Enabling Agility in Law Enforcement

Leveraging Collective Intelligence, Analytics, and Operational Capabilities to Optimize Mission Performance

Booz | Allen | Hamilton

delivering results that endure

Enabling Agility in Law Enforcement

Leveraging Collective Intelligence, Analytics, and Operational Capabilities to Optimize Mission Performance

By nearly every measure, the threat from Transnational Organized Crime (TOC) grows stronger every day. The National Intelligence Council, within the Office of the Director of National Intelligence, recently estimated that TOC generates these staggering annual revenues from its criminal activities:[1]

- **Money Laundering –** US$1.3 trillion to US$3.3 trillion (2-5 percent of world GDP)
- **Narcotics Trafficking –** US$750 billion to US$1 trillion
- **Counterfeited and Pirated Products –** US$500 billion
- **Human Trafficking –** US$21 billion (2.4 million victims)
- **Credit Card Fraud –** US$10 billion to US$12 billion

Perhaps most alarming are the growing interlinkages between TOCs, terrorists, and insurgency groups. Increasingly, TOC organizations are employing terrorist-like violence to spread fear and exert influence and control, while terrorists and insurgents are using criminal activities to help fund their political violence. Insurgent networks such as Colombia's FARC and the Afghan Taliban have become so deeply involved in smuggling narcotics, kidnapping, and extortion that crime has essentially become their raison d'être. Similarly, TOCs from Mexico's Sinaloa Cartel to the D-Company gang in Pakistan have adopted terrorist tactics to intimidate law enforcement and government officials as well as rivals. Collaboration between criminal groups and anti-state organizations is also growing more common. Although the motivations of TOCs and terrorists-insurgents are decidedly different—one's primary motive is financial gain, while the other's is political power—their activities are increasingly alike. The melding of these threats across national and international borders has blurred the distinctions between national security, criminal justice, and homeland security. There are no borders in the fight against transnational criminals, terrorists, and insurgents. National security, law enforcement, and homeland security missions have become intertwined.

These converging TOC and terrorist networks threaten US national security and economic interests in multiple ways. Powerful illicit networks from South Asia to West Africa to Latin America to the Former Soviet Union are destabilizing the regions where they operate, undermining state authorities, disrupting business and trade, and fueling migration. The worldwide expansion of trafficking in drugs, weapons, and humans has spurred a concurrent rise in violence that spills onto US soil. In Mexico, the criminal cartels have become so entrenched that the Calderon Administration enlisted more than 45,000 military troops to assist police, while spending billions of dollars in domestic funding and foreign aid under the Merida Initiative. However, as yet, the Mexican government has been unable to break the power and impunity of the criminal syndicates. Not simply traditional drug cartels, TOCs, many with terrorist links, are also escalating the number and sophistication of their cyber attacks on businesses and individuals to steal intellectual capital, hack into private bank accounts, perpetrate fraud, and commit other cybercrimes that go undetected for months and even years. For example, Central European cybercrime networks alone defrauded US citizens or entities of an estimated US$1 billion in a single year.[2] Legitimate businesses suffer enormous losses and compete at a disadvantage when their intellectual capital is stolen and their products are counterfeited and sold at reduced prices. They are likewise harmed

[1] National Intelligence Council, *The Threat to National Security Posed by Transnational Organized Crime*, www.dni.gov/index.php/about/organization/national-intelligence-council-nic-publications

[2] National Security Council, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, www.whitehouse.gov/administration/eop/nsc/transnational-crime, July 2011, p. 7.

by trade-based laundering, which distorts the prices of commercial goods, and by criminal enterprises that bribe and intimidate government officials worldwide to gain special treatment or access to markets. The global stakes are enormous. These highly sophisticated and well-financed TOC and terrorist organizations wield unprecedented political and economic power; and their potential to disrupt critical infrastructure, undermine markets, spread deadly viruses, and even obtain weapons of mass destruction poses a grave threat to the nation's security.

