



# The “New” Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security

**March 2013**

**Contributing Authors:** Mr. Gary Ackerman (START); Maj David Blair (USAF/Georgetown University); Ms. Lauren Burns (IDA); Col Glen Butler (USNORTHCOM); Dr. Hriar Cabayan (OSD); Dr. Regan Damron (USEUCOM); Mr. Joseph D. Keefe (IDA); Col Tracy King (USMC); Mr. David Hallstrom (JIATF West); Dr. Scott Helfstein (CTC); Mr. Dave Hulsey (USSOCOM); Mr. Chris Isham (JIATF West); Ms. Mila Johns (START); Mr. James H. Kurtz (IDA); Dr. Daniel J. Mabrey (University of New Haven); Dr. Vesna Markovic (University of New Haven); MG Michael Nagata (Army, J-37); Dr. Rodrigo Nieto-Gomez (NPS); Ms. Renee Novakoff (USSOUTHCOM); Ms. McKenzie O’Brien (START); Dr. Amy Pate (START); Ms. Gretchen Peters (George Mason University/Booz Allen Hamilton); Mr. Christopher S. Ploszaj (IDA); BG Mark Scraba (USEUCOM); Mr. William B. Simpkins (IDA); Dr. Valerie B. Sitterle (GTRI); Mr. Todd Trumpold, (USEUCOM); Mr. Richard H. Ward (University of New Haven); Mr. Tom Wood (JIATF West); Dr. Mary Zalesny, (Army Strategic Studies Group, PNNL)

**Editors:** Mr. Ben Riley (OSD-AT&L/ASD(R&E)) and Dr. Kathleen Kiernan (Kiernan Group Holdings)

**This white volume represents the views and opinions of the contributing authors. This report does not represent official USG or Command policy or position.**

Carley St. Clair  
Kiernan Group Holdings  
stclair@kiernan.com

## Contents

Preface, MG Michael Nagata (JS/J-3/DDSO).....	4
Executive Summary, Dr. Hriar Cabayan (OSD).....	6
Introduction, Mr. Ben Riley (OSD-AT&L/ASD (R&E)) and Dr. Kathleen Kiernan (Kiernan Group Holdings) .....	26
Chapter 1 Command Perspectives.....	28
a. DOD Role in Combating Transnational Criminal Organizations, Mr. Dave Hulsey et al (USSOCOM) .	28
b. Combating Transnational Criminal Organizations in the Western Hemisphere: It, too, Takes a Network, Col Glen Butler (USNORTHCOM) .....	39
c. USPACOM Perspective on Transnational Organized Crime, Mr. David Hallstrom, Mr. Tom Wood, and Mr. Chris Isham (JIATF West, USPACOM) .....	54
d. Transnational Organized Crime: A USSOUTHCOM Perspective, Ms. Renee Novakoff et al (USSOUTHCOM) .....	59
e. Stronger Together: Building EUCOM’s Network to Combat Organized Crime in Europe, BG Mark Scraba and Mr. Todd Trumpold (Joint Inter-Agency Counter Trafficking Center, USEUCOM) .....	65
Chapter 2: Interagency Cooperation for Major Multijurisdictional Operations, Ms. Lauren Burns, Mr. Joseph D. Keefe, Mr. James H. Kurtz, Mr. William B. Simpkins, Mr. Christopher S. Ploszaj (IDA), and Col Tracy King (USMC) .....	71
Chapter 3: The Intersection of Crime and Conflict, Ms. Gretchen Peters (George Mason University/Booz Allen Hamilton) .....	81
Chapter 4: The Connected Illicit System: A Glimpse at the Illicit Superhighway, Dr. Scott Helfstein (CTC/West Point) .....	86
Chapter 5: Analyzing and Evaluating Criminal Organizations, Dr. Daniel Mabry and Dr. Richard Ward (University of New Haven) .....	99
Chapter 6: The Contemporary Face of Transnational Criminal Organizations and the Threat They Pose to U.S. National Interest: A Global Perspective, Dr. Vesna Markovic (University of New Haven) .....	110
Chapter 7: The Threat of Pakistani Criminal Organizations: Assessing the Potential for Involvement in Radiological/Nuclear Smuggling, Collaboration with Terrorist Groups, and the Potential to Destabilize the Pakistani State, Dr. Amy Pate, Ms. Mila Johns, Mr. Gary Ackerman, and Ms. McKenzie O’Brien (START/University of Maryland) .....	120
Chapter 8: Networking and Legitimization of Transnational Crime Organizations, Dr. Mary Zalesny (Army Strategic Studies Group) .....	129
Chapter 9: The symbiosis of technology and TCOs and what that entails for the future, Dr. Valerie Sitterle (Georgia Tech).....	138

Chapter 10: The Geopolitics of Clandestine Innovation in the Drug Business: A Framework of Analysis to Understand Adaptation Capacities of TCOs, Dr. Rodrigo Nieto-Gomez (NPS) ..... 150

Chapter 11: Game-Changing Developments in the Proliferation of Small Arms and Light Weapons: Anonymizing Technologies and Additive Manufacturing, Dr. Regan Damron (USEUCOM)..... 160

Chapter 12: Turning Technology’s Tables on Trafficking: Building an Anti-Human Trafficking (AHT) Data Ecosystem, Maj David Blair (USAF/PhD Candidate, Georgetown University) ..... 175

Appendix A: References..... 181

Appendix B: Acronyms..... 202

## Preface

Major General Michael Nagata  
[michael.k.nagata.mil@mail.mil](mailto:michael.k.nagata.mil@mail.mil)

U.S. Army

J-37, Deputy Director for Special Operations

With the signing of the United Nations Convention against Transnational Organized Crime in Palermo, Italy, in December 2000, the international community demonstrated the political will to answer a global challenge with a global response. If crime crosses borders, so must law enforcement.

United Nations Convention Against Transnational Organized  
Crime

You can get more with a kind word and a gun than you can with just a kind word.

Al Capone

I begin this preface with these quotes because both matter. The examinations within this work are intended to assist the reader in considering and confronting the extraordinarily complex challenge of Transnational Criminal Organizations. I believe our consideration should be "bookend-ed" by two realities that our efforts are unlikely to change, listed below.

1. Criminals will be the first to exploit the vulnerabilities and opportunities that arise from a rapidly changing world. Governments, like our own, will be challenged to keep pace with, much less stay ahead of, such actors and their networks, though try we must.
2. Crime and the criminals that conduct it will remain with us. No TCO effort will eliminate crime itself.

As a serving Military Officer, I must acknowledge a very poor understanding of crime and criminals that commit it. Therefore, it is an easy transition to the admission that I also do not understand Transnational Crime. Finally, this also means I do not understand what Transnational Criminal Organizations are, how they operate, or how to combat them effectively.

I, and those I serve with in the U.S. Special Operations Community, have operated for years against terrorist and insurgent networks. Counterterrorist and counterinsurgent operations have become an enormously demanding mission area for these forces. Some of the terrorists and Insurgents we have combatted also conduct criminal activities, ranging from kidnapping, to extortion, to drug smuggling, and beyond. These criminal activities must be addressed, in addition to their terrorist and insurgent behavior.

After 11 years of such activity, there is still much to learn about terrorist and insurgent networks and their criminal activities. I understand them far more than I once did, but it is important to acknowledge that my learning and understanding, even after so many deployments and missions, is still very incomplete.

This is important because we cannot simply assume that all we need to do is transplant how we fight terrorist/insurgent networks into how we fight transnational criminal organizations. That is a dangerous trap. To attempt to do so would be simple, easy-to-understand, attractive, and probably badly incomplete and misleading. While there are certainly some aspects of what we have learned about fighting networks that is transferrable from the counterterrorism and/or counterinsurgency realms, it is equally certain that a great deal is not.

Crime is a permanent facet of human societies. One cannot exist without the other. As societies across the globe have become increasingly inter-linked and inter-dependent, it logically follows that crime would therefore follow-suit thus becoming transnational in ways that now concern us. Therefore, gaining the understanding that is required must therefore begin with understanding how our societies are changing and interacting with others.

It is probably now simpler to list what is **not** changing in the ways these societies interrelate than to list what is. Trade, monetary flow, urban sprawl irrespective of borders, legal and illegal immigration, and cyber connections, among many others, are changing at dizzying speeds and in highly complex ways. All of these trajectories, all of these changes, and the first, second, third, etc., order impacts each change and trajectory has on all the others, create a web of changing realities that constitute today's world. Within this almost incomprehensible maze of change lies the opportunities and vulnerabilities within which an increasingly interconnected array of criminal actors ply their trade.

While reading the thoughtful presentations, arguments, and narratives in this volume, I offer the foregoing as a reminder: first, we must understand, and not just the criminal, but also the rapidly changing environment within which he operates. To act before we understand is more likely to be folly than wisdom.

For myself, as a military officer, I freely acknowledge that I do not yet understand.

## Executive Summary

Dr. Hriar Cabayan

[Hriar.Cabayan@osd.mil](mailto:Hriar.Cabayan@osd.mil)

Office of the Secretary of Defense

Significant transnational criminal organizations constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and I hereby declare a national emergency to deal with that threat...Criminal networks are not only expanding their operations, but they are also diversifying their activities, resulting in a convergence of transnational threats that has evolved to become more complex, volatile, and destabilizing.

President Barack Obama

The 2011 White House Strategy to Combat Transnational Organized Crime defines TCOs as “self-perpetuating associations who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.”

Transnational organized crime and transnational criminal organizations refer to a network or networks structured to conduct illicit activities across international boundaries in order to obtain financial or material benefit. Transnational organized crime harms citizen safety, subverts government institutions, and can destabilize nations.

Department of Defense Counternarcotics and Global Threats  
Strategy, 27 Apr 11

Transnational organized crime is an abiding threat to U.S. economic and national security interests, and we are concerned about how it might evolve in the future. We are aware of the potential for criminal service providers to play an important role in proliferating nuclear-applicable materials and facilitating terrorism.

Director of National Intelligence James R. Clapper

Five key threats to U.S. National Security: (1) Transnational Organized Crime (TOC) Penetration of State Institutions; (2) TOC Threat to the U.S. and World Economy; (3) Growing Cybercrime Threat; (4) Threatening Crime-Terror Nexus; and (5) Expansion of Drug Trafficking (Mexican drug trafficking organizations continue to expand their reach into the United States.)

National Intelligence Council

Transnational organized crime represents a significant, multilayered, and asymmetric threat to our national security...It is not viable for DoD to continue to examine this complex threat through the lens of the drug trade.

Department of Defense Counternarcotics and Global Threats  
Strategy

...what we've had to do in response is we have become a network. To defeat a network, we've had to become a network...

General Martin Dempsey, Chairman of the Joint Chiefs of Staff, in an interview with NBC's Ted Koppel on January 24<sup>th</sup>, 2013

...to defeat a networked enemy we had to become a network ourselves. We had to figure out a way to retain our traditional capabilities of professionalism, technology, and, when needed, overwhelming force, while achieving levels of knowledge, speed, precision, and unity of effort that only a network could provide...

General Stanley McChrystal, March/April 2011 edition of  
*Foreign Policy*

The continually evolving strategic environment coupled with the ascendant role of Transnational Criminal Organizations (TCOs) necessitates a comprehensive understanding of these organizations. TCOs represent a globally-networked national security threat and pose a real and present risk to the safety and security of Americans and our partners across the globe. This challenge blurs the line among US institutions and far surpasses the ability of any one agency or nation to confront it. Thus countering TCOs necessitates a whole-of-government approach and beyond that vibrant relationships with partner nations based on trust. These are essential if the U.S. is to remain the partner of choice, and effectively counter TCOs globally. Weak and unstable government institutions coupled with scarce legitimate economic opportunities, extreme socio-economic inequities, and permissive corrupt environments are key enablers that allow TCOs to operate with impunity. These same factors enable the emergence of VEOs. The potential nexus between VEOs and TCOs remains an area of deep concern. In this context, deeper insight into the contemporary face of TCO's will facilitate the development of strategies to counter and defeat them. In this struggle, DoD lacks law enforcement authorities but brings to the government some unique capabilities. This white volume examines the "new" face of these transnational crime organizations and provides a geopolitical perspective and implications to U.S. national security. The nexus of culture and technology (including modern communication technologies) and their impact on the evolution of TCOs is discussed in addition to their implications to countering TCOs.

## Key Insights

- Nature of Transnational Crime Organizations (TCO) threat
  - Transnational Criminal Organizations (TCOs) represent a globally-networked national security threat and pose a real and present risk to the safety and security of Americans and our partners across the globe.
    - The struggle against TCOs is a long-term proposition, requiring continuous effort, creative solutions, and the assumption of some risk
    - This challenge blurs the line among US institutions and far surpasses the ability of any one agency or nation to confront it
  - The specific threats vary by region and sub-region
    - Many regions are plagued by a drug arm that is vibrant, expanding, and has both a solid supply and demand base
    - In many instances, criminal groups seem to be evolving towards a business model based on loose associations of individuals or small groups operating independently
  - Successful TCOs appear to adapt their operations to local conditions and geography
    - They utilize local resources and capabilities, outsource and enter alliances to further their interests, and rely on both local and global ethnic communities to network and operate
    - The connection of a TCO with a legal business operation lends an element of legitimacy to the group's other activities
    - They operate legitimate businesses as front companies to help launder money associated with illegitimate activities
    - Members and senior leaders, may participate in public or private political, charitable or social events attended by highly placed political, business, and community leaders
    - They exploit legitimate commerce and, in some cases, create parallel markets
- Key enablers that allow TCOs to operate with impunity
  - Weak and unstable government institutions that have limited reach and presence into the furthest corners of society
  - Scarce legitimate economic opportunities that entice citizens to cooperate with TCOs for security and economic well-being
  - Extreme socio-economic inequities that open some geopolitical regions to a much greater risk of criminal or ideological manipulation and growth than others
  - Permissive environments, loose financial controls, widespread corruption and fraudulent document facilitation networks
  - Extreme interconnectedness and gaps in socio-economic and political equity creating an overall environment favorable to the formation and continued growth of TCOs
  - Globalization via Information and Communications Technologies (ICT) transforming and increasingly hyper-connected markets and economies blur boundaries and even authority across socio-political processes and State control
  - Recent analytical work based on empirical data indicates however that a large percentage of the countries where convergence between TCOs and VEOs is prominent are among the richest in the world. One reason maybe in the distinction between “means and ends “whereby criminals and terrorists converge in the denial of governance

- Bottom line: The ability of TCOs to use violence or threat of violence to achieve their aims renders no one immune irrespective of governance because all systems are vulnerable from a micro or individual level
- Nexus of TCOs and Terrorist Organizations
  - In many war zones and in ungoverned spaces across the globe, criminal and terrorist groups have formed once-improbable relationships, finding new ways to collaborate with each other
    - Environments most conducive to the formation and support of TCOs possess the same characteristics as those favorable to VEOs
    - Organized crime not only sustains insurgencies from a financial standpoint, it also supports their asymmetric warfare campaigns
    - This VEO/TCO convergence can be tremendously corrosive and also self-reinforcing
    - On the other side of the coin, an insurgency can lose both its standing with the population and its internal sense of political identity as a result of criminalization. This can be exploited in a counterinsurgency campaign
  - However not in all instances is there such a proven nexus and in many instances, the degree of overlap is difficult to determine
  - Recent analytical work based on empirical data indicates that interconnectivity is greater than one might have predicted
  - Hybrid organizations (those that include both political extremist and criminal elements) are more of a threat across threat domains (RN smuggling, RN smuggling with extremist organization involvement, nexus formation, and instability threat) than are the more purely criminal organizations
- Top level considerations to Countering and Defeating TCOs
  - Countering TCOs is defined as the means to detect, counter, contain, disrupt, deter, or dismantle the transnational activities of state and non-state adversaries threatening U.S. and partner nation national security. This will require the following
    - Dismantling their networks across the globe and driving down their impacts to levels that can be handled by local law enforcement organizations
    - Fostering a transnational, cross-organizational response and development of strategic security partnerships
    - Coordinating intelligence and law enforcement actions between organizations and sharing data from a variety of organizations across the globe to identify criminal networks and activities
    - Developing a comprehensive Counter Threat Network approach, whole-of-government, whole-of-societies collaboration, and possibly even new structures
    - Deploying teams of globally focused financial and fraud investigators to follow the illicit money supporting TCO and insurgent networks
    - Recent analytical work based on empirical data suggests that it is difficult to disrupt the activities of the global network by targeting a few kingpins and that the most effective means of countering such a global illicit network should involve a mixture of tools used to counter criminal activity in conjunction with those used to counter terrorism

