OnPoint. Stay Informed, Stay in Touch, Stay in Front
A CounterTerrorism Journal
for Military and Law Enforcement Professionals

Understanding Consequences in Urban Operations

by **John P. Sullivan, Hal Kempfer, Jamison Jo Medby**

Abstract: This paper addresses the concept of operational intelligence for homeland security and terrorism. It defines Intelligence Preparation for Operations (IPO), as a concept for addressing the intelligence needs entailed in responding to terrorism and operating in urban environments. As such, IPO includes consequence management intelligence, and is designed to facilitate "all-source/all phase fusion." It should be noted that IPO is applicable in CONUS as well as in expeditionary operations. By definition IPO is multidisciplinary and bridges civil-military divides. IPO builds from IPB, Urban IPB, Consequence Management Intelligence, and the Terrorism Early Warning Group (TEW) process. IPO also integrates all intelligence disciplines (e.g., GEOINT, MASINT, Epi-Intel, etc.) into operational intelligence.

Effective response and management of complex urban operations—including terrorist attacks or campaigns, insurgency, natural disasters and public order situations—require information to be developed into intelligence to prepare for operations and ultimately to provide knowledge for commanders responsible for these operations. Commanders from local, state, federal, and military agencies need timely access to accurate information that includes a net assessment of all of the threats, real-time situation and resource status reports, and an adequate intelligence picture of the operational area.

Net Assessment of the Threat Envelope—Complex Opspace

The current operational environment is characterized by a series of inter-related conflicts on a global scale. As such the distinctions between foreign and domestic, crime and war, terrorism and insurgency are blurring. This complex operational space (Opspace) is the realm of fourth generation warfare (4GW). It is populated by networked threat actors, global crime, transnational threats, global insurgency, and humanitarian disasters. New intelligence approaches are required to craft responses to this global threat envelope. Postmodern security forces are and will continue to be faced with networked adversaries in a variety of settings, many in an urban environment. The urban operations segment of this threat envelope requires what General Montgomery C. Meigs describes as ‘a shift in the nature of the art of operations.’ The consequences of the information age and the attendant changes in the geopolitical situation and the nature of war are influencing the operational landscape.

Conventional forces on the one hand, and terrorists and a range of fourth generation non-state soldiers on the other are exploiting rapid advances in information and communications systems, improved sensors, precision guidance systems and the availability of novel off-the-shelf technology. Political and cultural factors, media intensity, and adaptation of networked organizations and command and control structures combine to contribute to new strategic challenges. Among the contemporary realities cited by Meigs is the employment of forces, usually in an incremental manner, in joint, combined or multinational formations. These joint/combined forces are likely to face an entrenched adversary fighting on his own turf with an initial numerical—and intelligence—advantage in a complex operational space (Opspace). According to Meigs:

'We will be operating on a very complex battlefield that combines the challenges of difficult and unfamiliar terrain, terrorists and paramilitaries, and refugees and unfriendly civilian organizations (some possibly having links to internationally networked organized crime).'

This observation implicitly acknowledges the continued expeditionary nature of future conflict. To that, it is necessary to add that much of this potential complex op- or battlespace will be urban, likely necessitating urban expeditionary operations. Some of these urban operations will occur in Mega-cities. Others may even be at home, involving civil public safety agencies (police, fire and health services), and potentially requiring military participation in "coalition-type" operations in support of domestic law enforcement and public safety agencies.

Urban Intelligence Challenges

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.

Urban operations are fraught with complexity. Increased operational tempo (due to the multiplicity of interpersonal and terrain interactions), compressed decision times, and a density of potential C2 systems complicate matters. Command and control are chaotic in intense urban situations. Communications and intelligence are frequently subject to degradation in these settings, since urban clutter limits the effectiveness of many sensor and communications technologies. As a result, control often devolves to a small-unit or squad level, increasing demand for accurate, real-time situational awareness at all echelons—a situational awareness that is both elusive and often hard to achieve.

The U.S. Army has tried to develop better situational awareness for both the tactical and strategic level soldiers by augmenting its intelligence collection and processing methodology. The method, called Intelligence Preparation of the Battlefield (IPB), is what the Army uses to assess the weather, terrain, buildings, infrastructure, non-combatant, and the threats in the area to which they will be deployed. It seeks to describe how all of these elements will act and react during urban operations in ways that can affect a unit's goals.

