The Application of "Spiral Analysis" to ABI: Lessons Learned in the Interagency Environment

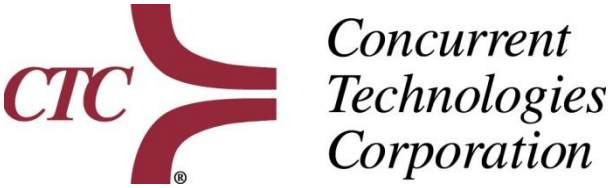
Version: 1.0

August 2014

An examination of lessons learned in the interagency law enforcement environment and the potential application of those lessons to Activity-Based Intelligence.

CTC Author and Technical Point of Contact:
Mr. Randy A. Weaver
Executive Director
Telephone: (814) 269-6223
Email: weaverra@ctc.com

Prepared by:



The Application of "Spiral Analysis" to ABI: Lessons Learned in the Interagency Environment

1.0 PURPOSE

The purpose of this white paper is to provide an in-depth examination of ABI-like analytic techniques that were developed, refined and employed to successfully support multiple, high-level, but dissimilar interagency law enforcement investigations over an extended period of time. The premise of this paper is that, as the Intelligence Community developes a strategy, framework and roadmap for enterprise-wide adoption of ABI, lessons learned from the law enforcement community are worthy of examination and possible incorporation into the IC strategy for ABI.

This paper consists of the following components:

- THE CASE – why lessons learned in an interagency law enforcement context are applicable to ABI
- INFORMATION SHARING, INTERAGENCY COOPERATION AND OSINT – how and why ABI-like processes for exploiting and integrating information from multiple sources were developed and implemented, as well as examples
- CLOSING THOUGHTS – the value of DOMEX and TEO

2.0 THE CASE

As the concept of Activity-Based Intelligence (ABI) moves from a tactical/operational focus to the development of an enterprise-wide, strategic-level approach and the community begins to lay out a roadmap for ABI, it is imperative that we identify and, where appropriate, incorporate experience and lessons learned from multiple mission areas. And, given that ABI is evolving out of intelligence support to military and law enforcement operations, an examination of some of those lessons learned might enhance and further the development of that roadmap and, ultimately, ABI processes and methodologies in a broader sense.

The methodologies described herein were developed primarily for intelligence support to high-level, interagency law enforcement operations. All of the cited examples are highly sanitized, but drawn from real investigations and operations. And, while all began as single-agency investigations – some of which were civil and not criminal in nature, the cited examples eventually evolved into cooperative, interagency investigations and operations. Many of these investigations produced actionable intelligence for other elements of the Intelligence Community and some proved to be directly actionable by military units overseas.While the practice of ABI in these examples was done manually for the most part, it shares a great deal in common with the practice of ABI as it exists today and as it is evolving. Verifiable and provable information from the public domain (OSINT) was integrated into intelligence products generally without regard for the source. Law enforcement data provided rich detail, while OSINT gave that data context and, to a great extent, led to the discovery of previously unidentified information (aliases, addresses, personal and business relationships, etc.) about target organizations and individuals that could be used to revisit other sensitive and classified sources. Furthermore, given advancements in technology, all are suitable for automation in the ABI context.

3.0 INFORMATION SHARING, INTERAGENCY COOPERATION AND OSINT: A MODEL FOR ABI?

As noted previously, the ABI concept is drawn heavily from intelligence support to military operations, especially in the Irregular Warfare (IW) arena, and from law enforcement operations that rely heavily on ABI-like intelligence practices. The Irregular Warfare Joint Operating Concept (JOC) underscores not only the interrelationship between various types of operations, but also the potential value of lessons learned in law enforcement operations when developing a framework and roadmap for ABI. The IW JOC identifies 14 distinct operations and activities that fall within the rubric of IW, the centerpieces of which are insurgency and counterinsurgency, but include such diverse areas as terrorism and a variety of law enforcement operations.

IW Operations and Activities

- Insurgency
- Counterinsurgency (COIN)
- Unconventional warfare (UW)
- Terrorism
- Counterterrorism (CT)
- Foreign internal defense (FID)
- Stabilization, security, transition, and reconstruction operations (SSTRO)
- Strategic communications
- Psychological operations (PSYOP)
- Information operations (IO)
- Civil-military operations (CMO)
- Intelligence and counterintelligence activities
- Transnational criminal activities, including narco-trafficking, illicit arms dealing, and illegal financial transactions, that support or sustain IW
- Law enforcement activities focused on countering irregular adversaries

The nature of the global security environment, including irregular warfare, is vast and varied, involving a wide range of security threats, activities and operations, many of which overlap and require the near-simultaneous application of political, military, intelligence and law enforcement resources to address the broad range of domestic and international threats. This overlap in the nature of threats, activities and operations underscores the necessity for information sharing and analysis at the interagency level and begs the inclusion of lessons learned and processes developed in the interagency environment.