- Whole-of-Government Approach
  - CTCO activities are primarily interagency in nature, with many authorities, capabilities, and capacities beyond the scope of DOD requiring a whole-of-government approach
  - Taking the whole of government approach in support of law enforcement agencies has helped build a cooperative partnership of networks to counter transnational organized crime
  - Need to develop a doctrine for stabilizing territories plagued by the crime-terror nexus and putting a focus on de-conflicting the work of disparate U.S. agencies, and crafting holistic strategy
  - Need to create trans-agency teams that would integrate military forces, diplomats, reconstruction and development specialists and legal experts tasked with reestablishing the authority, legitimacy, and effectiveness of the state in a target zone
  - However barriers remain to achieving a universal realization of TCOs as a true threat to homeland security
    - Sometimes interagency legal wrangling, sensitivities, parochialism, diminishing resources, and old-fashioned bureaucracy stymie U.S. responses
- Specific DOD Role
  - DOD lacks law enforcement authorities but brings to the government unique capabilities
    - Comprehensive, disciplined, and finely developed capacity to develop complex strategic plans
    - Global reach as well as unique and substantial resources
    - Collaborative partner capacity building
    - Certain counternarcotics authorities to assist law enforcement agencies
    - Capability to detect and monitor illicit trafficking and disrupt the illegal flow of precursor chemicals
    - Intelligence analysis and information sharing
  - There is however a lack specific knowledge of those capabilities and the processes to use to obtain them within the interagency
  - Improvements in key areas are identified:
    - Training programs to educate DoD analysts and planners on how organized criminal groups operate and how law enforcement and other governmental groups counter organized crime
    - Assigning more representatives from U.S. government agencies and organizations involved in combating organized crime to DoD organizations to facilitate the employment of DoD resources
    - Reviewing and streamlining authorities pertaining to DoD's support to law enforcement as well as regulations regarding the sharing of intelligence information
- Role of Partner Nations
  - Building the capacity of our partners to exercise their territorial sovereignty is crucial

- Vibrant relationships based on trust are essential if the U.S. is to remain the partner of choice, and effectively counter TCOs globally
  - Role of Strategic Communication in CTCO
    - Strategic communication should rise to the level of main focus in many instances, rather than as a supporting effort with unachieved potential
- The nexus of Culture and Technology in the evolution of TCOs and Implications to Countering CTO Strategies: An evolutionary biological perspective
  - The socio-technical nature of globalization is no longer treatable as separate elements
    - Current and future TCOs will be geographically and culturally dispersed
    - They will exhibit different socio-political tendencies and values
    - Evolve different socio-technical infrastructures to support and protect their activities
    - Mutate in response to environmental pressures ranging from market opportunities to government stability and even emergence of other criminal or VEO groups
    - Multiple and repeated interactions between system entities and individuals generate macro-level characteristics and dynamic patterns not found at the micro-level
    - Operate as fully developed platforms for innovation that compete violently with each other and provide deviant entrepreneurs key advantages
    - Result is a strategic environment where disruptive ideas rapidly become products or processes that are tested in the real world very fast, and success is easily imitated and iteratively improved
  - Modern communication technologies together with the explosion of electronically available information have
    - Hyper-connected markets and societies across the globe;
    - Enabled expansion of TCOs into emerging markets; and
    - Allowed TCOs to rapidly recruit expertise and employ various skills on a temporary or transient basis without the need to formally augment their enterprise. (Similarly, VEOs may recruit and sway sympathetic individuals without relying on old methods of radicalization or complete indoctrination to the cause).
    - Technological breakthroughs and their impact
      - Advances in additive manufacturing, online anonymity and anonymizable currencies, communication technologies amongst others between them, have the potential to change the contours of the landscape entirely
      - They increase the potential for violent upheaval and instability because they empower greater numbers of individuals
    - Make it much more difficult for law enforcement to monitor and/or trace communications and financial flows among nodes in the networks
  - Implications to Countering TCOs
    - Deviant innovators have one essential business requirement: to be one step ahead of the governmental deployment of interdiction technologies to remain a profitable operation while being ready to hack new inventions as soon as they are deployed

- This necessitates Governments respond accordingly
  - Constantly play the role of TCOs, penetrating governmental technologies
  - Policies should be designed in a way that whenever the environment changes, the shape of the governmental response can change with it
  - Think at the scale of big technology trends, devaluing the importance of any individual adaptation in any threat assessment
  - Cyberspace offers a solution in terms of collaboration environment providing CTCO groups a data ecosystem that is fluid enough to let organizations innovate from the bottom up, in response to local conditions and on the other hand balances security vs. access and provides scaffolding for an entire range of cyber-enhanced capabilities. This three-element structure allows coordination and collaboration in local spaces, as well as global data sharing
  - A better fundamental characterization of the cyber-socio-technical nexus can help form cogent U.S. defense-related policies and guidance for operational context

## Topic Overviews

Below are brief overviews of contributed articles. The contributions from six Geographical Commands offer their unique perspectives in reflecting upon conditions in their respective Commands are grouped in Chapter 1. Chapter 2 is an assessment by an IDA Team of Interagency Cooperation on Major Multijurisdictional Operations. Chapters 3 through 8 assess various aspects of networking between TCOs with terrorist organizations and other geographical based groupings. Chapters 9 through 12 assess the implications of the nexus between culture and technology to the future evolution of TCOs.

## Chapter 1

Dave Hulse et al (USSOCOM/Deputy J36 (Transnational Threats)) in a paper entitled “DOD Role in Combating Transnational Criminal Organizations (CTCO)” defines CTCO as “the means to detect, counter, contain, disrupt, deter, or dismantle the transnational activities of state and non-state adversaries threatening U.S. national security.” He observes in the 21<sup>st</sup> century era of globalization and irregular warfare (IW), the challenge of countering the financial and economic depth of our adversaries in conflict has become remarkably complex. In this vein, he makes two key points:

1. **All** terrorist organizations are Transnational Criminal Organizations; and
2. If you disrupt the money, you destroy the adversary.

He stresses that CTCO activities are primarily interagency in nature, with many authorities, capabilities, and capacities beyond the scope of DOD requiring a whole-of-government approach. He points out that despite the long history of finance and warfare being intermeshed, DOD largely has failed to recognize how money both supports conflict and can be used as a fulcrum in countering traditional or irregular threats. He goes on to state that in the 21<sup>st</sup> century, this doctrinal deficit has become increasingly problematic. He describe the role the DOD plays and states that among the most powerful capabilities DOD brings to the government is a comprehensive, disciplined, and finely developed capacity to develop

complex strategic plans. He advances a basic roadmap for DOD to be a major support element to the interagency community in combating the financing of state and non-state adversaries. He concludes with a quote by Lt. Gen. Fridovich "Success in this arena is, by its nature, not always conspicuous."

Col Glen Butler (Deputy Chief of Staff, Communication Synchronization, NORAD & USNORTHCOM) in a paper entitled "Combating Transnational Criminal Organizations in the Western Hemisphere: It, Too, Takes a Network" makes the case that Transnational Criminal Organizations (TCOs) pose a real and present risk to the safety and security of Americans, North American partners, and across the Western Hemisphere. Also, despite the increased focus on TCOs, the threat they pose has matured into a different and more dangerous enemy than yesteryear's cartels of the so-called "drug war." He quotes experts, who state:

Criminal networks transcend physical, geographic, and societal borders into the worlds of government, business, and finance. The criminal networks' ability to freely operate in the legitimate society increases the likelihood of their survival despite the best efforts of law enforcement.

As such, TCOs represent a globally networked national security threat and the struggle against them is a long-term proposition, requiring continuous effort, creative solutions, and the assumption of some risk. He alludes to the increasing possibility for a cartel-terrorist/violent extremist organization nexus even though that such a likelihood is low at the present time. He makes the case for an "Attack the Network (AtN)" or "Counter Threat Networks (CTN)" approach in addition to treating TCOs as a crime problem within the U.S. law enforcement agencies. Moreover, he emphasizes that defeating TCOs means dismantling their networks across the globe and driving down their impacts to levels that can be handled by local law enforcement organizations. No matter how difficult the process, embracing the network approach to combat the dangerous networks of TCOs will be key to collective success.

Mitigating the threat will also require continued development of strategic security partnerships between those invested in the fight against TCOs and other threat networks. He emphasizes the importance of cooperative defense and continental security including the economic aspects. Vibrant relationships based on trust are essential if the U.S. is to remain the partner of choice, not to mention effectively counter TCOs in the hemisphere. Homeland security is a shared responsibility built upon a foundation of partnerships. Yet, despite the danger TCOs pose to the U.S., our allies, and our partners, and despite recent improvements in synchronized planning and coordinated operations to counter this growing menace, barriers remain to achieving a universal realization of TCOs as a true threat to homeland security. There are fundamental challenges to efforts to counter the growing crisis stemming from the shared history of the U.S. and Mexico, which have prevented both nations from working together as effectively as possible in years past to achieve sufficient success. Even so, the last several years have seen historic warming and maturation of the relationship towards a real regional, strategic security partnership.

Finally, despite U.S. desire to be the "partner of choice" for international friends within the region, sometimes interagency legal wrangling, sensitivities, parochialism, diminishing resources, and old-

fashioned bureaucracy stymie U.S. responses to requests for assistance from others. He makes the strong case that ultimately what is required is a paradigm shift similar to that in scope and nature after 9/11. There are ways for such as change to begin, for example, escaping from the post-Cold War/pre-9/11 denial stage of this asymmetric conflict. Planners and strategists should strive to develop strategies that are comprehensive, whole-of-nation solutions. TOC will not be solved by counterdrug metrics alone. Strategic communication should rise to the level of main focus in many instances, rather than as a supporting effort with unachieved potential. Homeland security must remain a top priority. TCOs are intertwined in regional concerns that directly impact the homeland. Finally, the way ahead cannot be simply more of the same. Effective efforts against TCOs must include a comprehensive Counter Threat Network approach, whole-of-government and whole-of-societies collaboration, and possibly even new structures (e.g., the often debated "Joint Interagency Task Force, North" (JIATF-N)) and agreements (e.g., the Mexican-led "Hemispheric Scheme Against TOC"/Chapultepec Consensus). Step one is to honestly recognize these TCOs as the threat to homeland security they truly are. Step two is accepting that to defeat these networks, we'll need to become a better network ourselves.

Task Force members David Hallstrom, Tom Wood, and Chris Isham (JIATF West, USPACOM) collaborate in a paper entitled "USPACOM Perspective on Transnational Organized Crime". The paper starts off by stating the U.S. Pacific Command (USPACOM) Area of Responsibility (AOR) is a very diverse region comprising 50 percent of the world's population. In this vast region of the globe, as in other regions, transnational non-state threats are very diverse and involved in a wide array of criminal enterprises. They go on to state that permissive environments, loose financial controls, widespread corruption and fraudulent document facilitation networks fostered by Transnational Organized Crime (TOC) are key enablers for the freedom of movement of international terrorist and criminal organizations operating throughout the region. While TCO's pose broad challenges to nation-state power and interests across the region, the specific issues vary somewhat by sub-region and provides an assessment for each such sub-region. They point out that generally, there is not a proven nexus between organized crime and terrorism in the region and criminal groups seem to be evolving towards a business model based on loose associations of individuals or small groups operating independently. In this region, the drug arm of transnational crime is vibrant, expanding, and has both a solid supply and demand base. They provide examples of the international scope of these activities. They conclude by stating that while DOD lacks law enforcement authorities to counter TOC, it does possess certain counternarcotics authorities to assist law enforcement agencies in the fight. The Joint Interagency Task Force West (JIATF West) uses those authorities to apply DOD capabilities in a whole of government approach to combat transnational crime. Taking the whole of government approach in support of law enforcement agencies has helped build a cooperative partnership of networks to counter transnational organized crime.

In an article entitled "Transnational Organized Crime: A US SOUTHCOM Perspective", Ms. Renee Novakoff et al (USSOUTHCOM) states transnational organized crime is a global threat and a direct threat to western hemispheric stability and therefore a threat to US national security interests. Building the capacity of our partners to exercise their territorial sovereignty is crucial. Weak government institutions have limited reach into the furthest corners of society allowing transnational criminal organizations to operate with impunity. Besides, weak government presence and scarce legitimate economic

opportunities entice citizens to cooperate with TCOs for security and economic well-being. These borderless groups infiltrate government institutions to create, for themselves, space from which to carry out illicit activities. She provides several examples of such activities. She points out the potential exists for cooperation between TCOs and terrorist groups but the degree of overlap is difficult to determine. She states this challenge blurs the line among US institutions and far surpasses the ability of any one agency or nation to confront it. She goes on to say that key to mitigating transnational crime in this hemisphere, the US needs to help improve Latin American and Caribbean domestic institutions. Fundamental to this is understanding their associated networks and/or supply chains and in this vein, information sharing in the US and among its partner nations is crucial. DoD has an important supporting role in this effort to the interagency. For example, it is lead in detection and monitoring of illicit trafficking and also offers significant advantage in terms of Building Partner capacity and network analysis. She goes on to list several supporting lines of effort and emphasizes one of the continuing and important roles of the U.S. military is intelligence analysis and information sharing throughout the region.

In an article entitled "Stronger Together: Building EUCOM's Network to Combat Organized Crime in Europe", BG Mark Scraba & Mr Todd Trumpold (Joint Inter-Agency Counter Trafficking Center, USEUCOM) point out that since the early 1990s globalization has turned the region into a critical "turf" for some of the world's most powerful organized criminal organizations. The growth has been fueled by Europe's role as a central hub in the global economy. The magnitude of these illicit revenues results in organized crime's ability to control substantial sums of money and promote corruption, which can destabilize governments and undermine the rule of law. To address these threats, EUCOM established the Joint Interagency Counter-Trafficking Center (JICTC) in September 2011 to focus on three key areas:

- 1- The impact of organized crime on state security in Eurasia;
- 2- Military-civilian collaboration; and
- 3- Developing the necessary tools, practices, and authorities.

They point out that the scope and magnitude of the threat demands a transnational, cross-organizational response. Data from a variety of organizations across the globe must be shared to identify criminal networks and activities. Moreover, intelligence and law enforcement actions must be coordinated between organizations. DOD should be a key contributor to this whole-of-government response, given its global reach, as well as its unique and substantial resources. The challenge remains how best to integrate it. They point out that despite consensus on the need for cooperation, U.S. military collaboration on issues pertaining to organized crime is challenging in EUCOM's AOR. The JICTC's ability to assist law enforcement varies greatly and is influenced by a wide range of factors, such as partner nation laws, capabilities, willingness to combat organized crime, corruption, and political relations with the U.S. For these reasons, the JICTC operates almost exclusively in partnership with other U.S. government agencies and organizations. In its first two years of operations, the JICTC has had success in two broad areas of activities: 1) Collaborative partner capacity building efforts; and 2) Analytical support to U.S. law enforcement investigations and administrative actions. JICTC's analytical products are narrowly tailored to meet the ongoing efforts of other U.S. government organizations. America's War on Drugs, and more recently the War on Terror, have gone a long way to prepare DOD

for a larger role in supporting efforts to counter organized crime, but improvements in at least three key areas are needed for DOD, listed below.

1. Training programs should be developed to educate DOD analysts and planners on how organized criminal groups operate and how law enforcement and other governmental groups counter organized crime.
2. More representatives from U.S. government agencies and organizations involved in combating organized crime should be assigned to DOD organizations, such as the JICTC, to facilitate the employment of DOD resources.
3. Authorities pertaining to DOD's support to law enforcement as well as regulations regarding the sharing of intelligence information should be reviewed and streamlined.

They conclude by observing that if DOD is to support the CTCO mission, it should have express authorities to do so. Through the creation of the JICTC, EUCOM has taken a critical first step in supporting interagency efforts to combat organized crime in. Although the nature and gravity of the threat is broadly recognized, key enablers are not yet in place to optimize DOD support. Measures should be taken to facilitate counter-TCO efforts at the Combatant Commands, such as the development of training programs, streamlining of authorities and strengthening of working relationships with U.S. agencies and organizations who are leading the fight against TCOs.

## Chapter 2

In an article entitled "Interagency Cooperation on Major Multijurisdictional Operations", co-authors from Institute of Defense Analysis (Lauren Burns, Joseph Keefe, James Kurtz, Col Tracy King, William Simpkins, and Christopher Ploszaj) discuss a study conducted by the Joint Advanced Warfighting Program at the Institute for Defense Analyses, under the sponsorship of the Joint Staff Directorate for Joint Force Development (J-7), that was focused on lessons learned from 22 multijurisdictional, interagency operations that took place in the USNORTHOM area of responsibility between 1996 and 2011. These operations were directed against the command-and-control and the financial networks of Mexican TCOs, and were arguably the largest of their kind conducted by the US Government against Mexican TCOs. The study provided USNORTHCOM with insights into long-standing mechanisms for interagency coordination as well as into previous efforts to counter Mexican TCOs. This was part of a larger effort The Department of Defense (DoD) directed the combatant commands to establish a dedicated counter threat finance (CTF) capability that would integrate intelligence and operations, analyze financial intelligence, and coordinate the execution of DoD CTF activities in accordance with existing authorities, regulations, and combatant command initiatives. The Drug Enforcement Administration (DEA)–Special Operations Division (SOD) coordinated each of the operations. To identify the lessons learned, the IDA study team conducted a series of structured interviews with SOD's lead Staff Coordinators responsible for coordinating each of the 22 operations. The study team developed a set of 16 questions that the study team used to conduct structured, not-for-attribution interviews with each lead Staff Coordinator. The questions focused on lines of inquiry that would help identify the most important lessons learned. The IDA team summarizes lessons learned from the interviews in several categories: DOD Capabilities, Money Movement, Role and Importance of Coordination Meetings,

Foreign Involvement, and finally Technology and Adaptation. Following key observations are highlighted, listed below.

