Needed: State-level, Integrated Intelligence Enterprises

Dr. James E. Steiner

> ***"Needed is a single, integrated intelligence enterprise with well-defined lanes-in-the-road for each large, complicated state like New York."***

Following the terrorist attacks of 11 September 2001, a revolution has been underway in the relationships of federal, state, and local homeland security, law enforcement, and intelligence organizations. At the federal level, the Department of Homeland Security (DHS) has been created, the "wall" between law enforcement and intelligence has been nearly obliterated, some law enforcement organizations are being directed to become more like intelligence agencies, and the foreign intelligence community is being fundamentally reformed.

The impact of these changes has been even greater at the state level: state governments have been assigned the lead role in homeland security. Most states have responded by bringing together existing public security, law enforcement, and emergency response capabilities—linking them to similar local assets—and opening channels to other states.

But a piece has been missing. Before 9/11, none of the states had a robust intelligence capability. Most now have created multiple intelligence cells in existing structures, as well as fusion centers, which for the first time connect state and local homeland security and law enforcement—and especially the new intelligence organizations—with federal, community, and, in some cases, foreign intelligence services.

Needed is a single, integrated intelligence enterprise with well-defined lanes-in-the-road for each large, complicated state like New York. We will see that this challenge is as daunting at the state level as it has been in the national Intelligence Community (IC).

One thing is clear—replicating the federal IC structure in 50 states is NOT appropriate. Some of the concepts we use in analyzing national intelligence missions and structures are useful—for example, differentiating between national (or state-level) intelligence and departmental intelligence. But for the most part, the federal model is just not relevant: collection is less a state function than is analysis; single-function collection agencies such as NSA and NGA have no comparable state analogue; HUMINT

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US or New York State government endorsement of its factual statements and interpretations.

States need to tailor the structures they build to accommodate the robust capabilities that national organizations with intelligence capabilities maintain within their geographic boundaries.

(confidential informants) is the dominant collection discipline at the state level; and we clearly do not want any state-level entities developing covert action capabilities. Finally, most states simply do not have the resources to create and maintain the multilayered, redundant structures so prevalent at the federal level. On the other hand, states need to tailor the structures they build to accommodate the robust capabilities that national organizations with intelligence capabilities maintain within their geographic boundaries. In addition, state requirements vary significantly across the country, and a single model will not meet every state's needs.

State and local fusion centers are the designated focal points connecting the federal IC to state and local intelligence collectors and analysts on counterterrorism threats. In most cases, state police manage state fusion centers. The centers' primary mission is to move counterterrorism (CT) intelligence from the local level to the federal community and from the federal level back to local law enforcement. But as we shall see below, state-level intelligence missions go well beyond providing operational intelligence support to law enforcement CT programs. Some fusion centers have taken on broader missions, especially in the public safety arena, and have other customer sets, including state executives and the public. Others have remained narrowly focused on CT or intermediate all-crimes intelligence.

Much has been written about fusion centers from the perspective of their primary mission and their relationship with federal law enforcement and the IC. This article will not duplicate that discussion. Rather, I will emphasize state-level intelligence requirements *beyond* the support-to-law-enforcement mission and focus on the primary, non-law enforcement customer—the state governor and his executive-level homeland security team.

The article is informed by multiple state models, but it focuses on New York state. The Empire State has international land and maritime borders, coastal and riverine international ports, and a huge immigrant community from countries of special interest. It faces a broad array of threats emanating from terrorism, natural hazards (including floods, hurricanes, tornados), and pandemic diseases. But most importantly, the bulk of specific, credible terrorism threat intelligence collected since 9/11 specifies targets in New York City. (See table on facing page.)

Know your Customer –the Governor

The president has a director of national intelligence (DNI), but New York's governor has no such focal point for intelligence. Intelligence is not seen as a separate function, but something embedded into other disciplines. For example, the governor looks to the superintendent of the state police to manage most law enforcement issues and expects that department to conduct law enforcement intelligence. Similarly, the governor looks to his homeland security adviser to help him define the homeland security threat and to manage risk (strategic mission) and meet his immediate public security priorities (operational)—the most basic of which is crisis management and recovery. He assumes that his homeland security adviser has built the intelligence capability to do his job.