Intelligence Preparation of the Battlefield for Urban Operations

Urban operations and the densities that characterize them put a premium on gathering and interpreting data in ways that can support mission goals and situational understanding. Intelligence preparation of the battlefield (IPB) for urban areas tries to manage the operational complexities of these densities by dissecting and describing each relevant component of an urban area and the connections among them. In so doing, it highlights the most relevant characteristics of the environment, how they will affect operations, and how they might be shaped by them.

Urban IPB is conducted using four on-going steps that seek to demonstrate how the various conditions present in an urban area can affect and be affected by adversary and friendly activities within it. The four steps of urban IPB, along with brief descriptions, are listed below.

Step One—Define the operating environment
This step requires the analyst to identify the area for which the unit is responsible as well as any contiguous or non-adjacent areas that can affect operations. This step also requires the analyst to identify gaps in intelligence related to the operational area and the threat.

Step Two—Describe the operating environment
This step creates a picture of the operating environment. It describes all of the buildings, infrastructure, populations, terrain and weather that can affect operations. Descriptions include details about criticality and redundancy of infrastructure, construction and architecture of buildings and roads, diversity and relationships of population groups, identification of prominent media outlets or personages, restricted areas, legal issues, an assessment on the unit's allies, and the beginnings of a vulnerability assessment for all

relevant entities in the operational area. The objective is to assess the opportunities and constraints presented by the operational area to friendly, adversarial and non-aggressive population elements.

Step Three—Identify and Evaluate the Threat
Most often, IPB is conducted for operations being conducted against an already identified adversary. For this adversary, its capabilities (including composition, disposition, strength, leadership, weapons and the like), interests, intentions and any means it has to exploit a friendly vulnerability are described. Its doctrine, tactics, techniques and procedures are also analyzed.

The densities and diversity of urban populations require that this step also include identification and evaluation of other threats that might be present in the area. These threats might range from other groups seeking to do harm to the area or the friendly unit to well-meaning citizens who simply might get in the way during an operation.

As a result of this range of possible threats in an urban area, it becomes necessary to identify and assess the most threatening elements and evaluate all of the ways these elements can negatively influence mission goals. Identification of which population groups are neutral and allied to the friendly unit is also critical to understanding how they might be used to assist the friendly unit and how to keep them out of harm's way. The Continuum of Relative interests can help to achieve this goal. The Continuum is a method for mapping the allegiance to the friendly unit based on each element's interests, intentions, capabilities to harm or help the friendly unit, and the friendly vulnerability to this capability. For instance, a population element with the capability to do harm, but not the intent, would not be considered an adversary, but somewhere along the continuum between accomplice and obstacle. These types of groups must be monitored to ensure that friendly or adversary actions in the operational area do not create intent to harm the friendly unit. They should also be monitored for opportunities to co-opt or otherwise use these population elements to pursue friendly goals.

Step Four—Develop Courses of Action for Adversary, other threats and non-aggressive groups including potential higher order effects.

Once the population is parsed and categorized from adversary to ally, the actions of the most adversarial elements need to be predicted. In step four, the capabilities, doctrine, tactics, techniques and procedures (TTPs), intentions, what is known about friendly vulnerabilities and defenses, and other information known about how the adversary can operate is mapped onto the opportunities and constraints presented by the operational area to develop feasible predictions of its behavior called courses of action (COA). Several COA are developed to depict how an adversary can act within the area, including most likely, least likely and other likely scenarios. Each COA developed also includes hypotheses of the second and higher order effects that will occur as a result of adversarial activity. For example, if a COA involving a chemical attack on a train station is developed, the indirect effects that should be considered in step four include impacts on medical care facilities, first responders and the transportation system for the area.

COA for each element of the population should also be addressed. These should identify ways each element can assist the friendly unit, as well as ways it might be turned to assist the adversary.

Overall, urban IPB is intended to systematically reduce the guess work involved in adversary activity by helping analysts know what to look for, where to look for it, and how to act upon information once seen. It provides critical operational intelligence to army units during urban operations.

