others
Dr. Anat Berko, International Policy Institute for Counter-Terrorism
Dr. Nasra Hasan, United Nations Office on Drugs and Crime
Mr. Joshua Sinai, U.S. Department of Homeland Security (USDHS)

1730 Reception

Day Two

0800 – 0830 Coffee

0830 – 0915 Plenary Session 4: Technology and Counterterrorism
Dr. Abraham Wagner, Columbia University

0915 – 1000 Plenary Session 5: Operational Issues in the Post 9/11 World
Mr. Brian Jenkins, The RAND Corporation

1000 – 1015 Break

1015 – 1200 Breakout Session 4

4A: International Cooperation in Financial Investigation, Enforcement and Trans-Border Data Sharing
Mr. Greg Treverton, RAND Corporation
Mr. Dale Watson, Federal Bureau of Investigation (FBI) (ret).

Brigadier General Annette L. Sobel, USAF National Guard Bureau
Mr. Adrian Baciu, Interpol

4B: Choice of Legal Regime
Professor Norman Abrams, UCLA Law School
Professor Barry Kellman, DePaul University, School of Law
Mr. Tom Feucht, U.S. Department of Justice (DOJ)
Professor Alison Renteln, University of Southern California (USC)

4C: Trends in Terrorism 2: Terrorist Operations in the Urban Environment
Colonel Lior Lotan, International Policy Institute for Counter-Terrorism
Colonel Reuven Berko, Ministry of Police, Jerusalem, Israel
Mr. Clifford Karchmer, Police Executive Research Forum (PERF)
Mr. Alejandro Lopez Carresi, Spanish Red Cross
Colonel Eran Duvdevani (Res.), The International Policy Institute for Counter-Terrorism

1200 – 1330 Lunch and Luncheon Topic: Nuclear Terrorism: The Ultimate Preventable Catastrophe
Professor Graham Allison, Kennedy School of Government, Harvard University

1330 – 1415 Plenary Session 6: Emerging Legal Issues
Professor Jack Goldsmith, Harvard Law School

1415 – 1530 Breakout Session 5

5A: Emerging Legal Issues
Ms. Suzanne Spaulding, The Harbour Group, LLC
Professor Cottrol, George Washington School of Law
Mr. Ahilan T. Arulantham, American Civil Liberties Union (ACLU)
Honorable Jack Weiss, Councilman, Los Angeles City Council

5B: Comparative Terrorism Law: Case Studies
Dr. Mary Bossis, Pompandreau Center
Professor Andrew Silke, University of East London
Dr. William Rosenau, RAND Corporation

5C: Private Military and Intelligence Companies
Mr. Philip Carter, McKenna Long & Alridge LLP
Dr. Robert J. Bunker, National Law Enforcement and Corrections Technology Center-West (NLECT-West)
Mr. Doug Brooks, International Peace Operations Association
Mr. Mark Troy, McKenna Long & Aldridge LLP
Mr. Steve Cooley, Los Angeles County District Attorney

1530 – 1545 Break

1545 – 1715 Plenary Session 7: Conference Wrap-Up
Lt. John P. Sullivan, LA TEW
Dr. Abraham Wagner, Columbia University
Dr. Peter Katona, UCLA Medical School\
Ms. Geneviere Lester, UC Berkeley

Note: A transcript of this event can be found online at the Terrorism Research Center.
http://terrorism.com/modules.php?op=modload&name=document&file=get&download=565

TERRORISM
EARLY WARNING GROUP

Los Angeles Terrorism Early Warning Group
Conference 19-20 October 2006
Terrorism, Global Security, and the Law.

Thursday, October 19

7:30-8:15: Registration and Coffee: RAND Corporation Conference Center

8:15-8:30: Introduction
Lt. John P. Sullivan, Los Angeles TEW
Dr. Abraham Wagner, Columbia University, School of International and Public Affairs (SIPA)
Dr. Greg Treverton, RAND Corporation.

8:30-9:00: Welcome: Honorable Steve Cooley, Los Angeles County District Attorney.