The task of tracking and halting TOC activities has become increasingly difficult due to a number of factors. TOC and related terrorist organizations are extremely adept at exploiting cyber technologies, not just to commit crimes, but also to escape detection and operate hidden from view. Their highly decentralized networks adapt quickly to countermeasures, disbanding when threatened and later reappearing in new locations and disguises to resume their criminal activities. Their ability to collaborate and share information with a wide range of criminal and anti-state actors also adds to their strength and agility. Moreover, their many diverse criminal enterprises make it difficult for law enforcement agencies to bring them down solely by focusing on just one or two activities, such as narcotics or weapons trafficking. At the same time, government agencies are facing budget constraints not seen since government downsizing in the 1990s. Law enforcement agencies simply do not have the resources to fight TOCs by adding large numbers of personnel or buying expensive solutions. The alarming success of TOCs, combined with the constrained budget environment, has sparked a growing recognition that law enforcement agencies must find ways to operate more effectively and efficiently. This requires that current methodologies and procedures be adapted to meet the modern TOC threat, which is much more agile, elusive, and dangerous than earlier incarnations. When he released the government's "Strategy for Combating Transnational Organized Crime," President Obama declared, "Despite a long and successful

history of dismantling criminal organizations and developing common international standards for cooperation against transnational organized crime, not all of our capabilities have kept pace with the expansion of 21st century transnational criminal threats."[3] The challenge for today's law enforcement community is building the strategies, tactics, organizational structures, processes, partnerships and tools to exploit modern digital technologies and shift the advantage back in our favor in the fight against transnational criminals and terrorists.

Creating Agile Law Enforcement

The need to adapt law enforcement capabilities to the realities of new technologies and criminal activities is not new. In the early 20th century, the automobile enabled criminal gangs to travel quickly from one jurisdiction to the next, helping them stay beyond the reach of local sheriffs. Their crimes became national as well as local problems. Consequently, the Federal Bureau of Investigation (FBI) was created to counter criminal activities that crossed state and local borders, prompting federal, state, and local law enforcement officials to create new ways of working

[3] National Security Council, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, www.whitehouse.gov/administration/eop/nsc/transnational-crime, July 2011, p. iii.

together to defeat the new brand of criminals. The same challenge exists today: the Internet and other digital technologies have provided criminals with dramatically new modes of operation and new ways to escape arrest and conviction, similar to the advent of the automobile. Today, law enforcement and security agencies must chase cyber criminals across virtual networks stretching into every region of the globe. It is absolutely imperative that federal law enforcement agencies find new ways to work together to combat this modern, burgeoning threat. Moreover, collaborative efforts should include all relevant instruments of national power, including the intelligence community, military commands, diplomatic authorities, and other US national security organizations, as well as international partners who have shared interests and responsibilities in defeating transnational criminals and terrorists. Law enforcement entities must not only become more adept at interacting with each other, but also at interacting with the entire national security system.

A good starting point is understanding that the very same technologies that gave rise to modern TOCs can also give law enforcement an edge in uncovering their activities and shutting down their operations. These criminal enterprises leave digital footprints, just as all enterprises do. Travel, money transfers, and communications (including phones, email, instant messaging) generate data that can be combined and analyzed to gain a greater understanding of the TOC networks and activities. In addition, these organizations have common characteristics—for example, in how their leadership operates, how they communicate, and how they move money. Consequently, mapping a foreign fighter network in Iraq, for example, could provide lessons that fuel operations against Mexican cartels.

US government agencies have unique access to the data sources that can shine a spotlight on TOC leadership and activities. Much of this information is collected by law enforcement and other agencies for enforcement and regulatory purposes, but the data also contain significant potential for combating TOCs and sophisticated terrorist groups. A large portion of that data currently resides in separate agency divisions and systems that have different legal authorities, policies, and data tools. The information is not readily shared, nor are agency processes structured to provide a unified view of TOC threats. This hinders their ability to leverage the vast storehouses of data to uncover criminal activities or respond quickly against suspected threats. The law enforcement community recognizes the need for new approaches, but the challenge is figuring how best to facilitate the required integration and collaboration among agencies in the pursuit of shared mission goals, particularly given current budgetary constraints.