- DOD has capabilities to support law enforcement efforts; however, there is a lack specific knowledge of those capabilities and the processes to use to obtain them.
- DOD support in disrupting the illegal flow of precursor chemicals
- DOD support for agile means to recognize how the TCOs are implementing and using evolving technologies to protect and facilitate their command-and-control and financial operations

### Chapter 3

In an article entitled “The Intersection of Crime and Conflict”, Ms. Gretchen Peters (Author of Seeds of Terror / Affiliate Instructor at the Terrorism, Transnational Crime and Corruption Center (TRACCC) at George Mason University / Lead Associate at Booz Allen Hamilton supporting the DASD-CN/GT) focuses her attention on three interrelated areas; namely insurgency and crime; TCOs and conflict zones; and finally the need of reshaping intelligence and forging more effective, holistic U.S. interventions in conflict zones. She states that rebellions have a strong tendency to become involved in black and grey market activity because they cannot openly fund-raise nor participate in the state-regulated licit economy. Organized crime not only sustains insurgencies from a financial standpoint, it also supports their asymmetric warfare campaign. Most importantly, involvement in smuggling brings insurgents into contact with transnational crime organizations (TCOs). Illicit profits generate collective action logic to sustain war and instability, and a concrete financial incentive to spoil any peace process. On the other side of the coin, an insurgency can lose both its standing with the population and its internal sense of political identity as a result of criminalization. In other words, a highly criminalized insurgency faces strategic vulnerabilities, which could be exploited in a counterinsurgency campaign that protects the populace and attacks the rebels using tactics that are typically applied against organized crime networks. Conflict zones are also attractive to TCOs, which gain comparative advantage from doing business in unstable, chaotic environments. This VEO/TCO convergence is tremendously corrosive and also self-reinforcing; in other words, it gets harder to pull a country or region out of the downward cycle once it begins. Not only is corruption difficult to fight, but distortions to the economy and financial system caused by organized crime make it complex. As military strategists prepare for a world where so-called irregular warfare will in fact become the norm, she advances key enablers:

1. Framework for collecting, analyzing and utilizing economic data;
2. Teams of globally focused financial and fraud investigators to follow the illicit money supporting TCO and insurgent networks; and
3. Doctrine for stabilizing territories plagued by the crime-terror nexus and putting a focus on de-conflicting the work of disparate U.S. agencies, and crafting holistic strategy.

She advocates the creation of trans-agency teams that would integrate military forces, diplomats, reconstruction and development specialists and legal experts tasked with reestablishing the authority, legitimacy, and effectiveness of the state in a target zone.

## Chapter 4

In an article entitled “The Connected Illicit System: A Glimpse at the Illicit Superhighway”, Dr. Scott Helfstein (CTC/West Point) assesses the convergence between criminal and terrorist elements. He uses a unique dataset that provides an empirical assessment of global connectedness with primary focus on how often terrorists enter the transnational criminal network and in what types of numbers. Rather than solely focusing on activities and organizations, the network is built by mapping individuals and their relationships to others to assess the global interconnectivity between terrorists and criminals. The empirical analysis of almost three thousand individuals operating across one hundred and twenty countries is built on open source reporting and court records in over sixty languages gathered for financial compliance. The “static” structural analysis suggests following observations.

1. Interconnectivity is greater than one might have predicted and contrary to conventional belief. The structural analysis suggests that terrorists are likely to act as brokers linking unconnected groups and the visual evidence suggests that terrorists are distributed throughout the network. This challenges the idea that others in the illicit world eschew terrorists because of their stigma or the related security concerns. Rather, the analytics suggest that terrorists actually play a reasonably important role linking disparate cells and groups to one another.
2. The distribution of relationships is such that it is difficult to disrupt the activities of the global network by targeting a few kingpins. Such a strategy would work if there were a few hyper-connected individuals, but the relative shortage of these super-connectors means that the network is likely to withstand their removal.
3. The network analytics suggests that terrorists are no more or less operationally secure than other criminal enterprises. They are deeply imbedded in the larger criminal network, they span boundaries to link otherwise separate clusters or organizations, and they are relatively close to others in the network. These results might be interpreted to suggest that the most effective means of countering such a global illicit network involves a mixture of tools used to counter criminal activity in conjunction with those used to counter terrorism.
4. A large percentage of the countries where convergence is prominent are among the richest in the world suggesting that that conventional wisdom about crime-terror convergence may be incomplete. The article suggests that one reason lies in the distinction between “means and ends.” The economic ends of organized criminals are different than the political ends of the terrorists. This distinction according to ends may have masked a convergence in means that is increasingly prominent. While criminal elements seek economic profit, they usually require some sort of sanctuary to safely pursue and accrue the rewards. It is in this denial of governance where criminals and terrorists converge. It is in the final step that terrorists are substantively different than most criminals, where the later has no interest in governing. It is in this intermediate step, denying governance or achieving negative political control that terrorists and criminals are most likely to converge and work together despite different ends.

## Chapter 5

In an article entitled "Analyzing and Evaluating Criminal Organizations," Dr. Daniel Mabry and Dr. Richard Ward (University of New Haven) state that the Institute for the Study of Violent Groups (ISVG) has been researching terrorism, extremism, and transnational crime for more than 10 years and has compiled a comprehensive unclassified database of these groups and their activities. The database has more than 250,000 events since 2002 perpetrated by more than 4,000 organizations and more than 50,000 individuals. Through this database of networks and actors, ISVG has been able to develop an inductive understanding of criminal organizations globally and how they are associated with terrorist and extremist organizations. In assessing criminal organizations worldwide, ISVG developed a criminal organization hierarchy that seems consistent across countries and over time. They go on to discuss issues related to assessing and evaluating criminal organizations and conclude with a discussion of an approach developed by ISVG. They state that the approach they describe does not aim to replace or supersede other analytical approaches to understand criminal network structures, but should complement these analyses with a systematic, structured understanding of criminal organizations. As an example, they provide an example of how from 2008-2012 ISVG performed order of battle analyses on transnational criminal organizations operating along the US-Mexico border. For the article, selected portions of the Los Zetas order of battle from December 2011 are presented to illustrate the modified approach. These include discussions of Areas of Operation; Background discussions; Innovations and evolutions of the Group; Links to other Organizations; Corruption; Membership; Tactics and Operations; Training; Weapons and Ammunitions; Funding/Money Laundering; and finally Effectiveness. They conclude by stating that the transnational organized crime order of battle analysis provides a comprehensive framework for assessing and evaluating criminal organizations but it is not without its analytical challenges. A complete order of battle analysis needs to be performed at the regional and sub-regional levels according to how each criminal organization constitutes its operations. Another shortcoming is that it does not do a good job of tracking/visualizing the change or evolution of criminal organizations.

## Chapter 6

In an article entitled "The Contemporary Face of Transnational Criminal Organizations and the Threat They Pose to U.S. National Interests: A Global Perspective," Dr. Vesna Markovic (Assistant Professor Henry C. Lee College of Criminal Justice and Forensic Sciences, University of New Haven, West Haven, CT; and Program Manager, Institute for the Study of Violent Groups (ISVG)) highlights the fact that TCOs thrive in countries with a weak rule of law and present a great threat to regional security in many parts of the world. Bribery and corruption employed by these groups further serve to destabilize already weak governments. These TCOs also present a major threat to U.S. and world financial systems by exploiting legitimate commerce, and in some cases creating parallel markets. She points out that one of the most significant threats posed by contemporary TCOs is their alliances and willingness to work with terrorist and extremist organizations. In her paper, she focuses on contemporary TCOs by giving a brief overview of the most common criminal enterprises associated with these groups, such as drug trafficking, trafficking of small arms, smuggling and trafficking of human beings, product counterfeiting, and money laundering. She also discusses the nexus between various TCOs, the nexus between TCOs

and terrorist and extremist groups, case studies highlighting the nexus, and the threats they pose to U.S. national interests. She points out that these TCOs are willing to work with any group regardless of their affiliations or ideologies. She concludes by stating that in order to disrupt these networks it is important to cooperate on an international level. It is important to strengthen the skills and capacity of weaker governments in battling TCOs.

## Chapter 7

In an article entitled "The Threat of Pakistani Criminal Organizations: Assessing the Potential for Involvement in Radiological/Nuclear Smuggling, Collaboration with Terrorist Groups and the Potential to Destabilize the Pakistani State", co-authors from the Univ. of MD START Team (Amy Pate, Mila Johns, Gary Ackerman, and McKenzie O'Brien) describe and apply a methodology to assess risks posed by criminal organizations operating in Pakistan. The authors utilize openly available sources to identify significant criminal organizations. Searches were limited to criminal organizations active in the 2009-2012 time period and were conducted primarily in English, with supplemental searches in Urdu. The team identified 68 criminal organizations in Pakistan, of which 11 were selected to profile based on the size and scale of their operations and/or influence in specific criminal markets. The paper summarizes the results of their threat assessment, including rankings for risk of involvement in radiological/nuclear smuggling. The authors also perform social network analyses for each profiled criminal organization and its interactions with other actors in the Pakistani milieu, highlighting the existence and significance of linkages between important actors in the region. The conclusion highlights key findings, which indicate that hybrid organizations (those that include both political extremist and criminal elements) are more of a threat across threat domains (RN smuggling, RN smuggling with extremist organization involvement, nexus formation, and instability threat) than are the more purely criminal organizations.

## Chapter 8

In an article entitled "Networking and Legitimization of Transnational Crime Organizations," Dr. Mary Zalesny with the Chief of Staff of the Army Strategic Studies Group states that while traditionally considered a law enforcement issue, organized crime has developed into a powerful influence on the politics, economic viability, and governance of nation states. By virtue of their wealth, their ability to corrupt public officials at all levels, and their increasing control of legitimate markets, natural resources and key infrastructure, TCOs can distort global markets and threaten tightly linked economies. The scope and consequences of the threat posed by TCOs may eventually exceed the ability of law enforcement to contain or prevent it. Globalization, improved communication, and transportation technologies have benefitted both legal and illegal enterprises helping transnational organized crime become a potent financial and cultural force that undermines vulnerable state institutions and rule of law, and adversely affects millions of people. Furthermore, the recommendation to "think globally, act locally" appears to have been accepted by TCOs. Their reach, network, and the scope of their operations may be global, but they rely on networks at the local and regional level for much of their work. Successful TCOs appear to adapt their operations to local conditions and geography. Following that line of argument, her primary focus is on networks created by transnational crime organizations to operate in and move across primarily geographical borders. She summarizes the results of a recently conducted

study that investigated criminal group involvement with local populations along US borders and specifically the network dynamics in two US border areas. She relates how they utilize local resources and capabilities, outsource and enter alliances to further their interests, and rely on both local and global ethnic communities to network and operate. Like some political and business families, criminal groups develop relationships and marry strategically to gain entry into advantageous groups, networks, and locations they might otherwise not have access to. Friendship and marital connections can facilitate acceptance of an outsider to a group, provide legitimacy and cover, and provide information important to criminal operations and security. Networks are also increasingly used by transnational crime organizations over more traditional hierarchical structures as important organizing and operating platforms. Not all TCOs specialize solely in illicit activities. The connection of a TCO with a legal business operation lends an element of legitimacy to the group's other activities. Some TCOs operate legitimate businesses as front companies to help launder money associated with illegitimate activities. TCO members, especially senior leaders, may participate in public or private political, charitable or social events attended by highly placed political, business, and community leaders. Because TCOs and local organized crime groups (e.g., gangs) are already skilled at instituting their own rule of law in territories they control, urban warfare in megacities that may have a significant TCO presence will present a new adversary with its own set of tactics and rules of engagement.

## Chapter 9

In an article entitled "The symbiosis of technology and TCOs and what that entails for the future," Dr. Valerie B. Sitterle (GTRI) focuses on the convergence of technology with social processes and, notably, the influence technology may have on the future evolution of TCOs and their operations. She states at the outset that two factors - extreme interconnectedness and gaps in socio-economic and political equity - create an overall environment favorable to the formation and continued growth of Transnational Criminal Organizations (TCOs). The degree of societal "differentiation" is increasing as technologies permeate and empower individuals and small groups in new ways. Current and future TCOs will be geographically and culturally dispersed; they will exhibit different socio-political tendencies and values and, importantly, evolve different socio-technical infrastructures to support and protect their activities. She includes a discussion of socio-technical confluence and how TCOs employ technology, what this may mean for the future structural and dynamic nature of TCOs, and why this poses a great analytical challenge. In this context, she discusses three main themes: a description of the socio-technical confluence and how TCOs employ technology; what this may mean for the future structural and dynamic nature of TCOs; and why this poses a great analytical challenge.

She goes on to state that the socio-technical nature of globalization is no longer treatable as separate elements. This blended reality is now a part of our future and is dramatically affecting how we view the world as well as how we operate within it. To illustrate her argument, she focuses primarily on how advances in information and communications technologies (ICT) shape and mediate social dynamics. Modern communication technologies together with the explosion of electronically available information have hyper-connected markets and societies across the globe. TCOs use ICT either to facilitate their business operations or to expand into a cyber-criminal business space. Basing her arguments on biology inspired models, she states the link between macro- and micro-level behaviors that relates directly to

concepts of emergence, or system evolution. Multiple and repeated interactions between system entities and individuals generate macro-level characteristics and dynamic patterns not found at the micro-level, whereby a macro-scale system property is created as a consequence of repeated interactions among system entities at the micro-level. This translates to understanding TCO behavior and evolution as transnational enterprises. Similar to biological systems, specialization, and interconnectedness of many functional units and networks drive TCO behavior. Structurally speaking, TCOs evolve both structurally and dynamically. Traditionally styled TCOs are not designed from inception with a complex, highly networked, and layered transnational structure in mind. Instead, like biological organisms, they mutate in response to environmental pressures ranging from market opportunities to government stability and even emergence of other criminal or VEO groups. Adding to this complexity, TCOs not only react to their environment, they actively seek to redefine it in ways favorable to their activities.

The natural mutation of TCOs over time is further complicated by expansion into emerging markets made possible by ICT advances. For example, TCOs that exist solely to exploit the cyber realm do not tend to exhibit the same degree of structure and operational support as their more traditionally established counterparts. Additionally, environments most conducive to the formation and support of TCOs possess the same characteristics as those favorable to VEOs. Growing and persistent socio-political inequalities raise insurgent potential; globalization via ICT transformation and increasingly hyper-connected markets and economies blurs boundaries and even authority across socio-political processes and State control. She discusses challenges facing operationally relevant analytics such as data gathering as well as meaningful and effective synthesis of different dimensions of the problem within an operationally relevant analytical framework. She emphasizes the need for socio-technical perspective. For example, modern ICT capabilities allow TCOs to rapidly recruit expertise and employ various skills on a temporary or transient basis without the need to formally augment their enterprise. Similarly, VEOs may recruit and sway sympathetic individuals without relying on old methods of radicalization or complete indoctrination to the cause. Unstable governance structures and extreme socio-economic inequities open some geopolitical regions to a much greater risk of criminal or ideological manipulation and growth than others. She concludes by highlighting the need for a better fundamental characterization of the cyber-socio-technical nexus to help form cogent defense-related policies and guidance for operational context.

## Chapter 10

In an article entitled “The geopolitics of clandestine innovation in the drug business: A framework of analysis to understand adaptation capacities of TCOs”, Dr. Rodrigo Nieto-Gomez (NPS) advances the thesis that Transnational Criminal Organizations (TCOs) operate as fully developed platforms for innovation that compete violently with each other and provide deviant entrepreneurs key advantages. He illustrates this dynamic within the context of Mexico whereby Sinaloa initially provided the cluster of interconnected organizations, suppliers, and institutions to innovate and produce the sustainable smuggling market that TCOs run today. He posits, TCOs that operate without a central planning authority in Mexico innovate and compete to survive, remaining profitable in the context of a deadly, non-regulated, and highly competitive environment. The result is a strategic environment where

disruptive ideas rapidly become products or processes that are tested in the real world very fast, and success is easily imitated and iteratively improved. The path from clandestine innovation to deviant entrepreneurship is very short thanks to the removal of the key obstacles thus freeing the flow of information through this unobstructed pipeline. In addition, TCOs are innovation patterns in time. These networks manage complexity and environmental change with success through a constant innovation process that iteratively solves the challenge of “hacking” governmental technologies, institutions, and deployments.