New York's homeland security strategy demonstrates the centrality of both strategic risk management and operational crisis management/recovery to the governor and his senior resource managers in Albany.

Strategic Threat Assessments

At the national level, the DNI is required to provide the president and Congress an annual worldwide threat assessment as a necessary context for discussion of national security budget

Major Plots, Arrests, and Threats in New York State during 2001–2008

The list below is representative of the terrorism-related cases and plots the state has faced over the past eight years. They vary in their severity and their plausibility.

September 11 (2001): The most deadly terrorist attack in history, when Al Qaeda operatives targeted the World Trade Center with commercial airliners, resulted in thousands of deaths in Lower Manhattan.

Anthrax Letters (2001): The mailing of letters containing weaponized Anthrax spores, mainly to media and political targets, resulted in five deaths as well as numerous injuries.

The Lackawanna Six (2002): A group of Yemeni-Americans from outside Buffalo were convicted of providing material support to terrorism after spending time in an Al Qaeda training camp.

Iyman Faris/Khalid Sheik Mohammed Brooklyn Bridge Plot (2003): Iyman Faris, a truck driver who had been in contact with numerous Al Qaeda leaders, was involved in a plot to damage or destroy the Brooklyn Bridge.

Subway Poison Gas Plot (2003): Reports suggest that a Bahrain-based Al Qaeda cell intended to target the New York City subway system with a device that would disperse cyanide gas.

Herald Sq. Subway Plot (2004): Two men from Queens and Staten Island were convicted of conspiring to bomb the subway station at Herald Square.

Albany Missile Sting (2004): Two Albany residents were convicted of supporting terrorism for an incident in which they agreed to help launder money to purchase a shoulder-fired missile for a militant group.

East Coast Buildings Plot (2005): Three British nationals were charged with conspiring to bomb buildings along the eastern seaboard of the United States, including the Citigroup Center and New York Stock Exchange.

PATH Tunnel Plot (2006): This plot, disrupted in early planning stages, centered on a Lebanese national and several other individuals planning to attack the Port Authority Trans Hudson Tunnel connecting New York and New Jersey.

JFK Airport Plot (2006): Four men, from the Caribbean and South America, were convicted of conspiring to bomb the fuel distribution pipeline at John F. Kennedy Airport in Queens.

Aafia Siddiqui (2008): An American-trained neuroscientist wanted for supporting terrorism, Siddiqui was captured in South Asia with detailed information about numerous targets including Times Square, the Statue of Liberty, the subway system, and the Plum Island biological facility.

requests. Similarly, in New York strategic intelligence in the form of an overall state threat assessment comes first. In fact, state law requires that the homeland security adviser present a threat-to-New York briefing to selected legislators by 31 January every year. Some threats, such as terrorism, are new to governors but familiar to intelligence officers, but most of the threats facing a governor—blackouts, floods, hurricanes—are familiar to New York state but new to intelligence officers. Governors prefer a single, integrated threat assessment and look to their homeland security advisers to develop it.

At the national level, threat analyses are used to justify programmatic requests. At the state level, threat assessments are also a key input to the risk management process. As defined by DHS and included in New York's State Strategy for Homeland Security, risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence. It is determined by the event's likelihood and any potential consequences. Unwanted outcomes include loss of life, compromised essential services, economic damage, public anxiety, and other societal problems resulting from an attack or natural disaster. Preparedness efforts are designed to minimize the risk to the state, its infrastructure, and its citizens. The level of risk facing a region is a function of three compo-

The driving force for the DHS Intelligence and Analysis state fusion center program is intelligence support to law enforcement.

nents: threat (or natural hazard), vulnerability, and consequence. Addressing each of these components individually enables New York state to develop a cohesive strategy and to limit the risks it faces.

There are simply not enough resources to eliminate all of the risks we face. Risk management is the process by which senior leaders identify risks and threats, prioritize them (by likelihood and potential impact), and then direct federal, state, and local resources to act to minimize the likelihood of their occurrence and mitigate their consequences. The risk management process enables state leaders to prioritize mitigation steps that can be taken based upon potential occurrence of a risk, the potential impacts of that risk, and the economic and political capital available to take such action. The federal government alone has provided more than $3 billion to New York since 9/11 to buy down risk.