9:00-9:30: Keynote: Mr. Brian Jenkins

9:30-10:45: Plenary Session 1: Surveillance and Constitutional Issues

Dr. Abraham Wagner, Columbia University, School of International and Public Affairs (SIPA)
Dr. K.A. Tipale, Center for Advanced Studies in Science and Technology Policy
Prof. Paul Finkelman, Albany Law School

10:45-11:00: Break

11:00-12:15: Breakout Session 1

1A Counter-Terrorism: Tools and Approaches
Moderator: Mr. Eroll G. Southers, University of Southern California, CREATE
Prof. Detlof von Winterfeldt, University of Southern California, CREATE
Prof. Don Kleinmuntz, University of Southern California, CREATE.
1B Intelligence Sharing and Co-production
Moderator: Maj. General Annette Sobel, USAF and Sandia Laboratory
Dr. Greg Treverton, RAND Corporation
Prof. Jennifer E. Sims, Georgetown University
Prof. Amy Zegart, University of California at Los Angeles
Mr. Brent Durbin, University of California, Berkeley

12:15-1:30: Lunch:

Prof. Mark Danner, University of California, Berkeley. “Taking the Gloves Off: Terrorism, Torture, and Executive Power.”

1:15-2:00: Keynote: Representative Jane Harman (D-CA), House Permanent Select Committee on Intelligence.

2:00-3:15: Plenary Session 2: Torture, Rendition, and Detention

Mr. Scott Horton, Patterson Belknap Webb & Tyler
Prof. Rosa Brooks, Georgetown University Law Center
Mr. John Sifton, Human Rights Watch
Dr. Anat Berko, Institute for Counter-Terrorism (ICT) in Israel.

3:15-3:30: Break

3:30-5:00: Breakout Session 2
2A The Legal Landscape of Public Health Preparedness and Disaster Response
Dr. Peter Katona, David Geffen School of Medicine, University of California at Los Angeles
Dr. Richard A. Goodman, Centers for Disease Control and Prevention (CDC)
Dr. Peter A. Baldridge, California Department of Health Services
Prof. David P. Fidler, Indiana University School of Law
Dr. Robert Ragland, Los Angeles County Department of Public Health
2B Private Military Companies
Moderator: Mr. Philip Carter, McKenna Long and Aldridge, LLP
Prof. Deborah Avant, George Washington University, School of International Affairs
Mr. Derek Wright, International Peace Operations Association (IPOA)
2C The TEW Experience
Moderator: Lt. John P. Sullivan, Los Angeles TEW
Mr. Mark Hogan, Tulsa TEW
Dr. Greg O'Hayon, Criminal Intelligence Service, Canada
Ms. Sally Thomas, Los Angeles County District Attorney's Office

5:30: Reception

Friday, October 20

7:30-8:15: Registration and Coffee: RAND Corporation Conference Center

8:15-9:15 Plenary Session 3: Executive Power and the War on Terror
Moderator: Paul Finkelman, Albany Law School
Prof. Joe Marguiles, Northwestern University Law School
Prof. Philip Bobbitt, University of Texas Law School
Prof. Kal Raustiala, University of California at Los Angeles Law School

9:15-10:30: Breakout Session 3
3A: Information Sharing and Intelligence Production
Mr. Mike Himley, Eagle Intelligence
Mr. John Gordnier, Department of Justice, State of California
Mr. Neal A. Pollard, National Counterterrorism Center
Mr. Peter S. Probst, Center for Advanced Studies on Terrorism
Mr. Chuck Dodson, Oracle Corporation
3B Regimes for Global Security
Moderator: Professor Mike Intrilligator, University of California at Los Angeles and Milken Institute.
Prof. Joanne St. Lewis, University of Ottawa, Canada.
Dr. Katharina von Knop, George C. Marshall Center, Germany.