Operational Intelligence

Operational intelligence is the result of analysis and synthesis of all information needed to negotiate the operational environment. It is informed by—and informs—strategic intelligence. Essentially, operational intelligence (OPINT) is the actionable, vetted and validated information needed by decision-makers, commanders and operators at the operational level. It includes information about the adversary (or opposing force/OPFOR), their composition or network architecture, their capabilities and intentions, as well as the tactics, techniques and procedures (TTPs) they might employ at a given point in time to meet their objective. In addition, OPINT includes information about the Opspace where they may chose to operate or where we may be attacked, current and future weather, and our response capabilities. As such, operational intelligence involves all steps toward achieving all-source situational understanding.

Operational intelligence is not criminal intelligence aimed at achieving a criminal prosecution. Rather, OPINT complements criminal intelligence by providing investigators with the context they need to conduct operations while informing other operators of the dynamics involved in the criminal investigation along with all other pertinent factors which influence operations at given points in time.

Operational intelligence is the result of fusing the many separate intelligence disciplines to achieve all-source/all-phase intelligence. That is, exploiting all sources of information—classified, sensitive open sources (OSINT)— to address the information requirements at all phases of response: pre-, trans-, and post-incident. To do so, operational intelligence incorporates concepts and tools from consequence management intelligence, risk management intelligence, epidemiological intelligence, OSINT, and traditional intelligence disciplines, as well as new tools such as social network analysis, cyber intelligence (cyberINT), and a variety of technical means known as forensic intelligence support. These are linked with investigative/criminal intelligence to provide a complete picture. Intelligence preparation for operations (IPO) is a mechanism for achieving operational intelligence.

Intelligence Preparation for Operations

Developing 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. 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. IPO was developed by the IPO working group of the Los Angeles Terrorism Early Warning Group (LA TEW). The IPO working group is composed of full-time and adjunct members of the LA TEW from a variety of disciplines: law enforcement, the fire service, emergency medical services, hazmat, public health, several military services and combat arms, social scientists, and intelligence practitioners from local, state, federal and private organizations.

IPO is the synthesis of several multidisciplinary approaches to developing operational intelligence. As a starting point, IPO combines traditional military concepts of weather, enemy, and terrain with the emerging concepts of Urban Intelligence Preparation of the Battlefield, with the TEW process to achieve All Source Situational Understanding (ASU).

The cornerstone of the IPO toolkit is the TEW process, which was developed by the LA TEW over eight years of practice. The TEW has two major missions: indications and warning (I&W) and operational net assessment (ONA). The TEW process traditionally involved assessing trends and potentials on an on-going basis (known as scanning), adding an assessment of capabilities, especially during a known threat period (known as monitoring), and then developing a net assessment to provide to operational decision makers (forecasting). To do so, the LA TEW utilizes a number of tools, including response information folders, playbooks, and mission folders. Building from this foundation, IPO emphasizes Mission Folder development: a package of standardized playbooks, target (response information) folders, intelligence reports and a standardized "Mission Folder" for sharing incident information. The IPO process organizes and displays information in standard format designed to minimize ambiguity and speed the decision cycle.

The IPO Process

Building from the above elements, Intelligence Preparation for Operations (IPO) emerged as a distinct process for understanding and preparing for terrorist threats. The IPO Process is depicted in Figure 1. First, IPO is not linear (as in the case of linear case analysis), and is configured to address multiple threats, potentials, incidents, or events at any given point in time. Essentially rather than being viewed as a two-dimensional plane, IPO is best viewed as a three-dimensional canister, where the analytical team can be addressing more than one step at a time.

Figure 1: IPO Process

The Core of IPO

The center or 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 actionable intelligence. Embedded into this core in the entire classical intelligence process (in its many variations), including direction, collection, processing, production and dissemination. These steps are represented in short hand by "collection management" (i.e., getting the information) and "situational understanding" (i.e., interpreting the information). This core drives IPO's four steps through the process of pulsing out requests for information (RFIs) at all steps.

This core relies upon all-source collection and analysis. Whereas this term "all-source" regarding intelligence isn't new, the concept of applying it to both collection and analysis processes is different. Using a plethora of collection means (i.e., human, signals, electronic, imagery, etc.) is synonymous to all-source intelligence. In the military, analysis is primarily performed by intelligence specialists or officers and at higher levels by civilian analysts. IPB and all-source intelligence or what is sometimes called all-source fusion is usually a collections focused endeavor.