Responses to risk take many forms and fall into four major categories—prevention, protection, response, and recovery. A few of the many risk-reduction strategies New York and its partners are pursuing include increasing the capabilities of first responders, constructing and installing physical security systems, purchasing insurance, conducting public outreach campaigns, and sharing intelligence.

Operational Intelligence

Be it a terrorist attack, a pandemic, a flood, a hurricane, or a blackout, the governor is immediately in the public (often national) spotlight. The governor is

- CINC of the state forces responding to the incident,
- chief executive officer of the government,
- chief communicator to a worried public,
- chief liaison to the governors of neighboring states, and
- chief liaison to the federal government.

In fulfilling these roles, the governor must make decisions on declaring emergencies or disasters, using the National Guard, requesting mutual aid, calling for federal assistance, authorizing emergency spending, suspending state regulations, requesting waivers of federal regulations, and ensuring that state agencies are responding appropriately. No governor can begin to take on these roles effectively without advance preparation and excellent, intelligence-driven situational awareness.

The driving force for the DHS Intelligence and Analysis (I&A) state fusion center program is intelligence support to law enforcement. But savvy governors look to these centers for their comprehensive situational awareness, although they do so through their preexisting organizations. In New York, the State Emergency Management Office (SEMO) is responsible for the development and maintenance of state-level response plans and manages the multiagency emergency operations center.

Eventually, as they mature, most fusion centers and emergency operations centers almost certainly will be combined or co-located as they become focal points for information- and intelligence-sharing among local, state, and federal agencies from a variety of disciplines, including law enforcement, fire, EMS, emergency management, and, increasingly, public health, transportation, energy, and even the private sector.

Where the Strategic and Operational Meet...

Advance preparation is crucial to crisis management. The governor and his state apparatus need to be prepared and practiced before a crisis. Effective crisis-management programs encompass five critical components:

- Assessment of the threats facing the state;

- Development of a plan to mitigate those threats;
- Development of a strategy to prepare for all hazards;
- Development of and regular testing of response plans;
- Planning for short- and long-term recovery.

State governors support law enforcement efforts to disrupt and dismantle terrorist groups and prevent violent acts, and they enthusiastically support the DHS I&A fusion center initiative. But counter-terrorism (as opposed to homeland security writ large) is primarily a federal mandate. With the possible exception of New York City, the FBI, through the Joint Terrorism Task Force (JTTF), has first right of refusal on all CT leads/cases, and governors will not be held directly responsible if terrorists strike.

Governors are personally responsible for recovery after a terrorist incident, so it is not surprising that their focus is on minimizing the impact of a terrorist incident (or a natural or nonterrorist manmade event). Governors focus on mitigating threats to critical infrastructure and on facilitating quick recovery by preparing for and responding effectively to all hazards. As noted above, the strategic mission of state-level homeland security is risk management.

The strategic mission of state level homeland security is risk management. Critical infrastructure analysis and policy actions are central to this task.

Critical infrastructure analysis and policy actions are central to this task. Governors understand the federal government's role in infrastructure protection (especially funding) and develop plans and strategies in the context of that federal role. Governors focus on ensuring that vulnerability and risk assessments have been conducted and are adequate for the entire infrastructure in their state. Interdependencies among industrial sectors are identified and governors invest in public infrastructure and work with the private sector and other states to increase the resilience of infrastructure on a regional basis. A governor can take a number of steps to protect critical infrastructure. He can

- identify the state's critical infrastructure;
- conduct vulnerability and risk assessments;
- identify and understand interdependencies;
- invest in infrastructure improvements;
- develop regional strategies; and
- coordinate with the private sector.

New York State's Critical Infrastructure and Key Resources list (CI/KR) is as wide-ranging and important as in any state in the country. The items listed in the CI/KR are assets, systems, and networks—physical and virtual—that are so vital to the state that their loss, destruction, or incapacitation would have major cascading effects on security, economic security, public health, or public safety.

These sectors are not, however, just subject to terrorist threats. Natural disasters, human error, and poor maintenance can compromise critical infrastructure. Another key vulnerability that crosses all critical infrastructure sectors is their increasing reliance on computers and information technology. The threat of cyberterrorism or other cyberattack is illustrative of the interdependencies of modern society. New York's CI/KR have come to rely upon networked computers, data security, and the Supervisory Control and Data Acquisition (SCADA) systems that control infrastructure of all kinds.