3.1 Development of the Processes. Illicit activities frequently are not susceptible to collection by traditional or technical means, but, in the digital age, they do leave footprints if one knows where to look. And, given the nature of the global security environment and the overlap of threats, activities and operations, intelligence activities at all levels demand a different mindset and innovative approaches, focusing on elements of information and analytic practices not routinely incorporated into traditional "all-source" analysis. To best illustrate the application of these approaches, domestic law enforcement operations and overseas military and intelligence operations in the prelude to and aftermath of 9/11 clearly demonstrated a significant overlap between a broad range of criminal activities, insurgency and terrorism, as well as the value of information sharing and interagency coordination. The examples provided below, although sanitized, are drawn from almost 15 years of trial and error, experimentation, and continuous refinement of processes in an interagency environment:

- Law enforcement investigations of Mexican methamphetamine Drug Trafficking Organizations (DTO) in the early 1990s identified the emergence of individuals with ties to radical Islamic groups as suppliers of precursor chemicals to major Mexican DTOs.

- Although this phenomenon initially appeared in the U.S. Southwest, follow-on enforcement programs and associated investigations documented the fact that the diversion of precursor

chemicals by individuals and organizations with ties to radical Islamic groups was a well-financed and well-coordinated nationwide phenomenon with broad international reach.

- Progressive, iterative integration of interagency information with information from the public domain revealed sources and means of financing for multiple networks of small businesses that facilitated a wide range of criminal activities, including: diversion of precursor chemicals, money laundering, illegal alien smuggling, drug trafficking, arms trafficking and material support to terrorism and documented even more extensive associations with radical Islamic groups.

- The progressive integration and analysis of interagency and public domain information revealed not only details of target networks, but also connections to other, similar networks via identification of sources and means of financing and a variety of other, less visible but identifiable links.

- By the late 1990s, individuals and organizations with direct and indirect ties to radical Islamic groups had established themselves as the preeminent nationwide suppliers of precursor chemicals, especially pseudoephedrine, to Mexican methamphetamine DTOs.

- Several investigations involving the diversion of precursor chemicals – a civil offense, evolved into federal counterterrorism investigations, one of which – a chemical diversion investigation – culminated in the arrest of the so-called "Lackawanna Six" in 2003.

- Associated Document and Media Exploitation (DOMEX) missions uncovered a number of actionable international connections, elements of which were coordinated with the Intelligence Community (IC) and the Department of Defense (DoD).

- Analysis of law enforcement information and subsequent coordination with DoD revealed details of an extensive stateside criminal network associated with radical Islamic groups that is involved in organized retail theft, drug trafficking and the purchase and transportation of used automobiles to the Middle East. Some of the automobiles purchased and transported by this network were used or intended for use as VBIEDs in Iraq.

One of the most potentially exploitable commonalities of criminal, insurgent and terrorist groups and other non-state actors is their dependence upon financial support from a broad variety of state and non-state sources. All use a multitude of means to move and dispose of funds and support operations in multiple locations. Much of the information necessary to identify those transactions resides with law enforcement sources and within the public domain. Intelligence support to interagency investigations and operations in this environment led to the development and refinement of approaches like *Spiral Analysis, Counter-Threat Finance Analysis, Network and Cross-Network Analysis, and Event-Based Pattern/Trend Analysis*.

3.2 Spiral Analysis. As used here, *Spiral Analysis* – a term normally associated with medical diagnoses, is defined as the means by which deliberately-focused OSINT is systematically collected and fused with classified, sensitive but unclassified, law enforcement, and other types of restricted information in a progressive and iterative fashion to "drill" deeper

into networks. *Spiral Analysis* techniques led to the identification of the aforementioned criminal networks, many of which were and are associated with radical Islamic groups.

To develop detailed information in context on targeted networks and associated individuals and businesses, analysts concentrated on exploiting discrete, exploitable elements of information as they were discovered and used that information for subsequent federated searches of agency data. *Spiral Analysis* proved to be especially useful in an interagency environment and was used successfully to integrate and link information from multiple types of investigations (counterterrorism, drugs, illegal immigration, organized crime, fraud, money laundering, etc.) with IC and DoD information and information from the public domain. In many cases, this methodology provided tactically actionable leads to law enforcement and the military.