However, IPO deals with a world, not a notional "battlefield" that we are finding less likely to encounter today (hence the current "military intelligence" problems or "failures" of conducting asymmetric warfare in Iraq, Afghanistan, the Balkans and elsewhere around the world). IPO is built upon the premise of bringing together experts in multiple disciplines and organizations to drive the intelligence collection and analysis effort in preparation for or support of operational decision-making. IPO also assumes that the operations are not necessarily battle-focused, but can include a vast array of operations and operation approaches. All of this is designed at developing a very high degree of situational awareness at the center.

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 of defining the Opspace 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. A refined way of understanding the Opspace considers the local situation and terrain, looks at global connections and dynamics, and then looks at global influences on the local (e.g., the presence of Diaspora communities). It is in this step that "critical" or "influencing" structures as defined in urban operations challenges above would be defined.

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 (i.e., terrain awareness tools configured as

standardized information packages on what an adversary, such as al-Qaeda, would consider likely, high value or high pay-off targets). Response Information Folders are comprehensive venue-specific tools. They serve as an awareness tool to guide an integrated emergency response to a specific, high profile target within a specific jurisdiction. A RIF includes site plans, terrain analysis, interior and exterior plume dispersal models, blast analysis, maps indicating vulnerable points, potential sites for incident activities among other factors. The RIF Template utilized by the LA TEW is depicted in Figure 2.

Also in this step, information is collected and analyzed to understand an array of considerations and inputs such as population, terrain and weather. These factors are then considered among a variety of settings or context (i.e., what is influencing or surrounding the actions anticipated or taking place). Cultural features, including cultural intelligence or CULTINT (including "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) including potential infrastructural interactions and cascading affects, and the organizational dynamics of all actors are then assessed. It is in this step that density and the interaction of terrain and social features described in urban operations challenges above would be addressed.

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).

Step 3: Evaluate OPFOR (PTEs) & Threats

The third step is to identify and evaluate the opposing force (OPFOR) or potential threat elements (PTEs), such as al-Qaeda or other threat actors, and the weapons they may employ by class (i.e., chemical, biological, radiological, nuclear, suicide bombing, etc.). It is in this step that indications and warning are most analyzed. A key component of this analysis process is Adaptive Red Teaming that uses and develops "playbooks," or multi-faceted intelligence products that responders can use to shape response to unfolding scenarios. Playbooks provide pre-planned general guidance for use in complex situations, such as a chemical or biological attack. Playbooks are threat specific and can be developed for each echelon of response or threat assessment.

This step is intended to identify threats which reside in a notional "threat envelope." Within observation of the threat envelope IPO seeks to develop 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 utilizing statistical, econometric and analytical tools including non-obvious relationship awareness or analysis (NORA). These

tools envision going beyond doctrinal or normative to specific aspects of the threat fed from dynamic red teaming process.

Along with threats and influence evaluation, there is also a relatively new area called epidemiological intelligence, which is aimed specifically at integrating disease surveillance and understanding of human disease potentials for biological (as well as chemical, radiological and nuclear) threats. This realizes the unique nature of bio-terrorism and pandemic events that needs to separately be addressed by the adaptive red team.

The I & W Envelope

Conceptually, the Indications and Warning (I&W) Envelope is depicted as surrounding Step 3, with most I&W currently occurring just prior to an actual attack at the top of the envelope. By embracing advanced social network analysis and NORA, it is possible to discern terrorist potentials earlier in the step, by observing indicators and precursors for assembling the "terrorist kill chain" thus achieving "Deep I&W." Additionally, by employing a range of sensors and analyzing signals and indicators and using advanced information technology, we believe there is a potential to extend the I&W envelope into Step 2 exploiting all of IPO's predictive potential and developing cyber intelligence.

Step 4: Determine OPFOR & friendly COAs

The fourth step that eventually feeds back into the first step is OPFOR and friendly courses of action (COA) development. Step 4 builds upon all the previous steps and relies upon an accurate assessment of the current situation. 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 operational (and component tactical) situation.

This is the step where completed intelligence products are disseminated to support operations. Actionable intelligence is the goal. The products developed include "Mission Folders," advisories, alerts, warnings, net assessments and other tailored intelligence products. Mission Folders are incident-specific, combining pre-incident intelligence preparation (playbooks and target folders) with time sensitive threat information. The "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.

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, 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/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).