Threats to state-critical infrastructure are assessed in the context of natural, man-made, terrorist, and technological events, and risks are determined based on these threats, their likelihood of occurrence, and the impact they would have on the immediate infrastructure and on interdependent systems and facilities. (Governors

New York's state fusion center is the locus of its intelligence support to state and local law enforcement.

The 18 DHS Defined Critical Infrastructure Sectors:

Agriculture and Food

Banking and Finance

Chemical

Commercial Facilities

Commercial Nuclear Reactors, Materials and Waste

Critical Manufacturing

Dams

Defense Industrial Base

Drinking Water and Water Treatment -Facilities

Emergency Services

Energy

Government Facilities

Information Technology

National Monuments and Icons

Postal and Shipping

Public Health and Health care

Telecommunications

Transportation Systems

currently look to intelligence to provide the terrorism portion of these threat assessments.) This type of analysis is used to prioritize infrastructure for protection and to develop and implement a critical infrastructure protection plan that identifies measures to prevent, eliminate, or mitigate the threat.

National-level intelligence analysts once had significant expertise on critical infrastructures—albeit from a radically different perspective. During the Cold War, CIA and DIA analysts used input-output analysis and other econometric techniques such as linear programming to identify economic targets that, if destroyed or damaged, would maximize the disruptions to the Soviet economy. Remnants of this broad expertise still exist at CIA, and more recently the IC has built world-class expertise in the cyber area. The National Labs at Sandia and Los Alamos also have created an exceptionally capable group conducting such studies at the National Infrastructure Simulation and Analysis Center.

At the state level, similar expertise exists in nonintelligence government and academic centers, focused mainly on analyzing the economic impact of various natural disasters and (nonterrorist) man-made events. Many states also have similar cybersecurity efforts. Some targets are obvious, such as infrastructure in areas prone to flooding, but most are not. Analysts are thus forced to conduct sophisticated, data-intensive studies to identify critical nodes, single points of failure, and other high-value infrastructure that might warrant extra protection or redundancy to improve resiliency of the entire system. Intelligence must identify the most likely terrorist targets.

The Bottom Line on Customers, Roles, and Missions

State-level intelligence has three primary functions and customers—providing CT intelligence support to law enforcement; ensuring situational awareness for state-level executive and legislative decision makers; and providing critical infrastructure threat analyses to executive decision makers and policy implementation staff. State-level intelligence also provides unclassified information and assessments to the private sector and to the public when it is possible and appropriate to do so.

New York's state fusion center, NYSIC (New York State Intelligence Center), is the locus of its intelligence support to state and local law enforcement and is managed by the State Police. Its primary focus is CT support to law enforcement, but it has a broader "all crimes" mandate. The fusion center directs a network of over 1,500 field intelligence officers (FIOs) throughout New York state to collect intelligence on suspicious activities and persons. Virtually all of these FIOs are part-time intelligence offic-

ers and full-time law enforcement officers. They move intelligence directly to the NYSIC but are organized administratively through 16 counterterrorism zones (see map on facing page).

On the federal side, the NYSIC interacts with the IC through the National Counter-Terrorism Center (NCTC) and the DHS National Operations Center (NOC). The FBI has the domestic lead in CT intelligence and is connected to other law enforcement through the JTTF. The Bureau's Field Intelligence Groups (FIGs) are the lead domestic terrorism intelligence analysis centers outside Washington (with the exception of New York City where the NYPD intelligence and CT components dominate all other entities).

Homeland security advisers work for the governor and are responsive first and foremost to the governor's priorities, including intelligence priorities. A governor's top need for intelligence is not support to law enforcement, but to understand the terrorist threat as part of the risk-management process. The governor also needs to receive situational awareness in the run-up to a crisis and during ensuing crisis management. Both current intelligence and longer term threat analyses—especially on threats to critical infrastructure—are required to enable the governor and his staff to plan for, mitigate, and recover quickly from crises. Effective crisis management and recovery requires extensive intelligence support and executive action before the crisis.