Spiral Analysis proved to be effective at focusing research and analysis on high-priority targets. It helped to illuminate details of target networks, how they are funded, how they were established and operate and at exposing numerous connections to other, related networks and ferreting out details of those associated networks as well. Furthermore, it proved to be the best means by which OSINT could be fully exploited and integrated into ongoing analysis in a progressive fashion; as details were systematically exposed, analysts could "go back to the well" repeatedly to identify and clarify obscure links using data previously believed to be insignificant.

The illustration below (Figure 1) provides a simplified view of the *Spiral Analysis* process. Upon collection of information at each step, exploitable elements of information (names, aliases, addresses, associated identification numbers/indices, etc.) are identified and exploited by using them as search conditions for the subsequent step. The process is repeated in a "spiral" fashion, drilling deeper and deeper into the public domain and interagency sources of information to develop progressively greater detail and context.

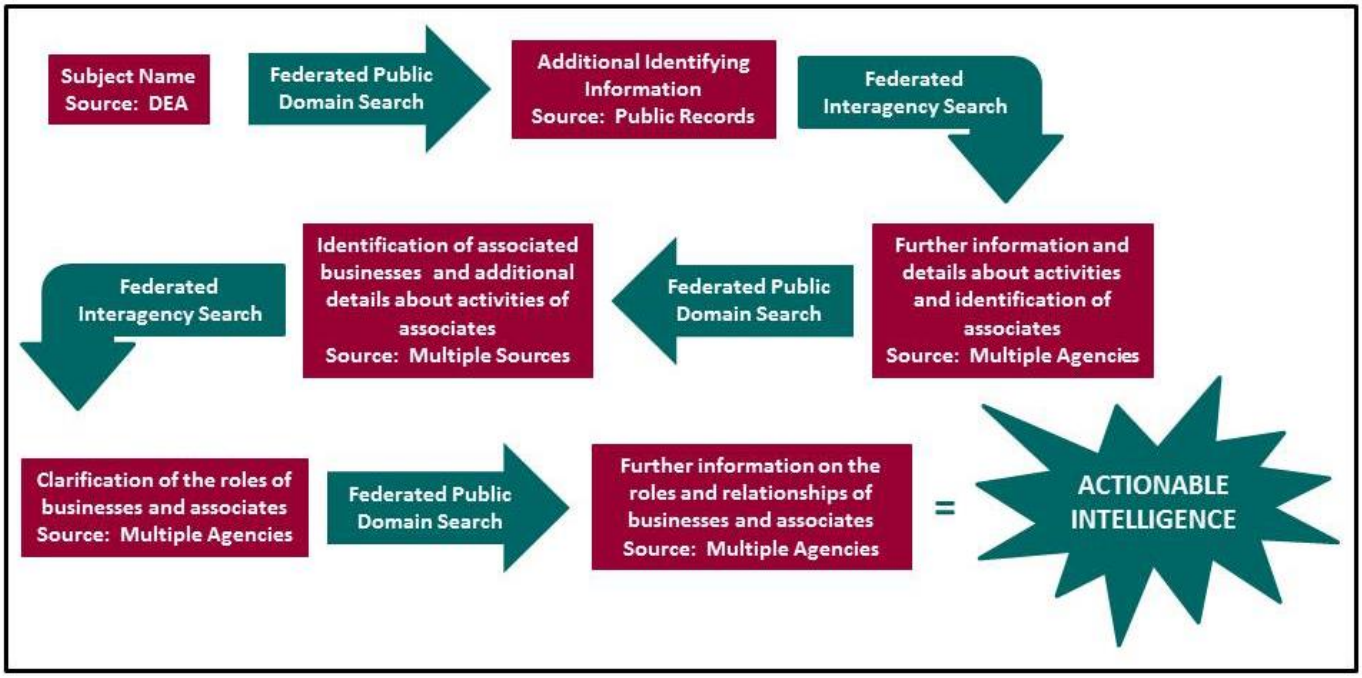


Figure 1 - Spiral Analysis

3.3 Counter-Threat Finance Analysis. Counter-Threat Finance (CTF) Analysis is not, as widely believed, merely forensic accounting. Nor is it simply the analysis of exclusively

financial information (account numbers, deposits, transfers, withdrawals, etc.) to ascertain the source, disposition and use of funds. CTF Analysis is an inherently interagency function wherein financial, business and commercial information is used to identify the source, disposition and use of funds, as well as the identification of businesses and persons, their associates, and other potentially exploitable information that illuminate the details of financial support networks and the activities they support. Ideally, CTF information is then integrated with information from other sources to understand and characterize the roles of those entities in the context of operational networks, the outcome of which *should be* actionable multi-source intelligence.

