

Next Generation Fusion Centers

Intelligence

Author:

Stephen G Serrao

Date

December 2009

Next-Generation Fusion Centers: Analysis is Action

By Stephen G. Serrao, Captain, New Jersey State Police (ret.)

Every time a cop walks the beat, a trooper patrols the highway, or a deputy questions a suspect, a key question enters their minds: “Is everything as it should be?”

In the wake of major terrorism acts, that question has taken on national and global significance. You also hear, “Are we safe?” From my perspective as a law enforcement professional of 25 years, we are. And here’s why. Before 9/11, law enforcement agencies and professionals didn’t always know the significance of information in their possession – much less shared that kind of intelligence with each other. Since then, officials have realized that multi-agency cooperation is the best way to deter terrorism and other criminal activities. While there is still much progress to be made, officials have embraced the power of collaboration and are breaking down traditional barriers.

Thankfully, information sharing is now the rule. From 2004-2007, law enforcement agencies have exchanged data on more than 100,000 terrorism-related threats, reports of suspicious activities, and encounters with people on watch lists, according to the Federal Bureau of Investigation.

For years, law enforcement agencies favored the time-honored principle of not sharing clues and leads until an investigation was completed. They were more concerned about protecting their evidence until a court case could be fully developed. But most now realize that sharing information may reveal larger or wider patterns of activity, and it takes the combined data of federal, state and municipal agencies to understand such patterns. Meanwhile, new systems and oversight allow law enforcement to respect the privacy rights and civil liberties of citizens.

Why Fusion Centers?

Fusion centers are best equipped to oversee and manage the complex role of information sharing and facilitate cooperation between sometimes competing interests. The U.S. Department of Justice (DOJ) defines a fusion center as “an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources.”

Fusion centers are staffed by multi-agency personnel with the technological capabilities to fuse and join millions of records concerning suspicious activities, terrorism and crime found in Computer-Aided Dispatch Systems (CAD), Records Management Systems

(RMS) and records held at Regional Information Sharing Systems (RISS). With the latest technology, fusion centers can store, search, retrieve and analyze data no matter the form it takes – whether it is a suspicious activity report, a phone call transcript, a handwritten note or unstructured data, such as e-mail attachments.

Besides effectively sharing intelligence and information among federal, state and local government agencies, fusion centers also are capable of providing real-time threat assessments and situational awareness to enhance the safety and security of critical public and private infrastructure.

The DOJ's "Fusion Center Guidelines" assert, "Leaders must move forward with a new paradigm on the exchange of information and intelligence." With more than 60 fusion centers firmly established throughout the country, public safety leaders have heeded this directive and established information sharing across agency borders.

Today's Fusion Centers

While the pieces are in place to deliver on the most rigorous fusion center objectives, a real concern is whether they are moving beyond just tactical information sharing and analysis.

The bigger question remains: "How prepared are agencies to anticipate criminal activity and terrorist attacks? That's where strategic intelligence analysis must come into play. In reality, most fusion center staff have a tactically oriented mindset, looking back in time to gather evidence for a prosecution. However, there is more work needed to gather and share strategic information so we can discern patterns of activity and connect the dots to thwart organized criminal groups, such as the Mafia and street gangs, or terrorism networks before a crime is perpetrated. Anticipating crime is a fundamentally different and a critical role for a strategic intelligence analyst.

Let's examine how strategic thinking and analysis could be employed for threat assessment.

In Los Angeles, for example, some 500 suspicious packages are reported to authorities each year. They come in all shapes and sizes, and are found in airports, stadiums, on buses and trains, among other places.

The discoveries are documented, such as in local jurisdiction RMS systems, but that's where things end in many cases. Even though some fusion centers are equipped with the latest data integration, intelligence management, search and analysis technologies, the qualified personnel necessary to analyze the data and create an action plan are not always in place. Without such strategic levels of examination, the information remains in silos, disconnected, and tactical – and no patterns are observed.

Take the Critical Infrastructure Protection (CIP) initiative as another example. It directs law enforcement to keep a watchful eye on communication hubs, energy production facilities, water reservoirs, and fuel refineries. That's a critical first step, but who can

affirm with any confidence which facilities are more likely to be attacked than others, and which are current or long-term targets? More strategic analysis is needed.

Keeping these points in mind, the 1999 Columbine tragedy offers a law enforcement primer for strategic response. As you may recall, 15 people were killed by teenage gunmen who telegraphed their actions in the days preceding the tragedy. While debate about how soon officers should have entered the high school has resulted in policy changes for both police departments and schools, Columbine illustrates how strategic analysis should be employed to anticipate threats, and reduce loss of life and damage.

This strategic approach involves trained analysts using technology in a three-step scientific method:

- Develop a hypothesis of the problem/threat
- Conduct information gathering on aspects of the issue
- Form a hypothesis that cannot be disproved, which becomes a theory and should drive both short- and long-term policing strategies

Such a process can be difficult and costly. But fusion centers are positioned to deliver this critical decision-making. In fact, law enforcement professionals at all levels need to have this conversation about strategic vs. tactical methods, and put the tools and personnel in place to uncover the potentially bigger threats and the proper responses.

Strengthening Fusion Centers

While challenges remain, there are positive developments. The National Information Exchange Model (NIEM), a national standard under adoption across the nation, is a major step forward toward strengthening information sharing and fusion centers. It requires that data be captured uniformly across the board for effective information exchange. For example, automobile manufacturers wouldn't think of making wheel rim sizes incompatible with available tire sizes. Why should intelligence sharing be any different?

In addition, RMS, and other law enforcement software and services mentioned earlier are a dramatic leap forward. Used to their fullest extent, such technical infrastructure helps fusion centers tackle mountains of data to create actionable information. They enhance a multi-disciplinary approach and minimize duplication. They help organizations discover unexpected facts and connect patterns of behavior between individuals, groups and events.

In the Analysis

The next-generation fusion center will make the best use of strategic analysts and robust technologies. It will mitigate the temptation to look backwards and instead direct our attention to predicting, preventing, rather than just responding to, criminal and terrorist threats in real-time.

Captain Stephen G. Serrao is a former New Jersey State Police Counterterrorism Bureau Chief, and now helps shape the direction of intelligence management software as Director of Product Management, Americas Region for Memex, Inc., a worldwide provider of intelligence management, data integration, search and analysis solutions (www.memex.com). Serrao can be reached at steve.serrao@memex.com.

Contact Us

Memex Technologies Ltd and Memex, Inc

UK and International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland
Telephone: +44 (0)1355 233804
Fax: +44 (0)1355 239676

America

Memex, Inc.
22636 Davis Drive, Suite 130
Sterling, VA 20164, USA
Telephone: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
Fax: +1 703 556 4282

Copyright ©

No part of the contents of this publication may be reproduced or transmitted in any form or by any means without the written permission of Memex.

More Information

For the latest information about our product and services, please visit

<http://www.memex.com>