Current intelligence and threat analyses—especially on threats to critical infrastructure—are required to enable the governor and his staff to plan for, mitigate, and recover quickly from crises.

Intelligence Capabilities in New York—Today's Realities

New York's state and local intelligence heavyweights include the NYPD, the State Police, and the National Guard, all of which have hundreds or at least dozens of full- or part-time intelligence officers. Within New York state's borders, several federal agencies have significant intelligence capabilities, and many other US law enforcement organizations have substantial intelligence assets. All are focused primarily on terrorism prevention through law enforcement.

The NY State Police, through the NYSIC, have taken the lead in state-level intelligence support to law enforcement. NYSIC is a model fusion center that includes intelligence cells on major crime areas such as gangs and narcotics. But its central effort is on counterterrorism. NYSIC has open storage of SECRET-level material, connectivity to secure intelligence systems, and a significant and growing cadre of analysts and agents from federal agencies, including DHS

New York State Intelligence Center maintains strong ties to CT initiatives on the state's border with Canada.

I&A, FBI, ICE, and Coast Guard. (See table on right.)

Federal analysts have connectivity to secure systems at their desks (as do a limited number of State Police). NYSIC coordinates intelligence collection and dissemination through its network of counterterrorism zones and FIOs. It maintains strong ties to CT initiatives on the state's border with Canada. These efforts are models of "jointness," being composed of officers from state, local, tribal, provincial, and US and Canadian federal intelligence and law enforcement organizations. On the downside, NYSIC currently has only modest linkages to the NYPD.

Strategic intelligence support to the governor is provided by the intelligence component (referred to as State Intelligence) of the state's Office of Homeland Security (OHS). This small unit provides strategic threat assessments and broad situational awareness to the director of OHS, the governor, other executive branch leaders, and selected members of the legislature.

New York state's OHS oversees the allocation and distribution of hundreds of millions of dollars in federal and state homeland security funding each year. In addition to funding law enforcement and emergency response, significant resources are directed toward developing a resilient critical infrastructure. OHS has developed a modest (albeit underresourced) internal intelligence capability to identify, collect, evaluate, and assess terrorist threats to critical infrastructure. The effort is modeled on the DHS Homeland Security Infrastructure Threat Reduction and Risk Analysis Center (HITRAC) office. This program is called CI/SAR, which stands for Critical Infrastructure/Suspicious Activity Reports. It is a GIS-based system which correlates SARs and New York's critical infrastructure. It is designed to identify proxy measures of threat (using the SARs) and targets (using CI) and then apply pattern analysis techniques to predict potential danger zones. Since the inception of this project in New York state in early 2007, the national level IC (acting through the DNI) has supported a similar approach nationwide.

The State Intelligence Vision

The list of state intelligence missions below is a vision for statewide intelligence analysis. It minimizes redundancy by tailoring the effort to support a primary customer—the governor—within existing threat assumptions, institutional arrangements, and other guide-

New York State Intelligence Center (NYSIC) Current and Former On-Site Partners

Local

NYPD

City Police and County Sheriff representatives

New York Metropolitan Transportation Authority

State

New York National Guard Counterdrug Task Force

Department of Corrections

Department of Motor Vehicles

Division of Parole

Office of Homeland Security

Police

Federal

DEA

DHS I&A

FBI

US Attorney's Office

Department of Defense-Defense Criminal Investigative Service

Immigration and Customs Enforcement

Coast Guard

Customs & Border Protection

Social Security Administration

lines. Specifically for New York state:

- New York City is the prime target for terrorists in the United States. NYPD Intelligence and Counterterrorism Divisions are and will remain the dominant intelligence organizations in New York City.
- State intelligence should not attempt to engage in all areas of intelligence. The state intelligence function is primarily analytic and has no role in the collection or analysis of tactical intelligence.
- Intelligence support to protect critical infrastructure through efforts such as CI/SAR is the "natural" intelligence domain for the state. In New York, OHS is the lead agency for the critical infrastructure account, OHS directs the homeland security funding process for infrastructure protection, and CI is central to the governor's roles in protecting the state through risk management and especially in recovering from an attack.
- The state's law enforcement and IC intelligence partners at the local, regional, national, and international levels produce massive amounts of intelligence on CT. State intelligence should focus some of its resources on identifying finished national intelligence and key producers or information nodes, gather relevant reports, and assess the implications for New York. This same approach should be used to harvest and tailor for the state open-source and academic research.