In the examples cited above, using financial, business and commercial information, analysts were able to identify that many of the small businesses facilitating criminal activity were funded by similar means and, in many cases, by common sources. Those common sources of funding were clearly critical to the support networks they had helped to establish. After identifying sources and means of funding and focusing further research and collection on those sources, analysts were able to identify additional businesses in other areas that were engaged in similar activity. By comparing information on those newly-identified businesses with information from multiple agencies, analysts identified the fact that many of those small businesses were also involved in issuing money orders, checks and other financial instruments that were couriered out of the United States and deposited in banks in the Middle East. In other words, they were not only used to facilitate criminal activity, but also to launder the proceeds of that activity.

The below illustration (Figure 2) shows many of the sources, methods of movement, and means of disposing or illicit funds. Some are clearly more exploitable than others, but in an interagency context, all are potentially exploitable, given access to the necessary information. Regardless of the origin of funds, specific points of vulnerability are exposed whenever money enters the traditional banking system, is wired from one point to another, or is expended in acquiring materiel or paying for services. When materiel is purchased, money is usually transferred in an identifiable manner and a purchase order or transaction receipt is generated. Likewise, the purchase of services such as transportation generates receipts, bills of lading, commercial invoices and flight plans, all of which are also exploitable.

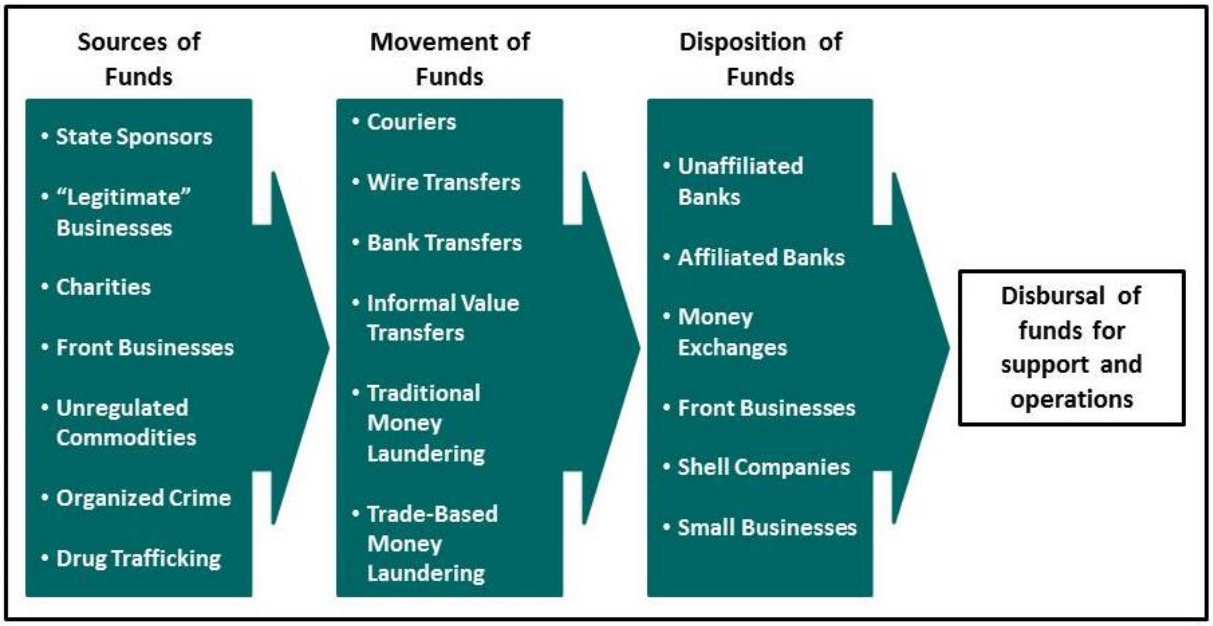


Figure 2 – Illicit Money Movement

Threat organizations are especially adept at identifying the inherent weaknesses and vulnerabilities of the banking, business and regulatory systems of the countries in which they operate. They will take advantage of any available opportunities to fund operations and transfer funds. If drug trafficking or related criminal activity is widespread, they will insinuate themselves into the drug trade or a supporting activity like precursor chemical diversion or money laundering. Likewise, they will take advantage of all available means to launder and transfer money. For example, if operating in a country like Colombia, they may use the Black Market Peso Exchange[1] and Colombian money brokers to launder the proceeds of illegal activity. In the United States, they may use high cash flow businesses like convenience stores, liquor stores, gas stations, etc., to place illicit funds into the banking system. If operating in a country with ready access to *Hawaladars*[2], they may use their services to transfer funds, or avail themselves of the use of wire transfer businesses. Their use of methods in any given area will probably not be restricted to a single method alone, but rather a combination of methods, especially as funds transit international borders.