No single action will instantly solve the problem. In working closely with multiple law enforcement agencies focused on TOC and terrorist threats, we have observed that the most successful organizations are characterized by several common capabilities and characteristics, the most important being the ability to share and analyze information with multiple partner agencies, and related ability to collaborate with those agencies in the pursuit of common missions. To defeat today's highly networked transnational criminals and terrorists, US law enforcement agencies must themselves become a tightly knit, collaborative network that leverages their collective intelligence, analytic, and operational capabilities to optimize mission performance. No agency can defeat these international threats on its own, but by strengthening their collaborative networks—with each other and with other national and international partners—they can become more agile, flexible, swift, and strong in achieving their mission goals.

Based on Booz Allen Hamilton's extensive experience assisting US law enforcement and Homeland Security agencies in countering today's converging criminal

and terrorist threats, we recommend the following actions for building collaborative networks among law enforcement agencies:

1. Build Out the Vision Outlined in the White House Transnational Crimes Strategy

Released in July 2011, the White House's Strategy to Combat Transnational Crimes provides guidance to "build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to our national security—and to urge our partners to do the same."[4] It lays out the nation's strategic objectives in the global fight against crime, such as breaking the economic power of TOCs, defeating their networks, and building international cooperation in these efforts. The strategy also identifies actions the nation and law enforcement community should take to enhance intelligence and information sharing, disrupt drug trafficking, protect the financial systems, and achieve other goals. Overall, the strategy provides guidance to help agencies develop strategies and take stronger action against TOC networks. Government agencies need to implement the strategy's guidelines and enhance information sharing.

2. Align Entities with Their Missions (not with their agencies)

Numerous federal agencies have law enforcement missions, each with a specialized area for countering domestic and international criminal and terrorist threats. Unfortunately, current rules and bureaucratic practices often prevent these agencies from combining efforts against common threats that transcend their own "lanes in the road." Even within the US Department of Homeland Security (DHS), member agencies pursue distinct missions, maintain separate records, and are not rewarded for internal DHS collaboration. Consequently, while the government expends a lot of resources tracking people, money, and goods, it often does so in stove-piped missions; and when government agencies attack TOC networks, they often do so separately, rather than mounting a collaborative operation to defeat the targeted network. Too often, our law enforcement entities operate as bastions aligned to agencies rather than to missions.

However, there exist a growing number of examples demonstrating how agencies can combine resources and efforts to pursue common mission objectives. For example, the Drug Enforcement Administration (DEA) is leading an interagency effort at the Special Operations Division with the FBI and DHS that is disrupting Hezbollah drug trafficking and money laundering. Similarly, the FBI, CIA, and other agencies are working together at the National Counterterrorism Center for a common mission, bringing together instruments of national power inside and outside the law enforcement community. Joint efforts by the FBI and DEA working against the Colombian FARC resulted in the indictments of 50 principle FARC members on drug trafficking changes. These and other examples can provide lessons for developing the methodologies, doctrine, training, and tools for enabling agencies to work together toward shared mission goals.

3. Make Integrated Fusion Centers the Norm, not the Exception

As criminal and terrorist networks become increasingly interconnected and collaborative in their operations, so too must law enforcement organizations. An important way to strengthen the law enforcement network is by enhancing the operations of fusion centers. Currently, most fusion centers are a collection of representatives from various law enforcement agencies who are co-located in federal buildings across the country. Unfortunately, in most instances, officers have little authority to collaborate with colleagues; and few are rewarded for serving in such centers. As a result, fusion centers rarely reap the benefits of the collective staffing talent.

Designated fusion centers could make multi-dimensional operations—such as the kind necessary

[4] National Security Council, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, www.whitehouse.gov/administration/eop/nsc/transnational-crime, July 2011, p. iii.

to counter evolving transnational terrorist and criminal threats—their principal missions, with the necessary authority to enhance effectiveness. Well-run fusion centers can serve as models for future practice. For example, the Organized Crime Drug Enforcement Task Force Fusion Center (OFC) is an inter-agency intelligence and investigative support center that excels at information sharing. The center maintains a single fused repository containing the most sensitive investigative information from all of the federal investigative agencies, including information from open investigations involving undercover agents, informants and cooperating witnesses, court authorized communications intercepts, etc. The single, fused database makes it possible to conduct a number of sophisticated analytic functions and proactively generate targeting packages. The interagency workforce has had tremendous success in coordinating and targeting sophisticated crime syndicates. Based on the OFC's success, the center has added a new component, the International Organized Crime Center (IOC2), to target non-drug related international organized crime.