New York and other major terrorist target states need federal resources and intelligence-sharing support to meet this vision.

The State Homeland Security Intelligence Mission

The mission areas for state intelligence listed below, when integrated into the matrix of existing organizations and capabilities, yield a single, integrated intelligence enterprise. The missions areas include:

- Developing and maintain a center of excellence in critical infrastructure threat intelligence using methods such as CI/SAR for the entire state.
- Developing and maintaining formal contacts with major local, regional, national, and international partners to ensure full situational awareness and access to intelligence/information products: specifically,
  - Working with state, regional and local fusion centers, which have primary responsibility for support to law enforcement, crisis management information flow, and tactical intelligence support.
  - Working with NYPD intelligence (staffed at roughly 500 officers) in its role as the primary developer of CT intelligence regarding New York City. Expand on NYC finished intelligence products to address implications for the entire state.
  - Working with the federal Intelligence Community in its role as primary developer of foreign and domestic CT intelligence.
  - Identifying high-value IC intelligence products and providing value-added by assessing threat implications for New York state.
  - Working directly with Ontario and Quebec intelligence partners. Border states are uniquely positioned to develop intelligence liaison relationships at the sub-national level.

The Federal Support Needed by State Intelligence

New York and other major target states need federal resources and policy support for intelligence-sharing to meet this vision, and President Obama has promised to step up to the challenge. His campaign platform states:

> *Improve Information Sharing and Analysis: Improve our intelligence system by creating a senior position to coordinate domestic intelli-*

States facing major threats should have a number of intelligence officers and elected officials cleared at the highest security level.

gence gathering, establishing a grant program to support thousands more state and local level intelligence analysts, and increasing our capacity to share intelligence across all levels of government. (from www.change.gov)

The following steps would help New York state achieve this vision of an integrated intelligence enterprise:

- *DHS should provide grant funding for most state-level intelligence analysts.*
- *DHS, as the primary conduit for moving intelligence to the states, must view the states as its primary customer.*
- *DHS must ensure that the substance of all CT intelligence (raw and finished)—on which the federal government spends roughly $50 billion per year—is made available to the states.*
- *DHS must take as a top priority strengthening of the fusion center system of states, regions, and localities.* These centers are now at the outer end of the spokes that move intelligence from the national level hub.
- *DHS should accelerate production and deployment of the the Homeland Security Data Network (HSDN) system.* HSDN is the primary pipeline for moving classified intelligence (at the SECRET level) from the federal hub to the states' fusion centers. In 2008, only about 50 HSDN terminals were deployed and operational outside Washington, DC. There are roughly 1,000 pending requests from states and major cities for HSDN terminals.
- *Virtually all HSDN's scores of homepages and sites should be made available to state officials.* Currently, only two are available to state-level intelligence officers and officials—NCTC's and DHS's. Even outside of the Washington, DC, area, federal officers have access to all sites.
- *The Interagency Threat Assessment Coordination Group (ITAC-G) at the NCTC should include state-level intelligence officers, and ITAC-G representatives from NSA, NGA, and CIA should have the mandate and authority to generate tear-line, SECRET-level reports from compartmented intelligence.* ITAC-G is responsible for reviewing all national-level intelligence and ensuring that highly classified intelligence is downgraded to the SECRET level so that it can be disseminated to state fusion centers. Currently, ITAC-G is minimally staffed and all state and local representatives must be sworn law enforcement officers.
- *Finally, the security clearance process must be fixed. The federal government should be able to process SECRET-level clearances within a month and higher level clearances for compartmented intelligence within 3 months.* States facing major threats should have a number of intelligence officers and elected officials cleared at the highest security level.

❖ ❖ ❖

A Note on Sources

This paper draws heavily and often directly from two studies. "A Governor's Guide to Homeland Security," prepared by the National Governors Association Center for Best Practices, and the "New York State Strategy for Homeland Security," prepared by the Office of Homeland Security and available at: www.security.state.ny.us/, especially the sections on risk, threat, and critical infrastructure prepared by Brian Nussbaum.