When moving funds from one area to another, threat organizations will probably pass transactions through different countries using a combination of means to launder and transfer funds from one location to another. The proceeds of the diversion of pseudoephedrine in the United States could be laundered through a small business that facilitates the illegal activity. From a bank account associated with that small business, the money can be withdrawn and wired to another account in Europe via a trusted wire transfer company. The money could be withdrawn from the bank in Europe and couriered to yet another country in Southern Europe or Africa, deposited to an account in a trusted bank, then transferred by the bank to an account in

[1] The Black Market Peso Exchange is a system by which drug money profits are laundered through the use of international trade and blocked currency accounts.

[2] Hawala (also known as Hundi) is an informal value transfer system based on the performance and presumed honor of a huge network of money brokers located primarily in the Middle East, North Africa, the Horn of Africa and South Asia. Hawala money brokers are known as *Hawaladars*.

yet another trusted bank in the Middle East where it is readily available for withdrawal by one or more threat organizations, sometimes from a common account. Even given the use of multiple methods to launder, move and disburse funds, whenever those funds transit formal banking and commercial systems, they are potentially exploitable.

The ultimate utility of CTF analysis, especially when practiced in an interagency environment and using a liberal infusion of OSINT is that it can greatly aid in exposing the details of support networks:

- At the source, exposing a business involved in illegal activity, the proceeds of which are used to fund terrorist or insurgent operations, can shed light on how and by whom such businesses are funded.
  - Identification of the sources and means of funding can lead to the identification of still more associated businesses involved in similar activity.
  - By following the flow of money from those businesses, agencies can gain valuable insight into the means of movement and the destination of funds.
- In the middle of this cycle is the actual transfer or movement of money.
  - Couriers can, and have been, intercepted carrying large amounts of cash or negotiable instruments, which can, in many cases, be tracked to specific banks, accounts and individuals.
  - Reporting vehicles like those mandated by the so-called Bank Secrecy Act (Title 31 U.S.C., § 5311-etc.) and the Patriot Act, as well as corresponding foreign anti-money laundering statutes can lend insight into suspicious financial activity.
  - Unexplained high volumes of activity at money exchanges can be an indication of threat finance activity, as can repeated wire transfers to and from banks and money exchanges in certain areas.
- At the end of this cycle are the banking and non-banking financial institutions, *Hawaladars*, and other disbursers of threat funds. While identification of the institutions and individuals responsible for disbursing funds for threat operations is difficult, it can be accomplished, but is primarily the purview of law enforcement, the IC, and the military.

The challenge for law enforcement is to prove that the proceeds of criminal activity ultimately are used to fund threat operations, whereas the challenge for DoD and the Intelligence Community is identifying the source of funds, the individuals and businesses responsible for moving those funds and the intended recipient(s). This common interest, but difference in focus regarding threat finance makes a clear and compelling case for greater information sharing and an interagency approach to analysis.

3.4 Network and Cross-Network Analysis. The techniques and methodologies discussed in the preceding paragraphs are not an end unto themselves, but rather a means to multiple ends, one of which is identification of key individuals in networks that support and conduct threat operations. As discussed above, the application of spiral and CTF analytic techniques can

identify not only critical persons or nodes in these networks, but also can identify links to other networks.

In the notional example depicted below, sources identify Subject 1 as the purchaser of a large quantity of IED components discovered on the battlefield in Afghanistan. Shipping documents identify Subject 2 as the payee for transportation of those components to a warehouse leased by Subject 3. Using spiral analytic techniques and incorporating financial, business and business-related information from the public domain, analysts identify Subject 2 as the payee for transportation of the components from the warehouse leased by Subject 3 to a recipient of the components, Subject 4, in Afghanistan. Subject 2 again pays for the transportation of the components to a village where the components are assembled by a bomb maker into an IED. Tactical sources indicate that Subject 5, a member of the Taliban, oversees the assembly of the components and arranges for the transportation of the IED to the location where it is emplaced.

Although network analysis of this type is by no means simple nor quick, it is entirely plausible, given access to the right information from the right sources. Furthermore, it need not be the final product of analysis. Using non-linear, or *Spiral*, analytic techniques and identifying potentially exploitable elements of information pertaining to Subjects 2 and 5, analysts identify their association with and involvement in yet another network. Subject 2, in this case, also paid for the transportation of a terrorist from his home country to a training camp and, upon completion of the training, paid for the terrorist's transportation to Afghanistan where he was met by Subject 6, another member of the Taliban. Analysts document an association between Subjects 5 and 6 and identify the fact that Subject 5 arranged for the transportation of the terrorist to a village in the Helmand province, where he is met and given instructions by Subject 7, who also arranges for his transportation to Kandahar, where he conducts a suicide bombing near a coalition base.