Dr. Nasra Hassan, United Nations Crime and Drug Officer, Austria.
Prof. Dejan Milectic, Braca Karic University, Serbia.
10:30-10:45: Break

10:45-12:00: Plenary Session 4: Bioterrorism Emergency Preparedness and Pandemic Influenza
Moderator: Dr. Jonathan Fielding, Los Angeles County Department of Public Health
Dr. Harvey Rubin, University of Pennsylvania, School of Medicine

12:00-1:30: Lunch
Speaker: Prof. Ian Lustick, University of Pennsylvania. "Trapped in the War on Terror."

1:30-3:00: Breakout Session 4
4A Military Commissions and the Law
Prof. Diane Marie Amann, University of California at Davis Law School
Mr. Philip Carter, McKenna Long and Aldridge, LLP
Prof. David W. Glazier, Loyola Law School
Prof. Gary Solis, Library of Congress and Georgetown University Law Center
4B Operational Intelligence and the Emergent Threat
Dr. Robert Bunker, Los Angeles TEW
Dr. Lars Nicander, Swedish National Defense College
Dr. Paul Swallow, United Kingdom

3:00-3:15: Break

3:15-5:00: Plenary Session 5: Civil Liberties and the War on Terror
Moderator: Prof. Paul Finkelman, Albany School of Law
Prof. Susan Herman, Brooklyn Law School
Ms. Renee Redman, Legal Director, ACLU of Connecticut
Prof. Philip Heymann, Harvard Law School

5:00-5:30: Conference Wrap-Up—Closing Remarks.
Lt. John Sullivan, LA TEW
Dr. Abraham Wagner, Columbia University, School of International and Public Affairs (SIPA)
Dr. Greg Treverton, RAND Corporation
Ms. Geneviere Lester, University of California, Berkeley and Center for Advanced Studies on Terrorism (CAST)

TERRORISM
EARLY WARNING GROUP

RAND ArroyoCenter
ARMY RESEARCH DIVISION

NATIONAL TACTICAL OFFICERS ASSOCIATION

TERRORISM
RESEARCH CENTER

LA TEW SUICIDE BOMBING WORKSHOP

THURSDAY, 21 NOVEMBER 2002, 0900 - 1700
Sponsored by LA TEW, RAND, TRC & NTOA (NTOA Certificate)

AGENDA

09:00 - 09:15	**INTRO /WELCOME** Sgt. John Sullivan, LASD/TEW Russell Glenn, RAND Lt. Phil Hansen, NTOA
09:15 - 10:00	**SUICIDE OPERATIONS & THE FUTURE** Brian M, Jenkins, RAND
10:00 - 10:45	**HISTORICAL PERSPECTIVES (LTTE/HAMAS)** Walter Purdy, TRC
10:45 - 11:00	Break
11:00 - 11:45	**SUICIDE ATTACKS WORLDWIDE** Walter Purdy, TRC
11:45 - 13:00	**Lunch**
13:00 - 14:00	**LOS ANGELES: ISRAEL AFTER-ACTION REPORT** Sgt. Heidi Clark, LASD, Dep. Mark Seibel, LASD
14:00 - 14:45	**TACTICAL ISSUES** Capt. Mike Hillman, LAPD, Lt. Phil Hansen, LASD
14:45 - 15:00	Break
15:00 - 15:45	**FIELD EMS / MEDICAL RESPONSE** Fadi Essmael, M.D.
15:45 - 16:30	**FUTURE MEDICAL THREAT SCENARIOS (Human CBRN Bombs)** Peter Katona, M.D.
16:30 - 17:00	**LA TEW SUICIDE BOMBING PLAYBOOK** Presentation and Panel Discussion

TERRORISM EARLY WARNING GROUP

RAND Public Safety and Justice

ENVISIONEERING

CENTER for ASYMMETRIC WARFARE

NAVAIR

National Law Enforcement and Corrections Technology

alpa AVIATION SECURITY

LA TEW MANPADS WORKSHOP

WEDNESDAY 18 JUNE 2003, 0800 - 1430
Location: Northrop Grumman Space Technology
One Space Park Drive, Bldg. R10, Redondo Beach, CA