These products are provided to command staff and decision-makers and are designed to be iterative in nature. Once a Mission folder is disseminated and briefed, the process begins again for the next operational period and to address changes in situation during an on-going event or campaign. The resulting flow of understanding becomes an integral part of the decision process within the Unified Command.

Foundations for the Core and Four Steps

All of the four steps, as well as the core rely upon a foundation of intelligence knowledge, process, capabilities, and practice. First among these are a capability for assessing and collecting information—sensors. The sensors could be a citizen information network utilizing human collection means, Internet scanning, telecommunications intercepts, geospatial collectors or any other means of forensic intelligence support. These ultimately involve the exploitation of real-time or near real-time monitoring or virtual reachback from multi-sensor arrays or field reconnaissance capabilities (as in the case of chemical, biological or radiological sensors or detectors).

Sensors, as well as the entire IPO process, also sit upon a "joint" toolbox. This toolbox includes the need to scan, monitor and drive forecasting. This involves scanning the horizon of potential threats, monitoring specific threat potentials when they are identified, and forecasting the likely outcomes (best case, worst case, most likely case) of potential or actual threat scenarios. This is a process-oriented way of describing the transition from Indications of Warning (I&W) to Operational Net Assessment (ONA) within the operational tempo (OPTEMPO) of unfolding events.

Another way to view this process is to employ the OODA Loop or Boyd's Decision Cycle. In the doctrine of the father of Maneuver Warfare, Colonel John Boyd, the Observation-Orientation-Decision-Action (OODA)cycle is essential to understanding conflict. In short, the adversary that best negotiates the decision cycle—that is the side that observes, orients, decides and acts, appropriately—with relative speed or better perception (orientation) and then acts is generally the side that wins! The OODA loop (or perhaps more appropriately getting inside your adversary's OODA loop), and its

implicit reliance on analysis/synthesis to understand, adapt, and act in the face of uncertainty underlies both the TEW concept and IPO process.

All of this relies upon an understanding of several concepts for understanding intelligence and conflict. These include an understanding of deception and counter-deception, of swarming and counter-swarming as tactics or approaches to conflict, as well as an understanding of intelligence and decision dynamics, such as the need to limit group think and/or 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. A center of gravity is that key aspect of the enemy force, 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.

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 phase of operations.

Conclusion

Intelligence Preparation for Operations (IPO) is a multiagency, multidiciplinary, civil-military operational approach that is tailored to support the unified commander's decision-making. IPO supports operations, and those may involve not only law enforcement, but fire, health, military, emergency management, non-governmental organizations and many other types of support. This is very different from a criminal investigation, to include investigative assistance or support (criminal intelligence that is aimed at criminal or civil adjudication through prosecution) that is often termed "intelligence" in current discussion of homeland security and counterterrorism.

Operational Net Assessment and developing a strong Indications and Warning (i.e., early warning) system are integral components of IPO. Neither of these is designed to support criminal prosecution, but is instead designed to support emergency management of resources (personnel and equipment) in preventing, preparing, protecting, responding and recovering from terrorist attacks. There is a rigorous analytical process in determining what are the indications of a pending threat and to what extent these represent early warning. Operational Net Assessment is that process that determines what the opposing force (i.e., terrorists) is planning to do and what we should do either reactively or proactively. It is methodology for defining courses of action (COA), either friendly or enemy.

Again, it is critical to point out that this is not strategic intelligence for nation-state military warfighting, or part of the investigative portion of crime fighting. IPO recognizes the blurring of crime and war, of marshalling resources either for natural or

man-made disasters. IPO is the intelligence needed for authorities dealing with the prospect of 9-11, the anarchy of the '99 Seattle World Trade Organization meeting, the '92 Los Angeles Riots, or the prospect of a major earthquake, floods or wildfires. Whereas IPO may develop products and knowledge that will eventually contribute to criminal intelligence or even traditional IPB, both of these are separate channels in indirect outcomes, not the driving force behind the process itself. Certainly with the Global War on Terrorism, intelligence on emerging terrorist tactics, techniques and procedures is part of the information age fabric of our global society, so what is happening in America or Arabia are implicitly interconnected.