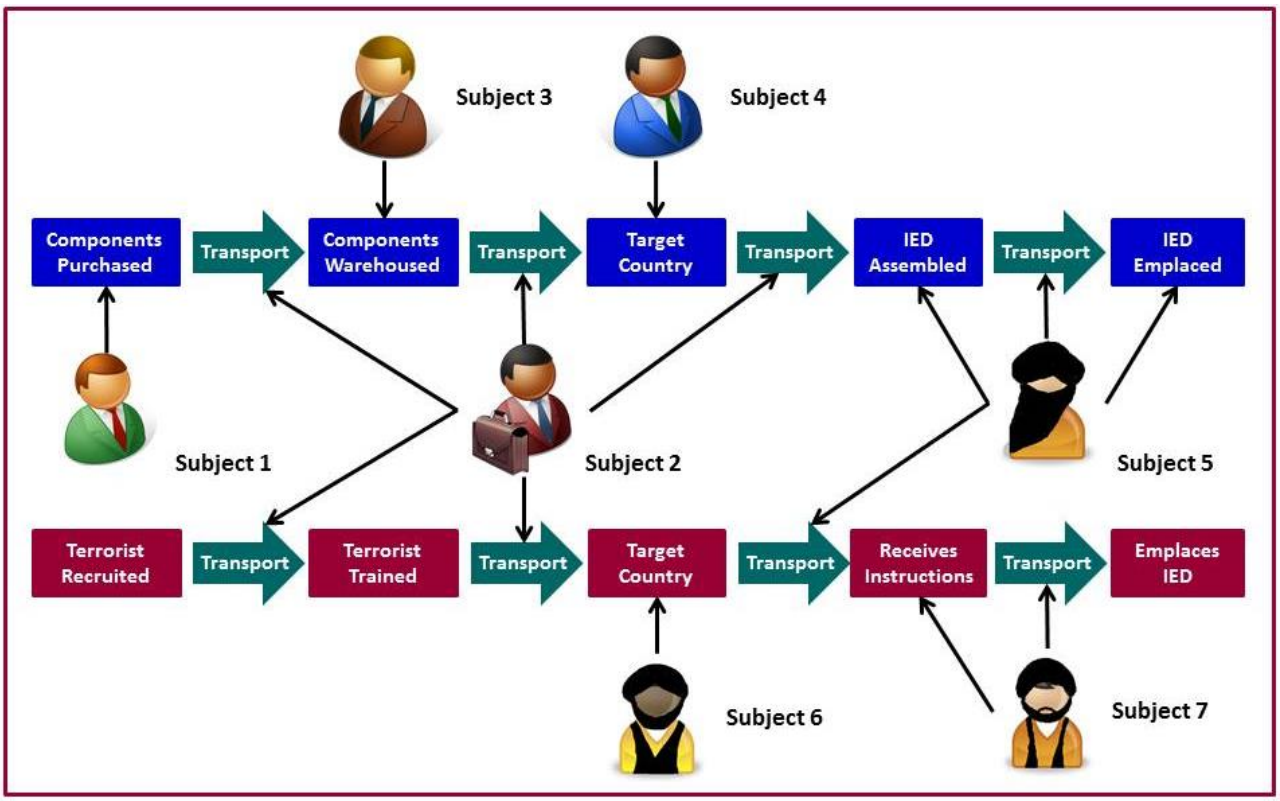


Figure 3 - Network and Cross-Network Analysis

Although greatly simplified in this case, the above example is an accurate depiction of how analysts were able to document many of the connections identified in the opening paragraphs. By repeatedly "going back to the well" as additional, potentially exploitable elements of information were identified, and conducting research of classified, law enforcement, and public domain sources, analysts developed considerable detail on target networks, identified additional, associated networks and, in the process, identified key persons associated with one or more of those networks.

3.5 Event-Based Pattern/Trend Analysis. Pattern and trend analysis is a well understood and long-practiced analytic technique. It is normally associated with high-interest, national security-related issues in which analysts establish patterns, or norms, of activity associated with a given issue and identify trends, or deviations, from the norm of that activity and ascertain their meaning.

Event-Based Pattern/Trend Analysis is a more focused variation of pattern and trend analysis and, by its nature, more suited to the IW operational environment. It tends to be more tactical in nature and, as indicated by its name, more focused on specific events and the activity that precedes them. As such, it is a hybrid blend of pattern and trend analysis and Indications and Warning planning and analysis, best explained by examples, and it can be applied to a broad range of threat-related activities.

