'Threat Finance' – Unraveling the Finances of National Security Threats to Choke Off Terrorism, Trafficking, Corruption and Other Perils

Thursday, May 16, 2013 | 10:45 AM-12:00 PM

Speakers:
Dan Barta, Jim Bischoff, Sonia Desai, JR Helmig and Marissa Michel
Jim Bischoff
Chief, Counter Threat Finance
US Special Operations Command
Tampa, FL
Dept of Defense Counter Threat Finance

• **FINANCE**: Refers to all forms of currency and items of value that are exchangeable for currency, material, weapons, shelter, transportation, communications, services, favors and other forms of support

• **THREAT FINANCE**: The manner in which adversarial groups raise, move and use funds to support activities.

**COUNTER THREAT FINANCE**: Activities and actions taken by the DoD and other US Government organizations to Deny, Disrupt, Destroy, or Defeat threat finance systems and networks. This includes persons and entities that provide financial and material support to illicit networks such as terrorists, insurgents, drug traffickers, weapons traffickers, human traffickers, and corrupt government officials.

**CTF:**

- Compliments Special Operations’ ongoing targeting and operations
- Adds another capability to Special Operations
- Unites many partners in targeting a threat network
- Provides for additional access and authorities
- Is a key enabler in non-kinetic environment
- Can save lives and reduce risk
# DoD CTF Methodologies

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Challenges</th>
<th>Enemy Countermeasures</th>
</tr>
</thead>
</table>
| Administrative Sanctions/Designations | • US or UN  
• Freezing of assets  
• Name and shame | • Lack of political will  
• Inability to monitor  
• Classification of evidentiary | • Sideslip  
• Use alternate low visibility money transfer methods |
| Diplomacy                  | • Persuading countries to take action                                       | • Lack of political will, fear of public backlash                        | • Operate in tolerant countries                                |
| DOD CTF                    | • Operational financial support  
• Critical targeting  
• Collection & analysis | • Traditional challenges (access)                                         | • Enemy adaptive                                                 |
| Law Enforcement            | • Domestic and Int’l investigations/ops  
• Prosecution | • Partner Nation lack of political will/legislation  
• Partner Nation lack of expertise  
• Evidentiary | • Operate in tolerant countries |
| Capacity Building          | • Education and training  
• Technology exchange  
• Combined ops | • Lack of political will  
• Lack of transparency | • Changes to TTPs |
| Military Operations        | • Kill/Capture  
• Information Operations  
• Network Analysis | • Limited to war zones, Rules of Engagement, timing  
• 3\textsuperscript{rd} & 4\textsuperscript{th} order effects | • Quick backfill  
• Alternate methods for finance |
Money Laundering at Lebanese Bank

The chart below shows the intricate money-laundering system the Lebanese Canadian Bank used to divert money to the Shiite militant group Hezbollah, according to United States officials.

According to American officials, the Lebanese Canadian Bank was the hub of an international drug money laundering operation with ties to Hezbollah. Used car and other consumer goods sales revenues had been used to mask the proceeds of illegal drug trade.

Cocaine is sent from Colombia to European markets via Africa.

Used cars are shipped from the U.S. and sold in Africa.

Drugs are sold in Europe. Proceeds are mixed with legitimate used car sale profits in Africa and sent to the L.C.B. through exchange houses.

Some money is returned to the U.S. to purchase more used cars.

Money from the L.C.B. is sent through U.S. accounts to pay Asian suppliers of consumer goods.

Goods from Asia are shipped to consumer product dealers and sold in South America in a scheme to pay off cocaine suppliers.

Dept of Defense Counter Threat Finance (CTF):

- Compliments Special Operations' ongoing targeting and operations
- Adds another capability to Special Operations
- Unites many partners in targeting a threat network
- Provides for additional access and authorities
- Is a key enabler in non-kinetic environment
- Can save lives and reduce risk

COTONOU CAR PARK OVERVIEW
COTONOU, BENIN

22 December 2002
FINANCE: Refers to all forms of currency and items of value that are exchangeable for currency, material, weapons, shelter, transportation, communications, services, favors and other forms of support.