AGENDA

0800 - 0830	Coffee/Registration, Administrative Instructions
	Welcome: Sgt. John P. Sullivan, LASD Pat Caruana, V.P. of Missile Defense, Northrop Grumman
0830 - 0920	**MANPADS Threat** • **Introduction to MANPADS** John O'Malley, NASA • **Historical Perspective** Arman Tchoubineh, Joint Warfare Programs Office, NAVAIR
0920 - 0930	**Break**
0930 - 1010	**Future Threat:** • Jim Chow, Manager, Technology and Applied Sciences, RAND
1010 – 1020	**Break**
1020 - 1110	**Threat Envelope: Airline Pilots Perspective** Captain Clyde Romero, Jr., Air Line Pilots Association
1110 – 1125	Pick-up Lunch
1125 - 1225	**Working Lunch/Case Study: Mombassa Attack** David Kuhn, Law Enforcement Instructor, Miami-Dade County
1225 - 1325	**MANPADS Countermeasures (Laser Approach)** Jeff Hassania, Dir. Missile Defense Marketing, Northrop Grumman Alvin Schnurr, Laser Weapons Manager, Northrop Grumman
1325 - 1335	**Break**

1335 - 1430 **Open Session:**
Response: Airport Consequence Management
Chief Dan Lindsay, Ontario International Airport

1335 - 1430 **Concurrent Classified Session** (SECRET//NOFORN):

1340 - 1410 Asymmetric Threat:

- Jim Kuga, Envisioneering, Inc.

1410 - 1440 **MANPADS THREAT**

- Mike Schuck, Dir. Ctr. for Countermeasures, White Sands
- Arman Tchoubineh, Joint Warfare Programs Office, NAVAIR

1430 **Close**

LA TEW CYBERTERRORISM WORKSHOP

Co-sponsored by LA TEW, Dartmouth College: Institute for Security Technology Studies, Terrorism Research Center, RAND Public Safety & Justice, National Law Enforcement and Corrections Technology Center-West

FRIDAY 17 OCTOBER 2003, 0800 – 1630
LAFD Frank Hotchkins Memorial Training Center
1700 Stadium Way, Los Angeles

AGENDA

0800 - 0830	**Coffee/Registration**
0900 - 0915	**Introduction & Welcome:** Sgt. John P. Sullivan, LASD LA TEW
0915 - 1015	**Cyberterrorism** Matt Devost, Terrorism Research Center
1015 - 1030	**Break**
1030 - 1200	Critical Infrastructure Vulnerabilities and Threats Eric Goetz, Sr. Research Analyst, I3P/ISTS, Dartmouth College
1200 - 1300	**Lunch**
1300 – 1350	**Deception Techniques for Computer Network Defense** Scott Gerwehr, RAND
1350 – 1400	**Break**
1400 – 1500	**Cyber Target Folders & Playbook** Trey Gannon, Sr. Research Associate, ISTS, Dartmouth College, Thayer School of Engineering
1500 – 1550	**Cyber Capabilities of Islamic Terrorist Groups** Andrew Macpherson, Technical Program Coordinator, Technical Analysis Group, IT IS, Dartmouth College
1550 - 1630	**Closing Panel: How to Apply Workshop Lessons to the TEW Process** John McIntire, Associate Chief Information Officer, LA County Sgt. John P. Sullivan, LASD/LA TEW Peter Katona, M.D., UCLA School of Public Health SSA Robert Kellison, Cyber Branch, FBI, Los Angeles

Author Biographies

Leroy D. Baca

Leroy D. Baca is Sheriff of the County of Los Angeles. Sheriff Baca commands the largest Sheriff's Department in the United States with a budget of 2.4 billion dollars. He leads over 18,000 budgeted sworn and professional staff. The Los Angeles County Sheriff's Department is the law enforcement provider to 40 incorporated cities, 90 unincorporated communities, 9 community colleges, and hundreds of thousands of daily commuters of the Metropolitan Transit Authority and the Southern California Regional Rail Authority. The Sheriff's Department also protects 58 Superior Courts and 600 bench officers. Moreover, the Department manages the nation's largest local jail system housing over 20,000 prisoners. Sheriff Baca is the Director of Homeland Security-Mutual Aid for California Region I, which includes the County of Orange. Sheriff Baca earned his Doctorate of Public Administration from the University of Southern California. He is a life member of the Honor Society of Phi Kappa Phi, USC Chapter. Sheriff Baca was elected Sheriff of Los Angeles County in December 1998, and was re-elected in June 2006 for his third term in office. He entered the Sheriff's Department on August 23, 1965. He served in the United States Marine Corps Reserves.