IPO is a process for achieving operational intelligence through All-Source/All Phase Fusion toward All-Source Situational Understanding (ASU). It integrates Urban Intelligence, Surveillance and Reconnaissance (ISR), geospatial intelligence, cultural intelligence and open source intelligence to achieve multi-INT fusion (i.e., fusion of multiple intelligence disciplines, including human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measures and signals intelligence (MASINT), etc. While distinct from investigative support/criminal intelligence it is an essential tool for identifying and understanding terrorist and non-state threats and providing intelligence support to operational commanders and forces in a range of missions for both civil and military authorities.

Situations where IPO can help provide the intelligence edge include homeland security, anti- and counter-terrorism, as well as a full range of expeditionary operations. These include stability and support operations (SASOs), constabulary operations, all levels of urban operations from SASOs to full-scale high intensity combat, and Military Support/Assistance to Civil Authorities (Homeland Defense and Support), as well as force protection and base defense. IPO is a combination of intelligence preparation of the "unconventional" battlefield along with the unique processes found in the Terrorism Early Warning Group (TEW) model to achieve All-Source Situational Understanding. In short, IPO is a process that helps unlock and clarify the knowledge needed by the entire range of decision-makers, both civil and military, to effectively craft responses to terrorism, global insurgency and emerging threats non-state and otherwise.

Figure 2: Response Information/Target Folder Template

1. SITE (NAME): Name of facility

2. LOCATION (ADDRESS, X STS., TG, GPS): Address, cross streets, map reference and GPS coordinates

3. TYPE: By Target Set/Venue (Describe)

4. HAZARDS (MSDS): List site-specific hazards refer to Material Safety Data Sheets

5. DAY/NIGHT POPULATION: People on site day & night

6. POINT OF CONTACT (POC): Name/title of contact person

7. PHONE/E-MAIL/WEB SITE URL: List numbers/addresses

8. FLOORPLAN: Attach floor plan diagram/map

9. PHOTOS: Photos of site and access/egress

10. POWER/WATER/AIR (HVAC): Locations/characteristics of utilities

11. DOWNWIND, DOWNHILL: Describe potential impact on sites; downwind/ hill (evacuation potentials)

12. LIGHTING/WATER: Describe lighting/water supply access

13. INTERMODAL LINKS: Describe impact on other facilities

14. SYSTEMIC IMPACT: Describe impact on site's ability to operate/sustain operations

15. PAST THREAT HX: Describe prior threat history

16. SYMBOLIC VALUE: Rate Low, Medium, High

17. KEY DATES FOR FACILITY: Indicate key dates for the venue

18. CRITICALITY (PEOPLE/FACILITY): Rate impact on people and facility as low, medium, high, very high, extreme should an attack occur

19. VULNERABILITY: Rate vulnerability to attack as above

20. LZ, CP, S, D LOCATIONS: Identify landing zone, command post, staging areas and decon corridor locations

21. COMMO. CAPABILITIES/LIMITATIONS: Describe communication characteristics

22. MICROCLIMATES/PREVAILING WINDS: Describe prevailing winds, typical weather

23. RESPONSE RESOURCE LIST: Describe typical Law, Fire, EMS response resources

Note: This standardized format was recommended by the InterAgency Board for Equipment Standardization and InterOperability (IAB) in its 2002 Annual Report (p. 34). It demonstrates a minimum information requirement for characterizing terrain (site/venue) awareness and geospatial information tags for use in a digital operational space visualization tool for incident response and planning. An adaptation of this

template for the cyber environment was published in the IAB's 2003 Annual Report at p. 47-48.

References

Matt Begert and Dan Lindsay, "Intelligence Preparation for Operations," in Robert J. Bunker (Ed.), Non-State Threats and Future Wars, London: Frank Cass, 2003, pp. 133-143.

Hal Kempfer, "Risk Management Intelligence," Competative Intelligence Magazine, Vol. 5, No. 6, November-December 2002, pp. 19-22.

Jamison Jo Medby and Russell W. Glenn, Street Smart: Intelligence Preparation of the Battlefield for Urban Operations, Santa Monica: Rand, 2002.

John P. Sullivan, "Intelligence Preparation for Operations: Developing Tools to Support Decision Making in Specific Incidents, " The InterAgency Board for Equipment Standardization and Interoperability, 2000 Annual Report, pp. 51-52.

John P. Sullivan, "A Cooperative Vehicle for Threat Assessment; A Case Study: Los Angeles County Terrorism Early Warning (TEW) Group," The InterAgency Board for Equipment Standardization and Interoperability, 2000 Annual Report, pp. 45-50.