THREAT FINANCE: The manner in which adversarial groups raise, move and use funds to support activities.

COUNTER THREAT FINANCE: Activities and actions taken by the DoD and other US Government organizations to Deny, Disrupt, Destroy, or Defeat threat finance systems and networks. This includes persons and entities that provide financial and material support to illicit networks such as terrorists, insurgents, drug traffickers, weapons traffickers, human traffickers, and corrupt government officials.

CTF:
- Compliments Special Operations’ ongoing targeting and operations
- Adds another capability to Special Operations
- Unites many partners in targeting a threat network
- Provides for additional access and authorities
- Is a key enabler in non-kinetic environment
- Can save lives and reduce risk
JR Helmig
Founder
Leveraged Outcomes
Washington, DC
Alternate View – Wall St. Style

• How to define “Threat”
• How to define “Finance”
• Plugging holes or draining swamps?
• Current vs. Future
Current State – Key Questions

- When does “it” become a threat?
- When is “it” observable?
- What can be ascertained?
- By whom?
- For what outcome?
- KYC redefined—who is hurt?
Future State – Key Questions

• Is it here already?
• Inside your system?
• If I were a bad guy...
• What if the flash crash occurred again, on purpose?
What fears keep you up at night?
What excites you the most?

jr@leveragedoutcomes.com
www.leveragedoutcomes.com
Daniel Barta
Senior Industry Consultant, Security Intelligence Practice
SAS Institute, Inc.
Cary, NC
Addressing Threat Finance with Data Analytics

• Analytic Approaches

• Data

• Challenges and Needs
Big data could uncover clue on marathon: Column

Scott Sigmund Gartner 11:19 a.m. EDT April 16, 2013

Americans object to invasions of their privacy. But in this case, video could help.

Having grown up in Atlanta, I remember the shock and fear sparked by the explosion in Centennial Park at the 1996 Olympics, which was followed by public frustration as the criminal investigation seemed to stumble and fail. Many could not understand how a bombing at one of the most public events in the world could be seemingly untraceable.

Forensics software could help finger Boston bomber

Byron Acohido, USA TODAY 5:05 p.m. EDT April 18, 2013

SEATTLE – Video forensics software that can recognize and catalogue nuances in the physical characteristics of a person’s face, or even a distinctively-shaped object, such as a backpack, could deliver key evidence in the Boston Marathon bombing investigation.

Forensic software has come a long way since terrorists detonated multiple bombs in London’s subway system in 2005. Then hundreds of investigators spent thousands of hours manually reviewing surveillance camera video with meager results.
# Using a Hybrid Approach for Threat Finance

## Issues

- Detect unknown patterns of financial fraud
- Keep track of new fraud schemes
- Unsure exactly what to look for

## Rules

<table>
<thead>
<tr>
<th>Suitable for known patterns</th>
<th>Suitable for unknown patterns</th>
<th>Suitable for complex patterns</th>
<th>Suitable for associative link patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up rules to filter fraudulent transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two transactions in different time zones within short period of time</td>
<td>Detect individual and aggregate abnormal patterns</td>
<td>Perform advanced analytics</td>
<td>Perform knowledge discovery through associative linkage analysis</td>
</tr>
</tbody>
</table>

## Anomaly Detection

- Mean, standard deviation, percentiles, univariate and multivariate robust regression, clustering, sequence analysis, peer group analysis

## Advanced Analytics

- Neural networks, decision trees, generalized linear models, econometric models, gradient boosting

## Social Network Analysis

- Social network + linkage analysis + community detection + advanced analytics

---

**Prevention vs. Detection vs. Investigation**

---

---
Data – What is Available?

Threat finance is not just about money. It is also about relationships between people and organizations and how they utilize funds.