Dr. Nieto-Gomez also introduces the concept of “stigmery” that are environmental stimuli that agents in a system perceive and evolve accordingly leaving in the process new signals for other agents to interpret, in a deadly iterative process. He postulates that this stimulus/response cycle is at the center of the development of innovation of technologies used by TCOs to hack governmental interdictions. He goes on to state that many of the failures in the current strategies to confront the threat of TCOs can be attributed to an important lack of systemic understanding of these innovation dynamics. Deviant innovators have one essential business requirement: to be one step ahead of the governmental deployment of interdiction technologies to remain a profitable operation while being ready to hack new inventions as soon as they are deployed. Once a deviant technology is proven by a deviant innovator, others deviant entrepreneurs will adopt what innovation literature calls an “early followers” approach. Because there are no patents or property rights limiting the use of clandestine technologies, successful hacks rapidly propagate throughout the system until, at one point, governmental technologies close the gap. Understanding the forces behind these innovations is essential to produce more effective strategies to counter the innovative capacities of TCOs.

He points out the main objective of security and defense policies to deal with the threat of TCOs should be to learn how to dismantle not a particular innovation or a particular subcontracting unit, but how to manage the wicked problem presented by the evolving and adapting innovation cycles. Governments should adapt a “contrarian technology perspective” in threat assessment processes when developing technologies to affect the geopolitical environment of deviant innovation. He argues in this respect, governmental developers must be allowed to constantly play the role of TCOs, penetrating governmental technologies. Furthermore governments should be “pivot friendly”; i.e. policies should be designed in a way that whenever the environment changes, the shape of the governmental response can change with it. This means that instead of thinking about one particular innovation that must be neutralized, it is important to think at the scale of big technology trends, devaluing the importance of any individual adaptation in any threat assessment. He advocates government strategies that do not just ask the question “will this particular response be hacked?” but instead, “what to do when this particular response is hacked?” In this way, decision makers can avoid the trap of concentrating too much in one particular strategy or technology program, and instead encourage a contrarian technology perspective that looks for the right points of intervention to limit the geopolitical availability of deviant innovation clusters, and also fragments the systemic effectiveness of the pipelines that provide the creative resilience to TCOs.

## Chapter 11

In an article entitled "Game-Changing Developments in the Proliferation of Small Arms and Light Weapons: Anonymizing Technologies and Additive Manufacturing", Dr. Regan Damron (USEUCOM) analyzes the contemporary tactics, techniques, and procedures (TT&Ps) associated with the manufacture and illicit distribution of Small Arms and Light Weapons (SALW) and how technological trends are likely to converge to augment and/or alter those practices. SALW draw his focus because in addition to proliferating more easily and more often than larger, more complex conventional weapons systems, they are especially nefarious in their potential to ignite, worsen, and prolong conflicts. Dr. Damron points out that currently, the illicit distribution of SALW is dominated by relatively few, large-scale traffickers; however, that may change because of developments on the technological front. The paper begins with an exposition of mature anonymizing technologies (online anonymity and anonymizable currencies) and then examines additive manufacturing (or "3D printing"). Between them, these technologies have the potential to change the contours of the landscape entirely. He states that these technologies increase the potential for violent upheaval and instability because they empower greater numbers of individuals to engage in the trafficking of small quantities of SALW as both consumers and suppliers-effectively democratizing access to weapons. And even as access is broadened and trafficking networks decentralize, the use of online anonymity in combination with anonymizable currencies makes it much more difficult for law enforcement to monitor and/or trace communications and financial flows among nodes in the networks. Looking deeper into the horizon, the maturation of desktop 3D printing (or "additive manufacturing") technology is likely to completely revolutionize both the manufacture and the trafficking of SALW. TCOs' near monopolies have allowed them to control the nearly 2 trillion dollar annualized trade in illicit goods, but additive manufacturing will eventually make those goods broadly available. Dr. Damron ends by raising some key questions. What happens to TCOs' business model when illicit goods are democratized? How will TCOs respond?

These are open questions whose answers will pose additional risks (and likely, opportunities).

## Chapter 12

In an article entitled "Turning Technology's Tables on Trafficking: Building an Anti-Human Trafficking (AHT) Data Ecosystem", Maj David Blair (USAF/PhD Candidate, Georgetown University) argues that Cyberspace is a key part of the business cycle of modern-day slavery. For traffickers, digital communications serve as key market enablers, yielding a massive implicit data aggregator, which transmits prices and best practices to each other. Simultaneously law enforcement and NGOs use the web to share data and collaborate. Traffickers have already targeted anti-trafficking websites. He goes on to argue that in order to counter this 'wicked problem,' state and Intergovernmental Organization (IGO) leadership needs to make cyberspace more secure for the anti-trafficking movement and far less secure for traffickers. In this context, the anti-human-trafficking (AHT) movement faces an endemic challenge in the inability to collaborate. His key point is that Cyberspace offers a solution - an online collaboration environment providing the movement both an Intranet and a Fusion Center, solving the coordination problem. He proposes a three tiered data ecosystem that is fluid enough to let organizations innovate from the bottom up, in response to local conditions and on the other hand

balances security versus access and provides scaffolding for an entire range of cyber-enhanced capabilities. This three-element structure allows coordination and collaboration in local spaces, as well as global data sharing.

## Introduction

Mr. Ben Riley, Principal Deputy, Rapid Fielding, OSD-AT&L/ASD (R&E)

[ben.riley@osd.mil](mailto:ben.riley@osd.mil)

Dr. Kathleen Kiernan, CEO, Kiernan Group Holdings

[kiernangroup1@comcast.net](mailto:kiernangroup1@comcast.net)

Today's threat networks have proven to be resilient, adaptive, interconnected, and agile. They have learned to operate flexibly, aggregating and disaggregating quickly in response to countermeasures, extending their reach in physical and virtual dimensions. They adapt technology in short cycles and rapidly evolve tactics, techniques, and procedures.

General Barbero, 2012-2016 JIEDDO C-IED Strategic Plan

Malcolm Gladwell described the aptitude of code breakers during the Second World War who could, with unassailable accuracy, identify the signal transmissions of the enemy without ever once hearing their physical voices or observing their behavior beyond the rhythm of their communications. This cadence was a convergence of speed, pattern, and personality, forming a signature unique to each individual transmitter. He called that union of factors a "fist" and the capability to identify the actions and intentions of the adversary in advance proved to be both a tactical and strategic advantage.

Although the application may be new, law enforcement officers have honed the skill of identifying anomalous behavior over time globally, long before the lexicon of "homeland security" entered American vernacular. These skills centered on the ability to identify activities associated with deception; concealment; manipulation, violence, and criminal behavior, including the aforementioned example. The developed ability to see what is hidden in plain sight, that which is invisible to the untrained eye, is a skill that is fundamental to officer safety regardless if the uniform worn is civilian or military. The skillset translates across culture, context, language, and rules of engagement. The "fist" of criminals in street parlance is articulated as "JDLR," that is, just does not look right. It is readily observable to the practiced eye with identifiable patterns and trends.

Forms of communication between and among criminal organizations ranges from rudimentary to technologically sophisticated. These systems, often, may be beyond the reach of the intelligence, law enforcement, or national security organizations designed to thwart them. If there is a common denominator, it is, in fact, the human sensor. It is this sensor that interprets the immense amount of data generated by novel technologies. For example, geospatial predictive analytics are able to, through layering numerous sources of data, identify areas that have a high likelihood of becoming a target, given previous targets. This technology allows users to make informed decisions of where to allocate limited resources. However, it is still the user who determines, of the high likelihood areas, which is *most* likely. It is this ability to forecast the actions of irrational individuals that makes human sensors irreplaceable. Geospatial predictive analytics and other technologies are imperfect, and will continue to be, due to their inability to get inside the mind of a criminal. Law enforcement, military, and intelligence officers are able to do this through years of earned experience. Deducing what behavior will be seen next, given what has been observed, is built upon previous experiences. This explains the chasm between an experienced officer trusting their gut instinct, sometimes unable to

articulate why, and a rookie's pedantic nature and inability to pick up on obvious criminal behavior cues. The aperture of an experienced officer is significantly wider than that of a rookie due to years of learning about human behavior. Illuminating the world of criminal activity cannot be automated.

The Army introduced the idea, "Every soldier is a sensor." This can be extrapolated across agencies and regions. DIA Director General Flynn has proposed restructuring the way intelligence is gathered to better reflect the way it is created. Rather than restrict data gathering by topic (i.e. weapons supply, trafficking) it should be collected in geographic regions. Analysts will go on site, interacting with information gatherers who know if something is JDLR. This is increasingly critical as the nexus of criminal and terrorist activity is more apparent, that is every terrorist is a criminal but not every criminal is a terrorist. Although the motivations may differ, profit versus ideology, each requires similar capabilities, to include weapons acquisition, fraudulent documents, illicit finance, and safe haven.

Transnational Criminal Organizations effect military operations and force protection through active manipulation of supply chains and systemic cooption and compromise of governing authorities through bribery, violent coercion, and illicit financial networks. These financial networks are interwoven and oft indistinguishable from legitimate commerce making them that much more difficult to identify and interdict. TCOs do not recognize geographic or jurisdictional borders nor delineated combatant command areas of responsibilities. Rather they rely upon the underground economy, which guarantees stability, anonymity, and long-term viability. This underground economy is based upon centuries old trade routes, originally designed to fuel economic progress however these routes also facilitated illicit trade and commerce. Over time, the commodities have changed but the rules of engagement are at times as ruthless and barbaric as the Han Dynasty.

The tension inherent in the persistent interaction of those who operate at the margins of civility and, simultaneously, the extremes of human behavior acts as a tuning mechanism for law enforcement and, increasingly, the military. These activities are educative and iterative. They educate on the constant evolution of TTP's from weapon concealment to, in many cases, the concealment of intent cloaked in legitimate business enterprises. They are iterative due to the adaptation cycle of the adversary unconstrained by law or ethics. Crime used to be personal in the sense it required proximity and access; that is no longer the case with the blurring of governance in the cyber realm nor the extended reach of transnational criminal organizations. Fists are no longer created by the speed and rhythm of messages but by IP addresses and social network analysis.

# Chapter 1 A: DOD Role in Combating Transnational Criminal Organizations

Mr. Dave Hulsey, et al

[david.hulsey@socom.mil](mailto:david.hulsey@socom.mil)

USSOCOM

## Introduction

In the words of the Roman statesman, Marcus Tullius Cicero, “Endless money forms the sinews of war.” Protecting or attacking such monetary sinews—including financial bases of support, means of sustainment, and lines of communication—has always played an important role in the history of warfare. Yet, in the 21st-century, an era of globalization and irregular warfare (IW), the challenge of countering the financial and economic depth of our adversaries in conflict has become remarkably complex.

Terrorists are Transnational Criminal Organizations (TCOs). Terrorists, insurgents, and weapons proliferators typically rely on irregular ways and means to fund their activities, including organized crime, donations from non-governmental organizations (NGOs), and clandestine financial support from hostile foreign governments. Sophisticated front companies—established by a criminal organization (or an adversary as part and parcel of an IW strategy)—are another important financial source, generating self-sustaining streams of revenue, laundering illicit money, and providing covert means to penetrate economies, states, and societies. Such legitimate looking companies can be used to cloak less sophisticated, large-scale means of transferring illicit funds, such as bulk cash shipment and trade-based money laundering.

One of the important lessons of the Iraq war experience is that combating insurgent funding streams and cover mechanisms is a key element in effective counter-insurgency strategy. In Afghanistan, a zone of conflict where narcotics income and foreign donations help define the operating environment, the urgency of countering insurgent financing is even greater, ranking among the Combatant Commander’s top priorities.

In Iraq and Afghanistan, The Department of Defense (DOD), Department of the Treasury (Treasury), and the Drug Enforcement Administration (DEA), in full partnership with interagency colleagues such as The Department of Homeland Security (DHS) and The Department of Justice (DOJ), have established Threat Finance Units (TFUs). These units—made up of qualified intelligence, law enforcement, policy, and military personnel—play an important role in identifying insurgent financiers, disrupting front companies, developing actionable financial intelligence, freezing and seizing illicit funds, and building criminal cases. These units operated under DOD-Treasury leadership in Iraq and under Treasury-DEA leadership in Afghanistan, and in both cases fully involve the interagency and report directly to the National Security Council (NSC) Terrorism Finance Working Group. This is a good model to follow in Counter Transnational Criminal Organizations (CTCO) operations.

DOD and its interagency partners recognize the key to success in countering threat financing is a whole-of-government approach. Furthermore, DOD capabilities and resources are but one element of the broader range of national powers. To better support evolving U.S. Government (USG) efforts globally, the Office of the Under Secretary of Defense for Policy (OUSD(P)) is working with Department and interagency counterparts to focus diplomatic outreach, coordinate bilateral and multilateral cooperation, and ensure effective analytic support. OUSD(P) has formulated revised DOD policy guidance on Counter Threat Finance (CTF) which will focus how DOD's TCO efforts—within an interagency framework—support overarching USG policies. If DOD implemented a CTCO initiative designed to bolster interagency CTCO capacity, The Department will further its TCO policy coordination with the interagency (under the NSC) and refine roles and missions for the Combatant Commands (CCMDs).

The purpose of this strategic vision is to emphasize the necessity of integrating DOD CTCO capabilities with, and in support of, the whole-of-government effort against illicit financial activity that threatens U.S. national security interests. This vision will also enhance the capacity of our warfighters on any 21<sup>st</sup> century asymmetrical battlefield. DOD recognizes this vision will be successful only through the full involvement and participation of its interagency counterparts during the planning and implementation stages of this effort. This document shows that implementing a CTCO initiative must be a near-term priority for DOD supporting and enhancing a whole-of-government approach to TCO, and will be resourced, directed, and coordinated from the top levels of policy, intelligence, and military leadership.

There are five interlinked strategic objectives for institutionalizing, operationalizing, and advancing CTCO within DOD. This “top to bottom” approach exemplifies how DOD's TCO policy is in support of broader USG efforts. Ultimately, DOD success in CTCO will depend on The Department's ability to fully integrate, support, and complement department and interagency counterparts' programs as part of achieving DOD's strategic objectives. These strategic objectives are listed below.

1. **Actively support a whole-of-government, full-spectrum approach to TCO.** DOD should serve as an enabling platform for interagency partners to work together against financial threats, synchronizing and sequencing policy, diplomatic, intelligence, law enforcement, and military authorities and capabilities. TCO priorities include counter-terrorism (CT), counter-narcotics (CN), counter-proliferation (CP), counter-intelligence (CI), and the interwoven component in all of these, CTF. The TCOs are not trafficking in people, weapons, and narcotics for recreational purposes but are doing so to gain access and placement and, more importantly, gain funding for their organization. The CTCO initiative should follow the CTF model. DOD should expand its commitment to, as well as, involve all interagency partners in DOD-focused CTCO efforts. Support for foreign partners and use of international laws and agreements is essential. DOD's ability to be part of a whole-of-government approach to TCO is predicated upon it developing sufficient internal ways, means, and doctrine as well as expanding its active support for interagency CTCO activities and capabilities. This capability must be developed out into a whole-of-nation effort, including the private business sector, which must combat the TCOs globally.

2. **Enhance TCO support for law enforcement against top-priority transnational threats.** DOD must work closely with U.S. and foreign law enforcement partners supporting efforts to provide strategic, operational, and analytical support for their respective judicial missions. This should be done by assisting in finding, following freezing, and seizure of illicit funds, prosecuting financiers, and targeting complex criminal revenue-generating and laundering mechanisms. This will aid the broader national security interest of disrupting and dismantling illicit financing networks, global drug-trafficking, and transnational organized crime threats. Law enforcement efforts have proven a very effective means of countering the financial base of support for state and non-state actors engaged in IW activities, and these actions will further enhance law enforcement's increasing role in supporting DOD's IW activities. Developing and deploying DOD financial intelligence support teams to law enforcement task forces based abroad must be prioritized, building on prior successes. A prime example of this occurred on February 10, 2011, when the U.S. Government designated Lebanese Canadian Bank as an institution of "primary money laundering concern" pursuant to Section 311 of the USA PATRIOT Act<sup>1</sup>.
3. **Organize, train, equip, and support CTCO/CTF units.** DOD must work in tandem with its interagency partners to build CTCO offices or units with the full range of capabilities at each of the CCMDs to complement OUSD(P)'s guidance based on the President's policy. These organizations must incorporate strategic planning, operations research, and tactical operational functions based on intelligence collection, analysis, dissemination, and database development.
4. **Develop Core DOD CTCO Capabilities,** including the following, which will be enhanced through partnership with the interagency community.
  - Interagency campaign strategies, which will support the creation and implementation of NSC CTCO campaign strategies with interagency partners.
  - CTCO operational capabilities including the development of deployable operational capabilities ranging from tactical through strategic levels, both within the context of DOD authorities and with the support and guidance of law enforcement, intelligence, diplomatic and policy partners.
  - Creation of military strategic plans, and where applicable, create CTCO and CTF strategic annexes for major military component plans.
  - Lines of operation and effort through creation of CTCO and CTF lines of operation and effort, using finance as a shaping capability within component plans.
  - CTCO Intelligence through expansion of the collection, analysis, dissemination, and database development of CTCO Intelligence to understand relevant nodes, networks, lines of communication, and bases of support for irregular and conventional military threats.
  - Defense from Foreign Threats Abroad through enhancement of the ways and means to defend against foreign threats—originating abroad—to the U.S. security, computer networks, banking, economic, and financial sectors.