Another effective example is the El Paso Intelligence Center (EPIC), which provides time-sensitive information to law enforcement customers who typically act on the information immediately upon receipt. EPIC has a 35-year history and is expanding its portfolio beyond the traditional "pull" model where individual users ask for specific information, so that now EPIC is increasingly "pushing" information to border operators and policy makers in a proactive way. On the international stage, interagency fusion centers in Iraq and Afghanistan have provided real-time analyses of terrorist and insurgent networks in support of critical multinational operations in those nations. Giving all fusion centers these kinds of capabilities and authorities would support the integrated and "networked" law enforcement required to defeat today's TOC and terrorist-insurgent networks.

With regard to state and local fusion centers, the Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations recently concluded that DHS' work with the more than 70 state and local intelligence fusion centers "has not produced useful intelligence to support federal counterterrorism efforts."[5] A bi-partisan subcommittee report said that DHS intelligence officers assigned to fusions centers rarely produced intelligence of any value for counter-terrorism, and that the centers lacked "must-have" intelligence capabilities. Clearly, this is an area where DHS must strengthen the collaborative law enforcement network by providing more oversight and training for both its own intelligence officers and the state and local fusion centers.

4. Reward Activities and Behaviors Aimed at the TOC Threat

It is well understood that police and other law enforcement personnel will pursue policies and goals that are actively encouraged and rewarded by their organizations. They will focus on seizures and arrests because they are graded on the number of seizures and arrests they make. Consequently, law enforcement organizations should establish incentives to encourage and reward collaborative efforts to defeat transnational criminal networks, rather than for simply seizing drugs and making arrests. To reinforce the seriousness of our commitment to counter evolving transnational threats, for example, federal and state agencies could require a "successful tour" working with interagency partners, such as at a fusion center, as a necessary condition for promotion beyond a certain grade. By devising measures and rewards to foster collaborative actions and behavior, law enforcement would also be ensuring more accountability in achieving desired outcomes.

5. Focus on Criminal Financial Transactions

The huge volumes of financial transactions that pass through the US banking system provide a valuable opportunity to spot anomalies, uncover criminal transaction, and identify the people behind them. As mentioned, DEA led a joint operation with DHS and the FBI that disrupted illicit drug trafficking and money laundering by Hezbollah. As a result of the investigation, US authorities seized US$150 million

[5] Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations, *Federal Support For and Involvement in State and Local Fusion Centers*, www.hsgac.senate.gov/subcommittees/investigations, October 3, 2012, p. 1.

from the Lebanese Canadian Bank in Lebanon, which has been sanctioned and required to pay significant fines and penalties. Similarly, the Department of Treasury was recently given expanded financial regulatory authority to investigate and prosecute international crime syndicates operating in the United States, essentially giving Treasury the same tools to combat organized crime as it uses to combat terrorist financing networks.

6. Use Analytics to our Advantage

Powerful analytic algorithms can sift through data at fusion centers and other locations to quickly uncover patterns of behavior or connect the dots between seemingly unrelated information and events. In addition, cloud computing now eliminates many of the technological barriers to centralizing and sharing data, giving agencies far greater reach into federated data sets containing potentially valuable threat information. Data analytics could be applied in a variety of ways. For example, law enforcement agencies that use supply chain attack models can go beyond traditional approaches, which typically examine contraband and the people involved in trafficking the contraband, to instead map out all of the sophisticated processes, people, technologies, and flows associated with the illicit enterprise. This would allow agencies to identify points of weakness that can be targeted with the goal of causing cascading failures to the system. In an era of budget constraints, cloud analytics will also help agencies operate more efficiently and effectively.