Event-Based Pattern/Trend Analysis can be either proactive or reconstructive, but in either case is highly data intensive and very focused. Although notional, the following examples are representative of how analysts would use multi-source and public domain information to produce potentially actionable intelligence based on pattern and trend analysis:

- Proactive:

  - Intelligence sources identify that a radical Islamic terrorist organization has established operations in southern Colombia and is trafficking Colombian cocaine and heroin to Europe to fund its operations (a *pattern*).

  - Law enforcement reporting notes that Colombian cocaine and heroin bound for Europe is concealed predominantly within shipments of coffee that originate in Barranquilla (a *pattern*).

  - Analysts amass and integrate large volumes of commercial shipping data, focusing on coffee shipments from Colombia to Europe, and update the data on an almost daily basis, noting that most shipments of coffee from Colombia originate in Cartagena (a *pattern*).

  - Shipping documentation identifies the ports of London, England, and Bremerhaven, Germany, as primary ports of embarkation for shipments of coffee from Colombia (*pattern*).

  - Analysts establish that coffee shipments from Cartagena, which take from 18 to 20 days to London and 19 to 21 days to Bremerhaven (*pattern*).

  - INTERPOL, Her Majesty's Customs and Revenue, Scotland Yard, the German Customs Administration and the Bundespolizei identify Liverpool, England, and Hamburg, Germany, as two European ports with a heavy influx of cocaine and heroin from Colombia (*pattern*).

  - In examining a daily update of commercial shipping data, analysts note that, of five shipments of coffee scheduled to depart Colombia, four originate in Cartagena and are bound for either London or Bremerhaven (consistent with previously identified *patterns*). However, they also note that one originates in Barranquilla and is bound for the Port of Liverpool (a *trend*), an area with high unemployment and a high incidence of cocaine and heroin abuse.

  - Analysts provide details on the suspect shipment from Barranquilla to a law enforcement liaison for notification and passage to the appropriate authorities in Great Britain and to INTERPOL. (In this case, actionable intelligence leads to a targeted inspection and the seizure of contraband constitutes the *event*.)

- Reconstructive – this example is independent of the above example and presumes that none of the information from the preceding example is yet available to analysts:

  - The German Bundespolizei seize a cache of automatic weapons from a shipment of coffee in the Port of Hamburg and identify that the shipment originated in Barranquilla. (In this case, an *event* leads to a detailed, focused examination of coffee shipments from Colombia to identify patterns of legitimate commercial activity, as well as indicators of suspect shipments.)

- Analysts conduct searches of multi-agency and public domain data and identify four similar shipments that have been seized in the past year. Of those four, two originated in Barranquilla with seizures in Calais, France, and Cadiz, Spain, and one originated in Buenaventura with a corresponding seizure in the Port of Zamboanga, Phillipines. In all cases, weapons, ammunition and cocaine were concealed within a shipment of coffee. (Given this information, both Barranquilla and Buenaventura would be considered *indicators* and potentially suspect origins for shipments of coffee. Likewise, the ports of Hamburg, Calais, Cadiz and Zamboanga would be considered *indicators* as potentially suspect destinations for shipments of coffee, assuming they were not routine destinations for such shipments.)

- In examining shipping documents associated with routine coffee shipments, analysts determine that well-known international coffee brokers constitute 97 percent of the owners of coffee shipped from Colombia. In the five instances in which weapons, ammunition and illegal drugs were seized, two trading companies, Tomateek Trading, Ltd., and Canadah International Trading, S.A., two import/export companies based in Yemen, accounted for all five. (Given this information, analysts would consider any shipments brokered by Tomateek and Canadah as suspect – two more *indicators*.)

- As a result of the preceding analysis, analysts conduct a thorough examination of shipping records and identify three other shipments of coffee brokered by Tomateek and Canadah, two of which originated from Buenaventura and the other from Barranquilla and note that one shipment is still in transit to the Phillipines.

- Analysts provide details of the shipment to a law enforcement liaison for notification and passage to the appropriate authorities in the Phillipines. (In this case, as in the preceding example, actionable intelligence leads to a targeted inspection and the seizure of contraband.)

- Unlike the preceding example, in this case – prior to the seizures, little if anything is known of the activity in Colombia and the organizations with which it is associated. In an interagency setting and under ideal circumstances, identification of the nature of the shipments and the identification of two import/export companies based in Yemen would prompt the initiation of a variety of operations by law enforcement, the IC and, potentially, the military. The resulting body of information resulting from those operations would, presumably, contribute to further, similar operations and more effective intelligence support to future operations.