---

<sup>1</sup>See <http://www.treasury.gov/press-center/press-releases/pages/tg1057.aspx> for more detail.

**5. Define and incorporate CTCO within DoD doctrine, strategy, and operational planning.** All of the strategic objectives listed above will depend on DOD incorporating CTCO as an element within DOD doctrine. This integration will include defense planning procedures and revisions of the Quadrennial Defense Review (QDR), and personnel, training and education programs. CTCO concepts should become integrated into DOD's evaluation of financial and economic bases of support, sustainment, strategic depth, centers of gravity, lines of communication, lines of operation, and lines of effort. CTCO doctrine will be applied within the full range of DOD intelligence, planning, and operational activities, in concert with interagency partners. Ultimately, the key to Department-wide CTCO success is centralized leadership by the interagency driving a uniform approach to combat this global threat.

### Countering Transnational Criminal Organizations

CTCO, mainly CTF, concepts have been employed in military operations and missions since the inception of the American Army. The first U.S. military expedition abroad, by the U.S. Navy and Marine Corps in 1801, was to safeguard America's trading and economic rights against the marauding Barbary pirates. During the Civil War, both the North and South waged sustained economic and financial combat against their respective industrial bases, banking systems, currencies, and supply lines. In World War II, the Office of Economic Warfare, the Office of Strategic Services, and the Strategic Bombing Survey were elements of a massive interdiction and infrastructure attrition strategy against the German and Japanese economies. As recently as the war in Kosovo, DOD-supported CTCO activities—in the form of implementing strong economic sanctions, engaging in rigorous interdictions of materiel and money, and providing active support for law enforcement against terrorists, war criminals, and corrupt officials—helped shape the strategic environment, contain the spread of conflict, and seal the grounds for a sustainable peace.

Despite historically symbiotic relationship between finance and warfare, DOD largely has failed to recognize how money both supports conflict and can be used as a fulcrum in countering traditional or irregular threats. Military doctrinal publications generally gloss over financing and economic sustainment issues. For example, the Army-Marine Counterinsurgency Manual highlights the importance of attacking insurgent money flows but does not describe, in any detail, potential ways and means for doing so (1-100-101).

In the 21st century, this doctrinal deficit has become increasingly problematic. America's adversaries, both military and criminal, have learned to operate in the seams of traditional doctrine, engaging in IW on not only political, social, and military levels, but criminally, economically, and financially as well. By integrating within the economic systems in which they operate and which they seek to control, adversaries shroud their financial centers of gravity and sustainment in civilian trappings. Our adversaries use practically every means

*"Sustainment requirements often drive insurgents into relationships with organized crime or into criminal activity themselves. Reaping windfall profits and avoiding the costs and difficulties involved in securing external support makes illegal activity attractive to insurgents. Taxing a mass base usually yields low returns. In contrast, kidnapping, extortion, bank robbery, and drug trafficking – four favorite insurgent activities – are very lucrative. ...Drugs retain the highest potential for obtaining large profits from relatively small investments."*  
Army-Marine  
Counterinsurgency Field  
Manual, 1-10 FM 3-  
24/MCWP 3-33.5 15  
December 2006, 1-56

available to generate and move cash and value to facilitate their nefarious activities. These mechanisms include formal and informal banking systems, trade-based money laundering schemes, illicit funding and transfer methods, legitimate cover businesses, and NGOs.

Economic IW has become big business for our political, military, and criminal adversaries. Businesses, NGOs, and media fronts have become major sources of financial support and conduits for operations globally for the Iranian Quds Force, MOIS, Hezbollah, the Taliban, the FARC, and others. These businesses provide self-sustaining means of financing and help launder massive amounts of illicitly generated income. They also enhance recruitment efforts by providing ready employment for group members. Finally, these front organizations and networks can advance the subversive penetration of our adversaries into foreign states, societies, and economies as well as clandestinely move materiel and personnel for terrorist operations. This strategy is designed to unveil the illicit activities of seemingly innocuous organizations.

Crime is perhaps the single biggest revenue generator for terrorist organizations today, producing billions of dollars each year to support, sustain, and spread their activities globally. Many terrorist groups have embraced the highly profitable illicit narcotics trade. Per the United Nations *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes* October 2011 report, drug trafficking and other transnational organized crime activities provide around US\$650 billion per year to the TCOs (p.7). Author and investigative journalist Gretchen Peters, who spent 10 years researching and reporting on the Taliban, argues that they have morphed from being a pious religious movement into something more akin to a drug cartel. Surveying 350 people “who work in or alongside the drug trade in 12 areas along the Pakistan-Afghanistan border,” Peters found that 81 percent of her respondents said that the “Taliban commanders’ first priority was to make money, rather than to recapture territory and impose the strict brand of Islam they had espoused while in power.” (Peters, 2009, pp. 12-13) The ability of the Taliban and other terrorist groups to fund their operations by participating in the \$300 billion+ annual global market for illicit narcotics is an obvious threat (UNODC, 2005, p. 16). Nonetheless, terrorist involvement in the narcotics business also is a significant potential vulnerability. To the extent that narco-terrorists can be indicted as “drug kingpin organizations” and internationally accepted asset forfeiture laws are successfully applied to seize and freeze their finances, the Taliban and other terrorist organizations could be imperiled.

DOD plays an important supportive role in effectuating all elements of national power (policy, diplomatic, intelligence, and law enforcement, and military) to defeat and defend against financially enabled and sustained adversaries and threats to our national security. Expanded DOD emphasis on all CTCO programs (e.g. CNT, CTF, weapons, and trafficking people) will support a full understanding of the people, mechanisms, and modus operandi of the transnational supporting infrastructure and networks used by our adversaries to finance and economically sustain their operations as well as promote their ideology. Interagency analysis will support planning and operations, from the strategic to the tactical level, to exploit vulnerabilities within adversaries’ depth and bases of support. In sum, it is DOD’s fundamental hope that CTCO will serve as a critical economy of force in wars of the present and the future, helping sever the “sinews of war” and minimizing loss of human life, degradation of infrastructure, and irreparable damage to the state and society.

## Strategic Objectives

The strategic objectives detailed in this document help define, guide, and build how DOD fully involves interagency as well as foreign government partners, and more specifically focus on developing DOD's internal capacity to strengthen interagency success. Meeting these objectives will be an important step in the ongoing evolution of DOD's capabilities to support non-kinetic ways and means to apply against the financing of state and non-state adversaries.

It is important to establish a baseline definition: CTCO is defined as *the means to detect, counter, contain, disrupt, deter, or dismantle the transnational activities of state and non-state adversaries threatening U.S. national security*. Monitoring, assessing, analyzing, and exploiting financial information are key support functions for CTCO activities.

The first objective is to **actively support a whole-of-government, full-spectrum approach to CTCO**. The objective of this initiative is for DOD to be a major support element to the interagency community in combating the transnational activities of state and non-state adversaries that pose a national security threat. Building on the successful progress serves as an enabling platform and force multiplier for interagency partners from Treasury, The Department of State (DOS), the Central Intelligence Agency (CIA), DOJ (including the DEA and FBI), DHS, and the National Security Agency (NSA). DOD must also understand that it will be required to closely coordinate and de-conflict its potential TCO targets with the interagency community working abroad to ensure that highly sensitive ongoing investigations and operations are not compromised, and that Agents, operatives and sources are not unnecessarily put in danger.

The second objective is development and support of **full-spectrum CTCO actions under the NSC**. The DOD CTCO strategy will maximize the value of the various interagency partner competencies, bringing to bear a more integrated approach to meet the unique challenges of addressing the 21<sup>st</sup> century's irregular threats. This approach, and the related shift in mind-set, will require strong relationship management skills as well as defined roles and responsibilities for each participating agency. Whereas past success was driven by personalities who saw the value in the interagency collaboration process, the goal will be to jointly establish formal mechanisms for institutionalizing interagency collaboration so it remains effective regardless of personnel changes. This strategy will serve to formalize the temporary threat finance cells currently in place and create a fully integrated, long-term, and whole-of-government approach.

The DOD CTCO strategy will be facilitated under the leadership of the NSC. The NSC is uniquely qualified for this role as it has previously coordinated foreign and defense policy and to reconcile diplomatic and military commitments and requirements. This jointly developed interagency CTCO platform will serve as a clearinghouse to reconcile competing priorities with everyone at the table. The interpersonal chemistry and interagency commitment among department and agency leaders has driven the collaboration to where it is today. This progress must be solidified into an institutionalized organizational structure that enhances the information flow and decision-making process. Much like the NSC, the CTCO interagency partnership must seek to foster collegiality between the agencies to work

toward what must be seen as an imperative, common goal to disrupt the transnational financing of state and non-state threats to our national security.

DOD seeks to be a supporting player in this effort, providing regional forums—through the infrastructure of Geographic CCMDs—where department and agency counterparts can interact in a collaborative environment. The strategy will mandate that DOD resources, expertise, and funding authority are brought to the CTCO fight and ensure The Department’s critical function is carried out in support of the interagency community. Based on the needed expertise of a particular organization, positions will be opened for the rotation of analysts and agents from the interagency community, who will cross-pollinate valuable knowledge and skills, leaving with an appreciation for the effectiveness of CTCO partnerships.

**The third objective is work with Congress.** Key to CTCO’s success within DOD is OUSD(P)’s ability to communicate with Congress and interagency partners. Continued clear and concise communication of the strategy that serves as the foundation of CTCO policy will assist lawmakers in making decisions with regard to appropriations and support. OUSD(P) will coordinate with DOD CTCO entities to provide periodic and voluntary presentations to congressional committees and sub-committees, such as the House Permanent Subcommittee on Intelligence (HPSCI), Senate Select Committee on Intelligence (SSCI), House/Senate Armed Services Committee, Senate/House Appropriations Committee, Senate Committee on Homeland Security and Governmental Affairs, and House Committee on Homeland Security, to increase awareness and deepen support for DOD’s efforts to further the overarching whole-of-government policy against illicit finance activities.

DOD will look to fully involve interagency partners in this communication effort. Joint DOD and interagency communication and presentations to relevant Congressional Committees can help support the shared goals of interagency partners and success of our combined efforts.

**Future Success Built On Lessons from the Past.** Achieving these strategic objectives will allow DOD to institutionalize and operationalize CTCO capabilities within and across all levels of military policy-makers, strategic planners, leaders, and operators. While DOD believes CTCO capabilities are both an extension of traditional military activities and a necessary activity for DOD to conduct, DOD firmly recognizes that such capabilities will be most effective when executed as an integral part of, and in coordination with, the interagency community. A key example of this concept is the Afghan Threat Finance Cell (ATFC), which is led by DEA even though it operates within an active war zone, as discussed below.

**Fourth, enhancement of CTCO support for law enforcement against top-priority transnational threats.** Providing increased and coordinated support to law enforcement operations is a core element of DoD’s CTCO strategy, particularly in the context of countering the financing and conduct of IW. Strategically coordinated law enforcement investigations can have a dramatic, deep, and sustained impact against the financial depth of organizations that rely on illicit income for even a part of their financing. This is especially true when jointly supported by domestic and international legal authorities for criminal

investigation, prosecution, and asset forfeiture. Such operations also bolster our national security, both domestically and abroad.

Individual successes from this approach are already evident. In May of 2008 Khan Mohammed, a member of an Afghan Taliban cell, was convicted on charges of narcotics distribution and narco-terrorism. In the DEA press release, DEA Acting Administrator Michele M. Leonhart was quoted as saying, "As an enemy of the United States, Khan Mohammed intended to ship heroin to the United States and use profits from that trade to assist the Taliban" (DEA 2008). This exemplifies a counter-narcotic priority target, operating in the AF-PAK theater of operations, convicted as a result of DEA and coalition law enforcement efforts.

Authorizations under §1004<sup>2</sup> and §1022<sup>3</sup> of the National Defense Authorization Acts can serve as significant force multipliers in that they allow DOD to provide support to law enforcement counter-drug and counter-terrorism activities. Increasing this support could provide another means for DOD to further USG efforts to counter the transnational financing of state and non-state adversaries. These could be the basis of bringing these authorities and modifying them to meet the current threats more effectively and providing the "teeth" to the President's TCO strategy. Conversely, the DEA's powerful extraterritorial jurisdictions, for example, Title 21 USC §960(a), provide formidable options to Combatant Commanders in non-declared areas of war outside Afghanistan and Iraq, as well as within both those countries when working with the DEA.

**Interagency Campaign Strategies are also critical to successful interagency operations.** Among the most powerful capabilities that DOD brings to the government is a comprehensive, disciplined, and finely developed capacity to develop complex strategic plans. As part of the USG's CTCO approach, DOD will support the creation and implementation of CTCO campaign strategies with the interagency community and the NSC, in concert with and fulfillment of various National Action and Implementation Plans. This would enable Federal Law Enforcement to posture themselves ideally to meet this ever-morphing threat more efficiently and reduce redundant efforts.

As perhaps best illuminated by the experiences of U.S. law enforcement against the finances of Latin American drug cartels, CTCO operations are optimally applied within a strategic campaign of dovetailing actions designed to significantly disrupt an organization's finances across the board, ultimately leading to the dismantlement of entire organizations. To achieve maximum effect, CTCO campaigns will be designed so that operational effects are distributed across organizational depth, time, and environment. Targets of CTCO Campaigns can span from kingpins and couriers to bank accounts and businesses. OUSD(P) will work with interagency partners to facilitate the coordination, sequencing, and synchronization of actions to turn tactical activities into high-impact strategic achievements.

**CTCO operational capabilities will be prioritized as well.** CTCO Operations are DOD-supported, or synchronized, operations with interagency partners against CTCO targets, networks, and lines of

---

<sup>2</sup> National Defense Authorization Act for Fiscal Year 1991

<sup>3</sup> National Defense Authorization Act for Fiscal Year 2004

communication designed to effectively counter the financial depth and sustainment capacity of adversaries engaged in irregular or traditional warfare. CTCO Operations can be applied to each level in Interdiction Operations as envisioned within Joint Publication 3-03: *Joint Interdiction*, including Direct Attrition of Enemy Capabilities, Constricting the Enemy's Logistic System, Disrupting Enemy C2, Forcing Urgent Movement Upon the Enemy, Channeling Enemy Movements, Denying Enemy Threat Potential, and Enforcement of Sanctions (JP 3-03- viii). Likewise, at the campaign level, CTCO Operations apply to complementary operations as defined in doctrine, including strategic attack, intelligence, surveillance and reconnaissance, space operations, and information operations. Each of these operations implicitly includes CTCO elements (see JP-03, II-02). In terms of broader application and doctrinal implications, CTCO Operations also fall under the rubric of the "Global Nature of Operations" as defined in JP-1, *Doctrine for the Armed Forces of the United States* (JP-1, I-8).

**Military strategic plans will include CCTO in their lines of operation and lines of effort.** Using a consistent and shared organizational framework, such as a Financial Order of Battle will ensure that appropriate attention is given to assessing and attacking financial centers of gravity. CCMDs will be responsible for their strategic plans and any related operations in their respective area of responsibility.

**Lines of operation and effort will be established.** CTCO strategic planning doctrine will detail a comprehensive and standardized framework for CTCO lines of operation and lines of effort against an adversary's FinOB. To be successful, each hierarchical line needs to be analyzed.

- **Command** will address the power and hierarchy of the adversary. This includes the identification of key threat financial managers – individuals responsible for managing financial affairs on behalf of the adversary as well as the sub-structure, including partners, alliances, parent, or subordinate entities, and any connections to government entities.
- **Financing** will include understanding how the adversary generates funding as well as the mechanisms the adversary uses to transfer funds. This line of operation will not be limited to cash and cash-equivalents in the formal banking system, but expanded to include analysis of trade-based schemes used to generate and transfer value. The financial strengths and weaknesses of the adversary can also be a valuable component for an Information Operations campaign.
- **Business Operations** will focus on understanding what the adversary does and where the adversary operates. This information drives comparative analysis between CTCO targets to identify key players in a region, business operations (whether licit or illicit), the public profile of the adversary, and ultimately identifies the critical targets to be aggressively pursued and attacked.
- **Material is necessary to sustain operations.** Understanding the inputs needed to sustain operations can assist in identifying key vulnerabilities of the adversary. Inputs include position in cash, inventory, and property, plant and equipment, as well as other items that represent value or a store of money.
- **Coordination** focuses on understanding how the adversary interacts with other entities, through trusted agents, logistics providers, and methods of communication.
- **Administration** functions are needed to support any organization. One needs to understand how a CTCO target recruits, retains, and trains personnel as well as conducts other "care-taking" activities. Administration also includes any legal function or external relations (i.e., propaganda).