**Monetary Activity**
- Transaction Monitoring
- Instructions (Wire, SWIFT, CHIP, etc.)
- Card – transaction value, merchant, & location
- On-Line banking – device ID and IP address
- Trade Finance/Import - Export

**Non Financial Information**
- Photos
- Video
- Cell/Mobile device – geo-location, relationships
- Travel information – flight/hotel reservations
- Investigative results
- Border Crossing information

**Unstructured Data**
- Email
- Phone conversation
- Text messages
- Social network sites
- Blog postings
Challenges and Needs

- Data characteristics
  - Unstructured data
  - Data access and privacy

- Organization structure
  - Hierarchical vs. matrix

- User interface functionality
  - Investigative findings

- AML vs. terrorist financing
  - Origins of funding
  - Informal remittance systems
Marissa Michel

Director, Threat Management Group
PwC
Mclean, VA
Threat Finance in today’s marketplace: why should companies care?

Private companies across industry - not just financial services - are increasingly concerned that threat finance will be uncovered in their organizations. This concern stems from the regulatory, reputational, operational, and financial issues that can result.

Primary considerations:
- Compliance with regulations
- Bottom line
- Fines
- Consumer confidence
- Reputation

Also concerned with:
- Playing a positive role in national security
- Knock-on effects – if bad actors are using your company to move money, what else are you exposed to?
- Other, connected risk areas – corruption, money laundering, tax evasion, cyber as threat vector
How do we define threat finance and who does it touch in today’s marketplace?

The financing of terrorist and militant groups, organized crime, as well as other state and non-state actors engaging in unlawful activities including the full scope of financial crimes. In short, it is the financing of actors that pose reputational and legal risk to global companies.

A more appropriate question might be: who doesn’t it touch?

Terrorist groups are increasingly using licit commerce channels, widely accepted currencies, and sophisticated means to raise, move, hide, and ultimately, deploy funds to conduct unlawful activities.

Why?
- Transaction speed
- Currency acceptance/universality
- Scalability
- Variances in law by jurisdiction
- Increasingly globalized/cross border transactions
- Easier to hide
- More lucrative than some illicit activities

Who’s at risk?
- Import export firms
- Natural resource extraction
- Cash intensive businesses
- Global supply chains
- Mobile telecom companies
- Shipping companies
- Companies operating in jurisdictions w/ weak governance
Addressing the problem of the weakest link

To fully address the problem of threat finance, companies must go beyond the obligatory checks in order to know who they are truly working with. This involves peeling back the layers of entities to unearth the connections, the financing, and the relationships of counterparties. Unexamined connections become the weakest link, and therefore the greatest exposure.

Current typical measures

- Basic customer checks
- Electronic party screening
- Counter-party representations and certifications
- Automated screening
- Internal system audits
- Risk-based client transaction monitoring
Moving toward comprehensive financial risk analysis

In today’s financial environment, private sector players need to take a holistic approach to risk analysis. This iterative process needs to be tailored to an organization’s size and resources in order to make informed, risk-based business decisions.

• **Risk assessment:** Companies should determine their exposure

• **Prioritize limited resources:** No unlimited budget or time

• **Enhanced due diligence:** Reputation and backgrounds of those involved in your partners, joint-ventures and suppliers

• **Appropriate governance structure:** clearly articulated roles and responsibilities, and enterprise-wide accountability

• **Compliance at the center:** Leading practices, proactive communications, employee training
Terrorists in the deal stream: If we find them, they are typically financiers many levels above operatives carrying out attacks

The indicators we find are rarely signposts of terrorist intent...

- Our research identifies financial connections, who may have limited or no knowledge of how or when their donations will be used
- Financial and commercial information is a necessary but insufficient condition to identify pending attacks
- Contextual or “insider” lead information is needed to complete the picture

... but are micro-level activity the involved parties don’t want exposed

- Vested interests and silent partnerships in companies
- Unusual transactions with no obvious business purpose
- Checkered business, financial, or personal history
- Criminal records, lawsuits, and hidden assets
- Hidden political connections, donations, and potentially worrying relationships
Please Join Us in Diplomat 1 for a Networking Luncheon Courtesy of:

FinScan
Powered by Innovative Systems