Alain Bauer

Alain Bauer is a criminologist. He is President of the French National Crime Commission, President of the Strategic Security Mission to the President of France, and President of the French National CCTV Commission. From 1981-1988 he served as Vice President of the Sorbonne University (Paris I) and as an advisor to French Prime Minister Michel Rocard (1988-1990). Mr. Bauer has served as a criminologist at Sorbonne University (Paris I, Paris II, Paris V), Gendarmerie Higher Studies Center, National Magistrate's Academy, and National Superior Police Academy. He also serves as a Senior Fellow at the Center on Terrorism at John Jay College of Criminal Justice, Chinese Criminal Police Academy in Shenyang, Political Science University of Beijing, and the Canadian Police College. He is a Colonel (Reserve) of the French Air Force. Mr. Bauer is a consultant to the New York Police Department, Los Angeles County Sheriff's Department, and Sûreté du Québec (Canada). He is the author or co-author of numerous texts, including *Violence et Insécurité urbaines, Imaginer la sécurité globale, World Chaos, Early Detection and Proactive Security, and Radicalization in the West* (NYPD, 2007). Mr. Bauer is a Knight of the Légion d'honneur, Captain of the National Order of Mérit, Captain of the National Order of Academic Palms, Captain of the National Order of Arts and Letters, and has been awarded the Grand Cross of the Lafayette Order.

Andre Demarce

Andre Demarce is an independent consultant in the field of global security, terrorism and insurgency analysis. His focus is terrorist and insurgent group strategies, tactics and organizational dynamics. In previous positions at the Terrorism Research Center, Inc. (TRC), he authored strategic intelligence reports on global security, political stability, terrorism and insurgency issues for corporations, academic institutions, and governmental bodies, as well as military, intelligence and law enforcement agencies. Mr. Demarce also conducted terrorist and insurgent 'red teaming' threat scenario development, war-gaming, instruction, and exercise support. Mr. Demarce holds a Master of Arts in Security Policy Studies from the Elliott School of International Affairs at The George Washington University in Washington, D.C., with concentrations in Transnational Security and Political Psychology.

Brian M. Jenkins

Brian Michael Jenkins is Senior Advisor to the president of the RAND Corporation and one of the world's leading authorities on terrorism and international crime. He founded the RAND Corporation's terrorism research program 36 years ago, has written frequently on terrorism, and has served as an advisor to the federal government and the private sector on the subject. He is a decorated combat veteran who served as a captain in the Green Berets in the Dominican Republic and later in Vietnam (1966-1971). He also was a former deputy chairman of Kroll Associates. In 1996, he was appointed by President Clinton to be a member of the White House Commission on Aviation Safety and Security. He has as served as an advisor to the National Commission on Terrorism (1999-2000) and in 2000 was appointed as a member of the U.S. Comptroller General's Advisory Board, a continuing assignment. Mr. Jenkins is also a special advisor to the International Chamber of Commerce (ICC) and a member of the board of advisors of the ICC's Commercial Crime Services. He has authored many books, including *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves, International Terrorism: A New Mode of Conflict,* and is the editor and co-author of *Terrorism and Personal Protection*, co-editor and co-author of *Aviation Terrorism and Security*, and co-author of *The Fall of South Vietnam*. His new book, *Will Terrorists Go Nuclear?* is available in September 2008.