**CTCO Intelligence will utilize existing USD(I) capabilities.** The USD(I) is the DOD lead on intelligence issues, including CTF Intelligence (CTFI). In building CTCO capabilities, USD(I), along with the Defense Intelligence Agency (DIA), provides intelligence support to DOD warfighters and planners. Like CTFI programs, CTCO, will also contribute to the Joint Intelligence Preparation of the Operational Environment. This includes the analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision-making process (Joint Publication 2009).

**Defense from Foreign Threats Abroad will increase through development and implementation of a CTCO program.** Specifically, a DOD CTCO program will enhance ways and means to defend against foreign threats, which originate abroad to the U.S. banking, economic, and financial sectors. DOD should have a permanent representative on the Treasury and Federal Reserve Board led Interagency Committee focused on protecting America's critical banking and financial infrastructure from strategic threats.

**CTCO will be defined and incorporated within DOD doctrine, strategy, and operational planning.** All of the strategic objectives listed above will depend on DOD incorporating CTCO as an element within DOD doctrine, including defense planning procedures and revisions of the QDR, and throughout personnel, training and education programs. Monitoring, assessing, analyzing, and exploiting financial information are key support functions for CTCO activities. DOD must understand that CTCO activities are primarily interagency in nature, with many authorities, capabilities, and capacities beyond the scope of DOD.

The importance and use of CTCO capabilities within the context of an effects-based approach to countering our adversaries must become embedded knowledge within DOD. Current DOD doctrine may highlight the importance of affecting insurgent money flows. However, it does not describe, in any detail, potential ways and means for doing so. DOD will integrate CTCO concepts within all relevant doctrine and manuals to ensure that evaluation of our adversaries' transnational financing; including their bases of support, sustainment, and strategic depth, centers of gravity, lines of communication, lines of operation, and lines of effort are routine procedures. In addition to integrating CTCO into revisions of the QDR, CTCO concepts and doctrine will be included in Keystone Joint Publications and subordinate documentation as appropriate and within the full range of DOD personnel, intelligence operations, and planning activities.

## Conclusion

However beautiful the strategy, you should occasionally look at the results.

Winston Churchill

It is critical to remember that, first and foremost, **all** terrorist organizations are Transnational Criminal Organizations. Second, if the money is disrupted, the adversary is destroyed: they cannot pay, feed, or outfit their members and they will turn on themselves or just disappear.

The strategic objectives outlined in this chapter provide a basic roadmap for DOD to be a major support element to the interagency community in combating the financing of state and non-state adversaries. When its CTCO program is fully implemented, envision that DOD will be:

- Integrated at a policy and programmatic level as well as operationally coordinated and de-conflicted, with interagency partners and the NSC;
- Operationalized within all DOD CCMDs; and
- Institutionalized within the entire DOD.

DOD has already made some progress toward its objectives and has established goals, milestones, and metrics to measure further success.

### **CTF Activities for a CTCO Model**

DOD has been actively working to formalize its CTF efforts and has implemented a Directive on Counter Threat Finance (DODD 5205 gg, August 19, 2010). The Directive provides CTF authorities and guidance. A similar DODD for CTCO should be implemented.

CDRUSSOCOM has established a staff at its headquarters. It was designated as the DOD lead component for synchronizing CTF operations. USCENCOM has also been very actively engaged in successful CTF activities through their ITFC and ATFC. Current CTF activities include a USSOCOM-led annual global synchronization conference, semi-monthly secure video teleconferences between the CCMD CTF units, development of CTF training for the DOD community, and support to their Law Enforcement Partners.

Other activities have been undertaken by DOD and the interagency partners, but as Lt. Gen. Fridovich noted in his testimony to the House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities, "Success in this arena is, by its nature, not always conspicuous" (2009).

## Chapter 1 B: Combating Transnational Criminal Organizations in the Western Hemisphere: It, too, Takes a Network

Colonel Glen Butler

[glen.butler@northcom.mil](mailto:glen.butler@northcom.mil)

USNORTHCOM

Deputy Chief of Staff, Communication Synchronization, NORAD & USNORTHCOM

Transnational organized crime and transnational criminal organizations refer to a network or networks structured to conduct illicit activities across international boundaries in order to obtain financial or material benefit. Transnational organized crime harms citizen safety, subverts government institutions, and can destabilize nations.

Department of Defense Counternarcotics and Global Threats Strategy, 27 Apr 11

### Introduction

In the March/April 2011 edition of *Foreign Policy*, General Stanley A. McChrystal dissected the “new front line of modern warfare” in his article “It Takes a Network.” Given General McChrystal’s in-depth description of network activity, this is a must-read for those participating in efforts to combat TCOs and Transnational Organized Crime (TOC).

Outlining the shift in tactics the U.S. military and its partners employed against insurgents in Iraq (including Qaeda), as well as the Taliban in Afghanistan, General McChrystal described how both foes were “more network than army, more a community of interest than a corporate structure.” More importantly, he (2011) stated:

To defeat a networked enemy we had to become a network ourselves. We had to figure out a way to retain our traditional capabilities of professionalism, technology, and, when needed, overwhelming force, while achieving levels of knowledge, speed, precision, and unity of effort that only a network could provide.

The Chairman of the Joint Chiefs of Staff, General Martin Dempsey, who, in an interview with NBC’s Ted Koppel on January 24th, 2013, discussed current efforts against the “global terrorist network,” recently echoed this line of thinking. General Dempsey reiterated McChrystal’s mantra: “what we’ve had to do in response is we have become a network. To defeat a network, we’ve had to become a network.”

In “It Takes a Network,” General McChrystal went on to say that:

...an effective network involves much more than relying data. A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to see, decide, and effectively act. But transforming a traditional military structure into a truly flexible, empowered network is a difficult process.

Foreign Policy, 2011

Nevertheless, no matter how difficult the process, embracing the network approach to combat the dangerous networks of TCOs and TOC—not only in the Western Hemisphere, but across the globe—will be key to our collective success.

### Background

U.S. Northern Command (USNORTHCOM) was established October 1<sup>st</sup>, 2002 at Peterson Air Force Base in Colorado Springs, Colorado, to provide command and control of DOD homeland defense efforts and to coordinate defense support of civil authorities. USNORTHCOM’s Area of Responsibility (AOR) includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico, the Straits of Florida, and portions of the Caribbean region. The “third border” includes the Bahamas, Puerto Rico, the U.S. and British Virgin Islands, Turks and Caicos Islands, and Bermuda. As the official Theater Strategy proclaims, it is a “complex operational environment and is a theater of operations with unique and special requirements.”

The commander of USNORTHCOM is responsible for theater security cooperation with Canada, Mexico, and The Bahamas. “Security Cooperation” was added to the USNORTHCOM mission statement in June 2010, and “partners” was added in November 2011. Today’s mission statement reads: “USNORTHCOM partners to conduct homeland defense, civil support, and security cooperation to defend and secure the United States and its interests.” (Northcom.mil, February 2013).

The commander of USNORTHCOM also commands the North American Aerospace Defense Command (NORAD), a bi-national organization responsible for aerospace warning, aerospace control, and maritime warning for the defense of North America. NORAD and USNORTHCOM have complementary missions, and members of the staffs are integrated and cooperate daily to fulfill homeland defense responsibilities.

## An Extraordinary Threat

Significant transnational criminal organizations constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and I hereby declare a national emergency to deal with that threat.

### Executive Order 135B1

Without question, TCOs pose a real and present risk to the safety and security of Americans and our partners in North America and across the Western Hemisphere. Although the close relationship between drug trafficking and criminal organizations is not a new phenomenon, the recent spike in violence and public awareness can be attributed with certainty to two basic shifts. First, the gradual rise in the power of the Mexican criminal organizations as they assumed control of the drug flow (and production) in increasing amounts from the Colombians of the 1980s and 1990s. Second, former Mexican President Felipe Calderon's bold decision to place the Mexican military on the streets to combat the TCOs. President Calderon's 2006 decision addressed decades of ineffective policing and even periods of alleged government accommodation.

TCOs pose a significant danger to the US, our allies, and our partners. Recent improvements to combat TCOS include synchronized planning and coordinated operations to counter this growing menace. Yet, barriers remain to achieving a universal realization of TCOs as a true threat to homeland security—and to effective solutions to this threat. Today's conflict is not the "War on Drugs" declared by President Nixon in June 1971. Nevertheless, despite cyclical progress from previous years, and the evolving partnership of US-Mexican security forces and leadership, initiatives to counter TCOs and TOC still have room for improvement.

## Why This Matters

Five key threats to U.S. National Security: (1) Transnational Organized Crime (TOC) Penetration of State Institutions; (2) TOC Threat to the U.S. and World Economy; (3) Growing Cybercrime Threat; (4) Threatening Crime-Terror Nexus; and (5) Expansion of Drug Trafficking (Mexican drug trafficking organizations continue to expand their reach into the United States.)

### The Threat to U.S. National Security, 2011

Before examining the current nature of the problem, it is useful to review the nature of the U.S.'s relationship with some of its North American and hemispheric partners. On September 5th, 2001, President George W. Bush declared that the U.S. "has no more important relationship in the world than the one we have with Mexico." The infamous terrorist attacks six days later brought new attention to the importance of cooperative defense and continental security shared by the nations of North America, with a renewed understanding of shared responsibility for collective peace and mutual prosperity.

Beyond security, another clear reason for our symbiotic existence is economic. The North American Free Trade Agreement (NAFTA) of 1994 accelerated the intertwining of the economies of the U.S., Canada, and Mexico. To the south, the "integration of the United States and Mexican economies has

transformed the nature of the bilateral relationship from one of competition to partnership...As the second largest destination for U.S. exports...6 million U.S. jobs depend on trade with Mexico.” (Wilson, 2011) Mexico is the third largest U.S. trading partner, with about 80 percent of Mexican exports going to the U.S., and roughly 30 percent of Mexican imports arriving from the U.S. As an example, Mexico spent almost \$200 billion on U.S. goods in 2011—that is more U.S. export sales than all U.S. exports to the BRIC countries (Brazil, Russia, India, and China) combined. Finally, for every dollar Mexico earns on exports to the U.S., it gives about 50 cents back, spent on American services or products (Keppel, 2011).

The threat of TCOs and illicit trafficking is not restricted the U.S.’s southwest border. Looking north, Canada and the U.S. are “staunch allies, vital economic partners, and steadfast friends.” Approximately \$1.5 billion in trade and 300,000 people cross our northern border each day: that is nearly one million dollars in goods and services every minute (Obama and Harper, 2011). Each country is the other’s number one trading partner, and share essential bi-national infrastructure such as pipelines, rail lines, water supplies, communication networks, and electric power grids. With 119 official border crossings and over 900 organized crime groups in Canada, a growing amount of methylenedioxymethamphetamine (MDMA/ecstasy) and high-potency marijuana continues to be smuggled across the border by these groups. To the southeast, places such as The Bahamas are vital partners in the Caribbean, representing longstanding tourist destinations for Americans as well as vulnerable transit corridors for illicit trafficking and potential inroads for influence competitors, particularly China, to counter U.S. presence and overall stability.

Vibrant relationships based on trust are essential if the U.S. is to remain the partner of choice, and effectively counter TOC, in the hemisphere. The *National Strategy for Homeland Security* states that “throughout the evolution of our homeland security paradigm, one feature most essential to our success has endured: the notion that homeland security is a shared responsibility built upon a foundation of partnerships” and “in addition to al-Qaeda, a host of other groups and individuals also use terror and violence against the innocent in pursuit of their objectives and pose potential threats to the security of the United States.” (October 2007) Similarly, the *National Military Strategy* calls on our Defense Department to “build an increasingly close security partnership with Mexico,” and stresses that by “working with Canada and Mexico, we will remain prepared to deter and defeat direct threats to our North American homeland” (May 2010)<sup>4</sup>. Clearly, partnerships are crucial to any successes against the TCO adversary.

Despite the rising attention being paid to TCOs, official statements proclaiming the importance of the issue and the efforts to address the problem are not new.<sup>5</sup> However, despite the commonality of past

---

<sup>4</sup> See also National Security Strategy, May 2010; National Military Strategy, February 2011; Western Hemisphere Defense Policy Statement, October 2012; and NORAD and USNORTHCOM Theatre Strategy, 2012.

<sup>5</sup>A U.S. Government Accountability Office (GAO) report to Congress in December 1974 cited efforts in February 1973 to “provide assistance to increase the effectiveness of the Mexican Government’s border, air, and sea anti-narcotics law enforcement” and claimed that the Drug Enforcement Agency (DEA) and the Government of Mexico (GoM) had “intensified enforcement efforts in recent years” and the DEA believed that “much information is now being exchanged between the GoM and DEA

and current narratives, the threat today has matured into a much different and more dangerous enemy than yesteryear's cartels of the so-called "drug war."

No longer simply "Drug Trafficking Organizations," modern TCOs operate well outside the narcotics realm—theirs is a vicious world of kidnapping, murder, money laundering, piracy, oil and agricultural theft, human trafficking, body parts harvesting, and other illicit activities. The costs for society of bearing these illegal and often gruesome enterprises goes well above that of financial losses or even the societal impact associated with drug abuse, and interdiction metrics (e.g., kilos of cocaine seized) associated with previous eras are proving insufficient—and, to a degree, irrelevant. According to The Department of Defense Counternarcotics and Global Threats Strategy, "Transnational organized crime represents a significant, multilayered, and asymmetric threat to our national security...It is not viable for DOD to continue to examine this complex threat through the lens of the drug trade" (2011) Indeed, these organizations—like al-Qaeda, and other VEOs—are evolving as complex threat networks unlike their predecessors of years and decades past.

Criminal networks are not only expanding their operations, but they are also diversifying their activities, resulting in a convergence of transnational threats that has evolved to become more complex, volatile, and destabilizing.

Strategy to Combat Transnational Organized Crime,  
2011

So, as the past decade has witnessed huge increases in the transnational economic interrelationships because of globalization, a growing necessity for cooperative defense of the homelands, and skyrocketing costs of drug abuse, other transitions illustrate why the fight is so different now, and has truly become a danger to the safety and security of our peoples. While the presence of drug dealers and

---

-A 1988 RAND report stated that "the importation of drugs into this country has been treated as a serious public policy problem for almost two decades" and said that "in 1986, the President's Commission on Organized Crime (PCOC) stressed 'the maintenance of persistent pressure on drug traffickers, both as a deterrent and a symbol of national determination.'"

-A June 1990 Narcotics Interdiction and the Military bibliography preface stated "recently there has been substantial controversy over the United States military's role in the drug war. Under legislation passed in 1981, the Department of Defense now assists civilian law enforcement agencies in their fight to combat illegal drug trafficking by lending military equipment and facilities, through intelligence sharing, and by providing expert training and advice to civilians...some policymakers see the drug problem as a threat to the economic, social, and national security of our country and look to the military for assistance and cooperation."

-In the May 1997 "Joint Declaration of the Mexican/U.S. Alliance Against Drugs" by Presidents Ernesto Zedillo Ponce de Leon and William Jefferson Clinton, the leaders officially stated: "drug abuse and drug trafficking are a danger to our societies, an affront to our sovereignty and a threat to our national security" and "Mexico and the United States will focus law enforcement efforts against criminal organizations and those who facilitate their operations in both countries...and enhance cooperation along both sides of our common border to increase security"

-The *US/Mexico Bi-National Drug Strategy* of February 1998 proclaimed "the Governments of the United States and Mexico recognize that the current dimensions of international drug trafficking and related crimes extend beyond national boundaries and exceed the capacity of any nation to face them in isolation. These have become a serious problem that affects the health and security of international society."

gang members in U.S. cities is also nothing new, their hierarchal organization, adaptation, expansion, and sheer numbers do represent a growing hazard (Expanding size, scope and influence, 2011). Today, Mexican TCOs are present in over 1,000 U.S. cities (National Drug Threat Assessment, 2011), up from an official estimate of 270 cities just a few years ago. (The Drug Enforcement Agency estimated TCO presence in almost 1,300 cities as of November 2012 (Horwitz, 2012)). Working in collaboration with the TCOs are sophisticated gangs, “expanding, evolving and posing an increasing threat to U.S. communities nationwide” and comprised of approximately 1.4 million members in over 33,000 gangs in our country (National Gang Threat Assessment, 2011, pp. 7 and 23). In January 2013, the FBI reported that 40 percent of U.S. gangs have Mexican TCO affiliation. According to experts, these “criminal networks transcend physical, geographic and societal borders into the worlds of government, business and finance. The criminal networks’ ability to freely operate in the legitimate society increases the likelihood of their survival despite the best efforts of law enforcement.” (Commander’s Handbook, 2011, p. c-3) To combat these criminal elements, the U.S. Government spends over \$5.5 billion every year on gang suppression, prevention, and corrections programs (National Drug Threat Assessment, 2011, p. 7). In addition, it spends roughly \$15 billion in annual drug control efforts (2010 Figure).