4.0 SOME CLOSING THOUGHTS

The examples provided above are but very abbreviated, albeit representative depictions of the results of applying advanced analytic techniques to support interagency/task force investigations. While I have focused on analytic techniques using examples from the interagency environment, I would like to offer some additional, closing thoughts on another issue that could greatly enhance the value and effectiveness of analysis and Intelligence production in an interagency environment, Tactical Exploitation Operations (TEO) and Document and Media Exploitation (DOMEX).

As indicated in virtually every one of the previous examples, analytic support to operations is heavily dependent on tactical information. One of the most valuable sources of tactical information is the information provided by TEO and DOMEX operations. DOMEX support to many of the investigations from which the previous examples were drawn demonstrated the value of Intelligence Requirement-driven DOMEX operations. By performing triage of seized evidence and providing timely, on-site exploitation of media (hard copy and electronic), as well as focusing on information requirements identified by case agents and prosecutors, analysts were able to generate highly-exploitable information almost immediately, as well as fully-referenced knowledge bases containing detailed information extracted from seized evidence, usually within a week. While rules of evidence applied in many of these cases, some information was immediately made available to interagency partners and greatly enhanced the body of knowledge available on high-priority investigative targets and subjects of national security interest. A similar approach to exploiting documents and other media captured during raids and ensuring that the resulting information is made available to analysts – especially in an interagency activity, would ensure the timely incorporation of that information and greatly enhance not only the body of knowledge, but efforts at targeting key individuals and other entities within threat operational and support networks.

Clearly, the very nature of the global security environment and the involvement of so many agencies with varying but complementary roles, missions and responsibilities demands a concerted, interagency approach to intelligence operations, analysis and, ultimately, ABI. The traditional "all-source" approach to analysis will not suffice if we are to succeed in addressing the broad range of overlapping security threats inherent to the current global security environment. The examples presented above, while sanitized, are drawn from real-world examples and offer some insight into the results that can be achieved by adopting an interagency approach to intelligence and integrating analytic techniques that go well beyond all-source analysis.

About the Author

Mr. Randy A. Weaver is the Executive Director, Advanced Intelligence Solutions, Concurrent Technologies Corporation, where he is responsible for technological support to the U.S. Intelligence Community. Mr. Weaver also serves as a corporate advisor in the areas of Irregular Warfare, Advanced Analytics, Interagency Operations, Counterterrorism and Counterdrug Operations, and Homeland Security.

He received a B.S. in Liberal Studies with concentrations in Political Science, Mathematics and Russian from the State University of New York at Albany, a M.S. in Strategic Intelligence from the Defense Intelligence College, and he is a 2001 graduate of the Senior Executive Fellows Program at Harvard University's John F. Kennedy School of Government.

Over the course of his almost 40 years as an intelligence professional, Mr. Weaver has served in a wide variety of intelligence positions in the United States and overseas. He has served with the U.S. Army, the Federal Bureau of Investigation, U.S. Department of Justice, the White House, and the U.S. Department of Homeland Security and has worked with, or for, virtually every member organization of the U.S. Intelligence Community. Mr. Weaver's military career covered a broad range of tactical, operational and strategic assignments and included nine years of experience in signals and electronic intelligence and over 10 years of experience specializing in intelligence support to unconventional operations. His career is highlighted by numerous Army and joint commendations, as well as commendations from Members of Congress, the U.S. and state Attorneys General, U.S. Attorneys, and the White House Chief of Staff.

Mr. Weaver has extensive experience in Signals Intelligence, Human Intelligence, and All-Source Intelligence analysis, as well as counterterrorism, criminal intelligence, counterinsurgency and counterdrug operations and analysis. Mr. Weaver spent almost the entirety of the latter half of his government career in the interagency environment where he coordinated intelligence support to high-level investigations and interagency programs with various federal, state and local law enforcement agencies, members of the Intelligence Community, and the Department of Defense. In the course of his time in the interagency community, Mr. Weaver developed a process he termed "Spiral Analysis", which was applied to various complex intelligence challenges and described in detail herein.

An experienced public speaker and author, he has taught and spoken at numerous state, regional, national, and international conferences on a variety of subjects related to intelligence. Among the highlights of his career, he served as: Chief of the Unconventional Warfare/Low Intensity Conflict Threat Branch at the U.S. Army Intelligence Center, where he instructed over 3,000 U.S. and foreign intelligence officers in the U.S. and overseas; Senior Intelligence Officer at the White House on the staff of former Pennsylvania Governor and DHS Secretary Tom Ridge; Deputy Director of Operations for the U.S. Department of Homeland Security; Chief of Document and Computer Exploitation for the U.S. Department of Justice, National Drug Intelligence Center; and concluded his career with the U.S. Government as Assistant Director for Intelligence, National Drug Intelligence Center.