Xavier Raufer

Professor Xavier Raufer is a Professor at the Paris Criminology Institute and Director of the Department for the Study of the Contemporary Criminal menace at the Pantheon-Assas Paris II University (*Université Panthéon-Assas Paris II*). He also serves as an Associate Professor at the Chinese People’s Security University in Beijing and Shenyang. He is editorial advisor to Editions Odile Jacob in Paris and author of several books in French on criminology, terrorism and related matters. These texts include *Dictionnaire Technique et Critique des Nouvelles Menaces, Violences et Insécurité Urbaines, Le crime organisé*. He also edited *Mafias, triades, cartels: la criminalité organisée dans le chaos mondial* and *Le nouveau Chaos mondial: penser la sécurité dans un monde chaotique, principes et perspectives* (with Alain Bauer). He received his Doctorate in Geography/Geopolitics from the University of Paris-Sorbonne and his Masters in Geopolitics/Terrorism Studies from the *Université de Marne-la-Vallée*.

John P. Sullivan

John P. Sullivan is a lieutenant with the Los Angeles County Sheriff’s Department. He currently serves as Tactical Planning Lieutenant managing command and control teams and crisis action planning. He is also responsible for special projects for counterterrorism, intelligence and emergency operations. His immediate past assignment was director of the National TEW Resource Center. He is co-founder of the Los Angeles Terrorism Early Warning (TEW) Group. He is a practitioner and researcher specializing in conflict studies, terrorism, gangs, intelligence, and urban operations. He holds a Bachelor of Arts in Government from the College of William and Mary and a Master of Arts in Urban Affairs and Policy Analysis from the New School for Social Research. He is co-editor of *Countering Terrorism and WMD: Creating a Global Counter-Terrorism Network* and author or co-author of *Jane’s Unconventional Weapons Response Handbook, Jane’s Facility Security Handbook, Policing Transportation Facilities*, as well as over 50 chapters or articles on terrorism, policing, intelligence and emergency response.

Acknowledgements

This edited collection, like any complex work, benefits from the contributions of many people. The editors would like to specifically thank the following persons for their efforts: Adam Elkus for his editorial assistance; Chris Bausch, Hal Kempfer, Dr. Robert Bunker, Matt Begert, and Charlie Bell for their contributions to the many processes and concepts described here. All the participants in the Terrorism Early Warning (TEW) Group's many conferences exercises, meetings and activations helped influence this work, while too numerous to mention individually, they all made unique contributions. Matt Devost, Ed Reed, and their partners at the Terrorism Research Center, Inc. and General Dennis Reimer and Brian Houghton at the Memorial Institute for the Prevention of Terrorism helped spread the TEW concept nationwide. Dr. Abraham Wagner, Center for Advanced Studies on Terrorism deserves recognition for his efforts in co-chairing the TEW's Annual Conferences at RAND. Many individual analysts at RAND helped inform the TEW's understanding of terrorism. These include co-author Brian Micheal Jenkins, Mike Wermuth, Maury Eisenstein, Russ Glenn, Jamie Medby, Greg Treverton, and Scott Gerwher. Sergeant Pete Jackson and Deputy Dennis Stangeland both contributed to the case study captured in Part Three. Sheriff Lee Baca encouraged us to produce this book. We thank him for his vision and support. We also thank our contributors, the aforementioned Sheriff Baca and Brian Michael Jenkins, as well as Xavier Raufer and Andre DeMarce. Reserve Captain Matt Wollman also played an important role in coordinating our cross-Atlantic interactions. Finally, a number of dedicated professionals helped transform the manuscript into a final product. These include Captain Margie Wagner, Graphics Specialist Sandra Enslow, Graphics Specialist Ignacio Mendoza, Operations Assistant III Cristina Casteneda at Sheriff's Headquarters Bureau, and the printing staff at the North County Correctional Facility Sergeant Edward Elliott, Deputy Barry Ellsworth, Vocational Instructor Ryan Wheeler, and Don Lynn and Jim Peterson, both teachers from the La Puente School District.

— John P. Sullivan and Alain Bauer, Los Angeles 2008

Terrorism Early Warning

10 YEARS OF ACHIEVEMENT IN FIGHTING TERRORISM AND CRIME

Los Angeles County
Sheriff's Department

www.lasd.org