Of course, the negative impacts of illicit drug use can be measured in many more ways than strictly dollars leveraged annually for drug control. But, the economic impact is not insignificant: the actual cost is approximately \$200 billion for Americans each year, based on data collected in three key areas: crime, health, and productivity (Economic Impact of Illicit Drug Use, 2011). Likewise, on the Mexican home front, a recent report noted that Mexico loses roughly \$50 billion a year in “illegal financial outflows.” Crime, tax evasion, and corruption have also, quite literally, robbed the Mexican economy, with losses of a staggering \$872 billion between 1970 and 2010 (Mexico Loses, 2011). Also, in January 2013, the Mexican National Business Council for Tourism President said that Mexico had lost approximately \$12 billion in tourism benefits because of “real and perceived insecurity.” (Southern Pulse, 2013) Beyond the impact of drugs, efforts to secure the U.S.’s Southwest Border have not been cheap. According to the *New York Times* (Ngai, 2013):

In the last quarter-century, we [the U.S.] have spent approximately \$187 billion on enforcement, mostly along the United States-Mexico border. This included a nine-fold increase in the size of the Border Patrol since 1980; nearly 700 miles of fencing; and the deployment of surveillance drones and motion sensors.

With a simple addition of these costs—supported by pronouncements from senior leaders such as former Chairman of the Joint Chiefs of Staff Admiral Mike Mullen, who have labeled debt as “the most significant threat to our national security,” (CNN, 2010)—the fiscal impact associated with TCOs increases their candidacy as one of the foremost threats to homeland security today.<sup>6</sup>

One common theme often heard is that U.S. consumer demand for drugs fuels the need for supply, and thus the associated crime and violence as well. While there is truth to this adage, the demand is not limited to American cities alone. TOC is, of course, a worldwide problem, with drugs and other illicit

---

<sup>6</sup> Globally, transnational organized crime is estimated, by some, to be over a \$2 trillion industry, spanning five continents.

products' trafficking routes spread across the globe. South American cocaine can be found in Europe just as heroin from Afghanistan appears in Russia and the U.S.

Internally in Mexico, drug consumption has risen dramatically in the last decade, and with it a corresponding surge in violence: there is a direct correlation between the two. Results from a survey published roughly every five years (most recently in 2008) showed that between 2002 and 2008, the number of Mexicans who had used drugs increased by a million—from 3.5 million to 4.5 million, and cocaine use almost doubled (Mexico Drug Addiction). In late 2009, one Mexican doctor stated, "Mexico used to be a transit place, the trampoline. Now it's a consumer country." (Althaus, 2009) Another national survey of addictions revealed that illegal drug use in Mexico rose 87 percent between 2002 and 2011 (Villagran, 2013). Along with increased internal production in Mexico, this rise in consumption has contributed to a blurring of the previously accepted definitions of drug "production, transit, and arrival zones," thus rendering that lexicon outdated. The borderlines have blurred as well: along the Mexico-U.S border, some experts believe that Mexican TCOs actually have a strategic plan that includes the creation of a "sanitary zone" inside the U.S., about a "county deep," that would provide refuge from Mexican law enforcement and serve as distribution sites for illegal products and personnel into our country (McCaffery, 2011, p.17).

A few other key aspects of the situation today warrant attention here. The first is the utter "all bets off" brutality of the violence, familiar to anyone in America with a television or Internet access. To some degree, cartels of the 1980s and 1990s followed an unwritten criminal ethics code of sorts, adhering to accepted norms that included not targeting family members or highlighting the violence, refraining from selling drugs to Mexicans, and generally "keeping a lid on it." Many of today's TCOs, however, have rewritten their criminal playbook. The brutality has expanded well beyond anyone's darkest imagination; drug abuse and addiction are reaching epic proportions; and the potential to exceed the next step of unimaginable remains high.

This leads to another vexing issue: the increasing possibility for a cartel-terrorist/VEO nexus. Many analysts today believe that the likelihood is low, but government officials are watching closely and stand poised to respond if such a threat elevates. Unfortunately, enemies do not give notice when they decide to change tactics or engage in practices previously deemed to conflict with their accepted business model. (Indeed, few airline flight attendants were on the lookout for boxcutter-wielding hijackers in July and August of 2001; often an emerging threat reveals our best response to be too slow and ineffective.)

Transnational organized crime is an abiding threat to U.S. economic and national security interests, and we are concerned about how it might evolve in the future. We are aware of the potential for criminal service providers to play an important role in proliferating nuclear-applicable materials and facilitating terrorism.

Director of National Intelligence James R. Clapper, 2012

## Challenges and Opportunities

A fundamental challenge to ongoing efforts to curb the growing crisis stems from the shared history of the U.S. and Mexico. America's history of intervention, coupled with an unyielding skepticism and distrust on the part of some Mexican partners, has prevented both nations from together as effectively as possibly in years past to achieve sufficient success. Former National Drug Policy Director and U.S. Southern Command Commander retired General Barry McCaffrey (2011) explained:

Our response and interaction on a people-to-people basis is extremely positive. There is an enormous affinity shared between the Mexican and American people, both along the border and throughout the country. But on an official level, for hundreds of years, there has been a tremendous anxiety—bordering on paranoia, on the part of Mexico...So the dialogue between the United States and Mexico, outside of the last ten years, has been based upon a combination of U.S. ignorance and arrogance, and Mexican paranoia...and that does not lead to sensible policy.

This “paranoia” General McCaffrey mentions lingers for some, and is rooted in Mexico's Constitution with text that limits partnering with foreign powers (see Article 76, 2005). Even so, the last several years have seen historic warming and maturation of the relationship towards a real regional, strategic security partnership—one that hopefully continues to mature over future months and years.

Others have different takes on the problem and prescribe solutions of, essentially, acceptance. Intelligence firm STRATFOR's founder and CEO George Friedman (2011) opined:

The American strategy will continue to be inherently dishonest. It does not intend to stop immigration and it doesn't expect to stop drugs, but it must pretend to be committed to both...Over the next ten years, the president will be engaged in constant investigations to provide the illusion of activity in a project that cannot succeed...the only solution is to allow the drug wars to burn themselves out, as they inevitably will. (p. 211, 213)

Waiting to allow “the drug wars to burn themselves out” might be tempting, especially after reviewing the reinventions of the counterdrug policy and strategy wheels over the last several decades. However, citizens depend on their government to do their utmost to protect them. This sacred trust that comes with the homeland defense and security missions<sup>7</sup> demands much more than appeasement.

---

<sup>7</sup> *Homeland Security* is defined as “a concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur.” (JP 3-28, *Civil Support*, 14 Sep 07). *Homeland Defense* is defined as “the protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the President.” (JP 3-27, *Homeland Defense*, 12 Jul 07) “The Homeland Defense [HD], Civil Support [CS], and Homeland Security [HS] missions are separate, but have areas where roles and responsibilities may overlap and/or lead and supporting roles may transition between organizations...In addition, operations may transition from HD to CS to HS

This is no longer just a law enforcement issue; it is a problem that demands the attention, and assistance, of a broad spectrum of partners.

Attorney General Eric H. Holder, Jr., 2011

Competing global threats and challenges, limited resources, and the lack of a bi-national, interagency, unifying policy or strategy—as well as absence of an associated centralization of command, or true unity of effort—round out the dilemma. Coupled with a veritable alphabet soup of agencies, task forces, initiatives and mini-strategies to attempt to confront the threat, the tendency is to operate too often in stereotypical stovepipes. These stovepipes contain well-meaning professionals, and are often loosely duct-taped together, but without a single authority and absent specific, overarching hemispheric guidance around which the disjointed efforts can coalesce, actions to combat TCOs risk remaining insufficient, and some believe, are potentially doomed to fail (Kerlikowske, 2011). The President's Strategy to Combat TCO (released in July 2011) is a promising start. The first of five key objectives in the strategy is to “protect Americans and our partners from the harm, violence, and exploitation of transnational criminal networks,” and the first of the six priority actions is to “start at home: taking shared responsibility for transnational organized crime.”

The *Department of Defense Counternarcotics and Global Threats Strategy* (April 2011) is also valuable. One strategic goal, for example, is that “the size, scope, and influence of targeted TCOs and trafficking networks are mitigated such that these groups pose only limited, isolated threats to U.S. national security and international security. The U.S. and partner nations have developed layered, coordinated approaches that regularly disrupt the operations of these organizations and networks, limit their access to funding, reduce their assets, and raise their costs of doing business.” But, this is a DOD product, not Whole-of-Nation guidance. In the end, more actionable responses to senior-level guidance such as these must be realized; however, even with such responses, the broad, global emphasis of these strategies makes them unlikely to yield tangible benefits for North America within the next decade.

Part of the reason behind the lack of a single, coherent strategy is that many stakeholders have yet to agree on how to approach the issue. Treating TCOs primarily as a crime problem within the U.S., law enforcement agencies focus on patiently building cases against the criminals. In their supporting role, the U.S. military prefers to “Attack the Network (AtN)” or “Counter Threat Networks (CTN)” and aggressively bring down the entire network of the TCO enemy, while building partner capacity with other nations' security forces in the long-term view towards strengthening strategic security partnerships. Many partner nations have, until recently, preferred a “kingpin strategy” aimed at taking out TCO leadership. (However, recently inaugurated Mexican President Enrique Peña Nieto has stated a determination to move away from the kingpin strategy and focus instead on reducing violence (and specifically, crimes such as murder, kidnapping, and extortion and is creating a European-modeled gendarmerie, a national intelligence center, and embarking on other new government restructuring as part of these efforts). Without U.S. consensus or an international agreement on how to go about

---

and vice versa with the lead depending on the situation and US Government's desired outcome.” [JP 3-28, *Civil Support*, 14 September 2007, Executive Summary p. vii]

disrupting or defeating TCOs' illicit activities, and capstone measures ping-ponging over the last few decades between interdiction, source disruption, and (less so) institution building,<sup>8</sup> significant challenges will remain.

Another obstacle to achieving a greater margin of success is the legalization debate; put simply, this is a red herring. As discussed, drugs are but one of many avenues for making money by today's TCOs, and although analysts have yet to concur on the percentage garnered from drug sales, most agree that it's less than 50 percent. Many experts say that marijuana revenues are closer to the 20 percent mark (UNODC, Estimating Illicit Financial Flows, 2011). For reasons beyond the scope of this paper, suffice it to say that legalizing drugs is no panacea and will not put a substantial long-term dent in TCOs' profits sufficient to "win the war," to say nothing of the additional economic and cultural burden that would be assumed by our society with such a radical shift in policy.<sup>9</sup>

[Marijuana legalization] creates certain distortions and incongruences since it's in conflict with [U.S.] federal [law], and that will have an impact on how Mexico and other countries in the hemisphere respond. Personally, I'm against legalization; I don't think it's the [correct] route. But I am in favor of a hemispheric debate on the effectiveness of the drug-war route we're on now.

Padgett, 2012

Lastly, despite our desire to be the "partner of choice" for international friends within the region, sometimes interagency legal wrangling, sensitivities, parochialism, diminishing resources, and old-fashioned bureaucracy stymie U.S. responses to requests for assistance from others. This not only degrades our credibility, but increases the likelihood that these partners will eventually tire of waiting, and seek assistance elsewhere. With Iran and China actively courting allies in our backyard, this is not

---

<sup>8</sup> A Joint Hearing in June 1994 before the Subcommittees on International Security, International Organizations and Human Rights, and the Western Hemisphere of the Committee on Foreign Affairs was titled "Counternarcotics Strategy for the Western Hemisphere: A New Direction?" At this hearing, the Honorable Robert S. Gelband, Assistant Secretary for International Narcotics Matters, U.S. Department of State, said: "Last year, we developed a new counternarcotics strategy for the Western Hemisphere. It addresses the twin concerns confronting this administration and this Congress in January of 1993, the perception that the past strategy was not working and the need to reduce budgets. The new strategy calls for a gradual shift in emphasis from transit interdiction to source country efforts. It calls for us to support democratic counternarcotics institutions in source countries and to integrate counternarcotics into global alternative development strategy. It seeks greater involvement by international and multinational organizations and continued efforts against entire trafficker organizations. In short, the new strategy seeks to reinforce what we have seen that works, coordinate and consolidate among multiple programs to ensure efficiency and engage international organizations that previously had shied away from involvement in counternarcotics." A summary of a Congressional Hearing in June 1996 declared that there is "a growing national security threat posed to all Americans by four powerful, well-financed, and violent Mexico drug cartels," and "the United States and Mexico have created a framework for increased cooperation and are expected to develop a joint counternarcotics strategy by the end of the year. Also, although there are several written agreements on specific issues between the US and Mexico, the last time there was an overarching bi-national strategy was fifteen years ago (US/Mexico Bi-National Drug Strategy of February 1998).

<sup>9</sup> See also: <http://www.justice.gov/dea/demand/speakout/index.html> for basic reasons why legalization is not the answer to counter TCOs

an issue to be taken lightly, lest we're soon faced with a modern day version of a competitor soft power "Cuban missile crisis"—consummated first by gifted soccer stadiums, and eventually with weapons sales, alliances, and treaties.

### Countering TCOs and Threat Networks: The Bottom Line

As many senior civilian leaders have said, there can be no doubt that TCOs represent a globally-networked national security threat. The corrosive effects of the threat posed by TCOs, the complex challenges associated with defeating them, and the abundant opportunities for progress underscore the vital importance of the U.S.'s close relationship with Mexico. Both countries share a responsibility to work against this threat alongside Canada, The Bahamas, and others in the hemisphere. USNORTHCOM personnel respect the patriotism, courage and resolve of the Mexican Government, Military, and Security institutions in their ongoing battle against the TCOs, and understand that this struggle is a long-term proposition, requiring continuous effort, creative solutions, and the assumption of some risk. Defeating TCOs and ensuring future security for the U.S. and Mexico means dismantling their networks and driving down their impacts to levels that can be handled by local law enforcement organizations, with full respect for Human Rights and the Rule of Law along the way.

It is important to highlight that this is not just about Theater Security Cooperation, or routine support of civil authorities. It is bigger than that—it's about Homeland Defense. Inside our borders, USNORTHCOM has unique military capabilities it can provide to assist the DHS, DOJ, and other civilian organizations and law enforcement agencies in the lead. Outside our borders, USNORTHCOM supports The Department of State, U.S. Embassy Country Teams, and other partners, understanding that it is not Americans helping Mexicans or other nations; it is us working together within a common problem frame toward common goals: regional prosperity, security, and economic development.

Mitigating the threat will require continued development of strategic security partnerships between those invested in the fight against TCOs and other threat networks. The foundation of this approach envisions an end state where the U.S. and Mexico are enduring strategic partners in regional mutual security (and other) interests.

Today, Mexico and the United States are strategic partners, respecting the laws and sovereignty of our individual nations, yet at the same time learning from each other and applying lessons learned from our experiences. While our Mexican colleagues share information about fighting transnational criminal organizations, as well as their expertise in providing humanitarian assistance and disaster response, we share our experiences in asymmetrical conflict and irregular warfare conditions in Iraq and Afghanistan.

#### NORAD and USNORTHCOM Theater Strategy (2012)

The U.S.—Mexico defense relationship has strengthened considerably since President Bush and President Calderon ushered in the Merida Initiative in 2007. Dialogue today between our militaries has grown into a strong cooperative defense relationship based on mutual trust and respect for each

country's national sovereignty. Two officers from the Mexican military serve in the USNORTHCOM headquarters in Colorado Springs, CO: one each from SEDENA (Mexican Army and Air Force) and SEMAR (Mexican Navy and Marine Corps). These officers serve as liaisons to their respective headquarters in Mexico, keeping open channels of communication and fostering new opportunities for continued defense cooperation between our nations. According to Mexico's *Reforma* newspaper, during the six-year term of former President Felipe Calderon, the Mexican and U.S. Governments signed 22 bilateral agreements, on topics of "intelligence, exchange of information, and training to face organized crime." (2012) There is much hope and expectation that this collaboration and trust-based partnership will continue to evolve and grow under the new Mexican Administration.

## Recommendations

In transnational criminal "Attack the Network (AtN)" operations, governments are often hindered by being organized along hierarchical lines, bureaucratic rivalry and competition, interagency antipathies, and a reluctance to share information and coordinate operations. To be as agile as the networks they confront, it may be necessary to form intergovernmental JTFs that pool resources and information (preferably on a regional basis) to pursue the network (Commander's Handbook, 2011, p. 107).