7. Promote Information Sharing

Over 12 years have passed since 9/11 and many law enforcement agencies remain reticent to share data, creating information gaps readily exploited by sophisticated transnational criminal entities. However, many notable examples exist within government showing that agencies can effectively share and extract value from data while also keeping it secure, preserving privacy, and complying with federal regulations regarding the handling of data. For example, the FBI's Investigative Data Warehouse collects data from multiple law enforcement and intelligence community databases, and makes the data available to authorized personnel throughout the country. The Integrated Automated Fingerprint Identification System (IAFIS) is a national fingerprint and criminal history system that is widely available and used by local, state, and federal law enforcement officials to track and capture criminals and terrorists. Similarly, the OFC, mentioned earlier, contains the most sensitive investigative information from seven federal agencies, as well as other data sets, which are shared among agencies. And the CIA's Crime and Narcotics Center, which collects and analyzes information relating to international narcotics trafficking and organized crime, supports law enforcement as well as the US military, State Department, and other agencies, providing one model for information sharing across a wide spectrum of national security organizations.

A starting point for promoting information sharing is the creation of department-wide technology systems, rather than allowing individual agencies to create their own silos of excellence. Within DHS, for example, virtually all of the major component agencies, including the US Coast Guard, Immigration and Customs Enforcement, Customs and Border Protection, and the Transportation Security Agency, run their own separate IT systems. Regrettably, the agency specific systems are frequently incompatible with technology platforms used by other agencies within the same department. Creating a department-wide IT system would facilitate information sharing within the department, and made it easier to share information and collaborate with agencies outside the department.

Conclusion

The converging threats of transnational criminals, terrorists, and insurgents are not only exacting enormous costs on citizens and businesses, but they also pose a significant danger to national security with their growing potential to disrupt major government operations, distort or undermine economic markets, and proliferate weapons of mass destructions. No single law enforcement agency, acting alone, can

counter this threat. But collectively, agencies have the information and capabilities to identify, track, and dismantle these organizations. Countering today's emerging threats will require US law enforcement and security agencies to adapt new operating models that leverage new mission enabling technologies and foster significantly greater collaboration across the traditional boundaries of agency affiliation. The expanded collaboration must include not just other law enforcement organizations but also other US agencies and international partners whose shared mission responsibilities and complementary capabilities can provide valuable support in the global fight against transnational criminals and terrorists. The current environment of budget austerity makes this collaboration vital, while the emergence of well-funded hybrid organizations that facilitate both crime and terrorism argue for an increased sense of urgency. By creating collaborative mission-focused networks and using powerful new analytical tools, law enforcement organizations can operate more efficiently and effectively against sophisticated transnational adversaries. Networked law enforcement operations will provide the agility, flexibility, and strength needed to defeat these threats to our national security and homeland.

Contacts

Bob Sogegian
Vice President
sogegian_bob@bah.com

Anthony Placido
Executive Advisor
placido_anthony@bah.com

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

The firm's management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant's problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm's many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs approximately 25,000 people, and had revenue of $5.86 billion for the 12 months ended March 31, 2012. *Fortune* has named Booz Allen one of its "100 Best Companies to Work For" for eight consecutive years. *Working Mother* has ranked the firm among its "100 Best Companies for Working Mothers" annually since 1999. More information is available at www.boozallen.com. (NYSE: BAH)

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Booz | Allen | Hamilton

Principal Offices

Huntsville, Alabama
Sierra Vista, Arizona
Los Angeles, California
San Diego, California
San Francisco, California
Colorado Springs, Colorado
Denver, Colorado
District of Columbia
Orlando, Florida
Pensacola, Florida
Sarasota, Florida
Tampa, Florida
Atlanta, Georgia
Honolulu, Hawaii
O'Fallon, Illinois
Indianapolis, Indiana
Leavenworth, Kansas
Aberdeen, Maryland
Annapolis Junction, Maryland
Hanover, Maryland
Lexington Park, Maryland
Linthicum, Maryland
Rockville, Maryland
Troy, Michigan
Kansas City, Missouri
Omaha, Nebraska
Red Bank, New Jersey
New York, New York
Rome, New York
Dayton, Ohio
Philadelphia, Pennsylvania
Charleston, South Carolina
Houston, Texas
San Antonio, Texas
Abu Dhabi, United Arab Emirates
Alexandria, Virginia
Arlington, Virginia
Chantilly, Virginia
Charlottesville, Virginia
Falls Church, Virginia
Herndon, Virginia
McLean, Virginia
Norfolk, Virginia
Stafford, Virginia
Seattle, Washington

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com

www.boozallen.com