There are hundreds of good ideas about how to fight TCOs, and thousands of dedicated individuals focused daily on the threat; to be sure, progress has been made and the relationships between Mexico, the U.S., and others in the region are better than ever before. Nevertheless, what is perhaps ultimately required is a paradigm shift similar to that in scope and nature after 9/11. Today, existing legislation and authorities (and in many cases, a lack thereof) are often used as reasons for an inability to act; the U.S. post-9/11 epiphany stands as testimony that laws can be changed and organizations remolded to better suit critical national needs. Some examples of changes as a result of al-Qaeda's 2011 actions include the President's Surveillance Program; USA PATRIOT ACT; the creation of U.S. Department of Homeland Security and U.S. Northern Command; Intelligence Reform and Terrorism Prevention Act of 2004; and the FISA Amendments Act of 2008, just to name a few.

There are ways the U.S. can transition towards such change; one start would be to get out of the post-Cold War/pre-9/11 denial stage of this asymmetric conflict. Despite the numerous changes and significant transformation of yesteryear's drug cartels into the TCOs of today, much terminology and effort remains stuck in the Cali and Medellin era (a continuing focus on cocaine interdiction is too narrow, and insufficient). With North American criminals increasingly producing their own marijuana and heroin, manufacturing methamphetamine, and—again—continuing their expansion into other lines of crime, a shift in strategy as well as thinking is necessary.

Plenty has been written about how new programs in the tradition of the Merida Initiative should focus on training exchanges and information-sharing, rather than on equipment transfers; it is time to make these words reality in whatever bi-national and regional agreements the future holds. Buying boats for partners who can barely afford fuel (over \$15 per gallon in some parts of the hemisphere) is not always the best policy; conversely, sending equipment to peers who possess sound resources even as Americans struggle with our own financial restraints perhaps isn't the solution it once was. Even so, the

amount of resources applied should amount to more than symbolic gestures—with the limited multi-year Merida funds approximating that provided yearly to several other nations (e.g., Egypt), some overseas investments are worth analyzing when compared side-by-side with the potential benefits of spending within the Western hemisphere.

The U.S. should tread cautiously when comparing Mexico to Colombia and looking to the South or Central America of the past for textbook cut-and-paste solutions. There are lessons to be learned, to be sure, but problems remain in those regions and “Plan Colombia” is no panacea for defeating TCOs domestically. Prudence dictates pushing the horizon further and following Walter Gretzky’s advice, who once told his young hockey-prodigy son Wayne to “skate to where the puck is going, not to where it has been.” Hybrid threats, terror-crime nexus, innovative strategies...all merit further exploration to move us beyond the “war on drugs” dilemma. Seek to address what the world might look like in 2020-2025, and how individuals can help to best shape that to their nations’ advantage, rather than continuing to focus primarily on what is right around the corner in coming weeks and months.

Planners and strategists should strive to develop strategies that are comprehensive, whole-of-nation solutions and not “bad strategies.” The 2011 National Drug Control Strategy has some noble, specific, and attainable goals; however, once again, TOC will not be solved by counterdrug metrics alone. Yardsticks such as “decreasing the 30-day prevalence of drug use among 12- to 17-year-olds by 15 percent by 2015” do contribute to drug control, but will not adequately address the TCO threat—that will require a broader interorganizational approach, and sound strategy.

As Richard Rumelt (2011) wrote:

Too many organizational leaders say they have a strategy when they do not...Like a quarterback whose only advice to his teammates is ‘let’s win,’ bad strategy covers up its failure to guide by embracing the language of broad goals, ambition, vision, and values...[bad strategy] key hallmarks [include] four points: the failure to face the challenge, mistaking goals for strategy, bad strategic objectives, and fluff. Bad strategy [also includes roots such as] the inability to choose and template-style planning--filling in the blanks with ‘vision, mission, values, strategies.’ Crafting good strategies have a basic underlying structure: a diagnosis...a guiding policy...and coherent actions.

A holistic lens should focus on El Ponchis, not just El Chapo.<sup>10</sup> Catching or killing the leader of the Sinaloa Federation would no doubt be a significant morale boost and likely disrupt the operations of that criminal organization for a period, as did last year’s killing of Los Zetas leader Lazcano Lazcano. But when 14-year-olds are being recruited into TCOs and committing unthinkable acts like torturing and beheading people, more robust emphasis must be placed on the youth. The “ni-nis” (who “neither work, nor study”) today are easy fodder as “child soldiers” for the criminals; there is much more to be

---

<sup>10</sup>See also, <http://www.dailymail.co.uk/news/article-2019113/Teenage-gangster-El-Ponchis-14-jailed-Mexico-judge-beheading-people.html>

done to provide better options for this next generation.<sup>11</sup> The “3D” model of blended defense, diplomacy, and development must be better leveraged and applied.

There will be no truce or deals with organized crime or drug trafficking; there will be a full assault. But preventing violence and promoting economic and social development are part of a vicious cycle. Without better economic opportunity, you can’t have better public security, and vice versa.

Padgett, 2011

As frequently voiced by Mexican officials, not enough attention has been paid to drug demand reduction within the U.S. Many Americans shy away from this issue, fearing political ramifications and believing it to be “out of their lane,” and resources for such efforts are already stretched. Yet much could be accomplished in this area, and attention to it is especially critical given the challenging backdrop of the expanding legalization movement (witness states such as Washington and Colorado). Leaders should attempt to harness the power of celebrities and athletes to help stigmatize drug use, and—at a minimum—put forth effort at least comparable to that expended nationwide against tobacco use.

Increase emphasis on strategic communication and the use of social media. Al-Qaeda and the Taliban proved to be formidable adversaries in these areas, and TCOs are now doing the same. Strategic communication should rise to the level of main focus in many instances, rather than as a supporting effort with unachieved potential. Here, the “hearts and minds” of our publics are no less vital than of those overseas during counterinsurgency operations; citizens must be informed to understand, and care about, the complexities of TOC. Americans also need a better, more accurate understanding of Mexico today. In a recent survey of 1,000 U.S. adults, half of them had an unfavorable opinion of Mexico, only 17 percent viewed its economy as modern, and 72 percent thought the country unsafe as a travel destination—the same percentage who admitted that their negative views stemmed from the ongoing fight against the TCOs and related violence. When asked to list three words that describe Mexico, almost 50 percent said “drugs,” followed by “poor” and “unsafe.” Other responses showed that many Americans view Mexico as “corrupt, unstable, and violent...more problem than partner.” (O’Neil) Bi-lateral attention is required to help correct these inaccurate views.

The one-year-old U.S. defense strategy *Sustaining Global Leadership: Priorities for 21st Century Defense* (January 2012) does not mention Mexico, and much has been publicized recently about America’s rebalancing to the Asia-Pacific region. Nevertheless, homeland security must remain a top priority, and TCOs are intertwined in regional concerns that directly impact the homeland. Resources must meet the demands of the threat, balanced against the real risk of inadequate action, when funding decisions are made to counter these tangible dangers to American peace and prosperity.

---

<sup>11</sup> One simple example is former President Bill Clinton partnering with Mexican mogul Carlos Slim in 2011 to launch a Mexican youth soccer program, “A Ganar.” The U.S. should encourage initiatives such as this, and broaden their reach.

Consider unorthodox approaches. Some have forecasted a shift in security contractors from Southwest Asia to Mexico, as opportunist companies seek to fill the demand official government representatives have been unable to meet (Miroff, 2012). Similarly, several businesses in Mexico have reached their tipping point and are beginning to rise up against the TCO scourge. These corporate organizations are helping to fund police recruiting, paying for government redevelopment plans, and “injecting money into community groups and sponsoring school programs.” (Malkin, 2012) Ensuring that Mexico remains in the lead in their country, government representatives from both nations should cooperatively coordinate with these groups to synchronize efforts and prevent additional stovepipes from developing; otherwise, increased, counterproductive vigilantism is possible.

Finally, the way ahead cannot be simply more of the same. Effective efforts against TCOs must include a comprehensive Counter Threat Network approach, whole-of-government and whole-of-societies collaboration, and possibly even new structures (e.g., the often debated “Joint Interagency Task Force, North” (JIATF-N)) and agreements (e.g., the Mexican-led “Hemispheric Scheme Against TOC”/Chapultepec Consensus). Step one is to honestly recognize these TCOs as the threat to homeland security they truly are. Step two is accepting that to defeat these networks, we’ll need to become a better network ourselves.

## Chapter 1 C: USPACOM Perspective on Transnational Organized Crime

Mr. David Hallstrom

JIATF West

Mr. Tom Wood

JIATF West

Mr. Chris Isham

[christian.isham@jiatfw.pacom.mil](mailto:christian.isham@jiatfw.pacom.mil)

USPACOM

The U.S. Pacific Command (USPACOM) Area of Responsibility (AOR) is culturally, socially, economically, geographically, and geo-politically diverse. The 36 nations in the AOR comprises 50 percent of the world's population, speaking and writing three thousand languages. More than one-third of the Asia-Pacific nations are smaller, island nations. Transnational non-state threats include pirates, terrorists and criminal organizations involved in a wide array of criminal enterprises to include drug and precursor chemical smuggling, human trafficking, counterfeit goods smuggling, money laundering, and document fraud. Permissive environments, loose financial controls, widespread corruption and fraudulent document facilitation networks fostered by Transnational Organized Crime (TOC) are key enablers for the freedom of movement of international terrorist and criminal organizations operating throughout the USPACOM region. Additionally, Pacific Island nations face a particularly challenging security environment as large numbers of remote islands, vast Exclusive Economic Zones (EEZ), low national budgetary resources, and a scarcity of law enforcement resources all work against counter transnational crime efforts.

Transnational Criminal Organizations (TCOs) have attained a level of sophistication and activity that can threaten national sovereignty and international security in a variety of ways. While TCO's pose broad challenges to nation-state power and interests across the Asia-Pacific, the specific issues vary somewhat by sub-region.

Globalization continues to internationalize the once regional or local organized crime and allow criminals to become more entrepreneurial and market-focused. These organizations continue to evolve—and as the global economy continues to grow, change, and innovate, so will criminal organizations, enabling them to react quickly to changes in both licit and illicit economies.

Criminal groups seem to be evolving towards a business model based on loose associations of individuals or small groups operating independently. They interact with one another, sharing expertise, skills, and resources to successfully conclude specific criminal ventures, and then disassociate and move on to other ventures with other "partners." These criminal networks

transcend national boundaries and, due to their fluid nature, are difficult to identify and target. They benefit from compartmentalization, which makes it possible for a network to operate without a single person in command of the entire enterprise.

Within Asia, ethnic Chinese are the backbone for most organized crime, but increasing involvement of Mexican, Iranian and West African organizations in the region is of growing concern. Of the four named organizations in Executive Order 13581, two are currently known to operate in the Asia-Pacific region— Yakuza, and Brother's Circle. Also, while the general trend is toward self-organizing networks, loosely affiliated groups forming and re-forming as business opportunities dictate—there is still a degree of regional affiliation. Some of this is due to historical precedent, and some due to market specialization.

In the USPACOM AOR, the drug arm of transnational crime is vibrant, expanding, and has both a solid supply and demand base. No sub-region of this AOR is free from drug-related threats. Production of industrial chemical precursors; manufacturing of designer drugs; Amphetamine-Type Stimulant (ATS) production; heroin abuse; marijuana production, trafficking, and abuse; and, cocaine trafficking and abuse are all prevalent to varying degrees throughout the region. TCOs operate freely across national (and DOD CCMD) boundaries linking one country or region's drug with another's drug users.

For example, a network of criminal activity that provides Mexican meth labs with industrial amounts of Asian-sourced precursor chemicals—primarily from India and China—plays a critical role in the production of methamphetamine produced in Mexico and sold in the U.S. This Asia-sourced and Mexican-trafficked methamphetamine comprises approximately 80 percent of all methamphetamine consumed in the U.S. Methamphetamine use in the U.S. is now approaching cocaine usage (DOJ, 2011). According to U.S. Customs and Border Protection (CBP) data, the amount of methamphetamine seized along the southwest U.S. border has significantly increased since 2008 and is nearing the amount of seized cocaine, which has been declining since 2009 (JIATF, 2012). Moreover, cocaine shipped from the Western Hemisphere and sold in extremely lucrative Asia and Australia markets also serves to help finance the power and influence of Latin American cartels.

Many of the well-established organized criminal groups not previously involved in drug trafficking—including those in Russia and China— are now establishing ties to drug producers to develop their own distribution networks and markets. Heroin produced in Afghanistan is regaining measurable fraction of the U.S. heroin market and is also flowing into both Europe and Asia. TCOs connect methamphetamine production facilities in Iran and Africa with users in Southeast Asia, Oceania, and Northeast Asia.

Generally, there is not a proven nexus between organized crime and terrorism in the Asia-Pacific region with the exception of "D-Company" in South Asia. Dawood Ibrahim, an Indian national, has for over three decades led a criminal organization extensively involved in international crime and terrorist facilitation and has contributed to friction between the governments of Pakistan and India.

The major terrorist groups in Southeast Asia, such as Abu Sayyaf Group (ASG); Jemaah Islamiyah (JI); Moro Islamic Liberation Front (MILF); and New People's Army (NPA) rely on varying degrees of criminality to finance their operations, but are not generally considered to be significant players in the transnational crime arena. That said, the permissive environments, loose financial controls, corruption, and fraudulent document facilitation networks fostered by transnational organized crime are key enablers for the freedom of movement of international terrorist organizations operating in the region.

#### **Sub-Regional Challenges: Northeast Asia**

This sub-region encapsulates some of the largest global population centers and some of the most affluent countries and vibrant economies. In this region, Eurasian, Chinese, and Japanese TCOs intermingle to meet the drug demands of the region.

China has recognized its heroin problem, growing ATS problem, and potential for increased cocaine trafficking. Drug abuse is found amongst the impoverished, middle class, and urban rich alike. The historical Triad presence is pervasive, versatile, and resilient.

Japan is home to a well-established and historic TCO—the Yakuza. Yakuza are involved in a wide range of criminal activities. From a drug perspective, demand in Japan for methamphetamine, primarily amongst the business class, has created the most lucrative methamphetamine market in the world.

North Korea's likely ongoing relationships with criminal organizations engaged in counterfeiting of currency, drug production, weapons proliferation etc. remains a problem (White House, 2011). The unknowns associated with the North Korean regime potential and desire to support drug production and trafficking makes the northeast Asia drug picture much more complex—especially given the other strategic challenges associated with North Korea (nuclear weapons, technology proliferation, etc.).

#### **Sub-Regional Challenges: Southeast Asia**

This sub-region is characterized by pervasive drug abuse problems and persistent TCO presence. The historic abuse of heroin, opium, and marijuana continues at some level in every country. Trafficking of methamphetamine pills, especially amongst the urban poor, and the production of crystal methamphetamine has made synthetic drug abuse the recognized primary drug threat. Thailand, Philippines, Indonesia, Malaysia, and Vietnam all have significant ATS abuse populations. Burma, Cambodia, and Laos are primary regional production areas for methamphetamine and ecstasy; however, production also occurs in Indonesia, Malaysia, and the Philippines to meet local domestic demand. Cocaine is no longer just a transshipment concern but is now abused by the wealthy.

Chinese and Burmese TCOs work together to move needed precursor chemicals to drug production facilities along the headwaters of the Mekong River, an important waterway. These TCOs work with

regional and local crime elements to move finished drugs back into China and to users in countries along the Mekong River.

Eurasian organized crime is establishing a presence in Thailand, and while that presence is not currently focused on drugs, the prevalence of drug use in Thailand and the international trafficking routes both offer lucrative drug-related investment opportunities. Although at a nascent stage, there is evidence that Mexican TCO's are making inroads in the Philippines as well.

### **Sub-Regional Challenges: Oceania**

Australia and New Zealand are the richest countries in Oceania and host some of the highest per capita consumption rates in the Asia-Pacific for methamphetamine and ecstasy. The cocaine market in Australia remains one of the most lucrative in Asia. Both Australia and New Zealand successfully control the movement and sale of precursor chemicals, though this has driven precursors out of the licit sphere and into the illicit networks; the same illegal networks which move ATS, cocaine, heroin, and marijuana. Local gangs and outlaw motorcycle gangs work with traditional Asian organized crime elements to operate these networks.

The Pacific Island states are beset with poor legislation, infrastructure, and enforcement capacity to counter drug-related transnational crime. These states also have a low rate of accession to international drug control treaties, and are increasingly becoming destinations and transshipment points for trafficking of drugs and precursors. This inability to comply empowers criminal organizations to conduct drug-related crime in Oceania with low chance of disruption. Vast territories, low population density, and low national budgetary resources all further work against counterdrug efforts.

### **Methamphetamine Production and Trafficking**

The two primary areas of methamphetamine production in the AOR are southern China and the Shan state in Burma. TCOs in China generally produce methamphetamine for markets in North Asia while Burmese drug trafficking organizations (DTOs) generally produce methamphetamine for markets in mainland Southeast Asia. The Philippines produces a significant amount of methamphetamine. This production exists primarily for local consumption, but some quantity is transshipped north to Taiwan and Japan. Additionally, African Drug Syndicates and Iranian DTOs traffic large amounts of methamphetamine into the region from western Africa and the Middle East. Some reporting exists of Iranian drug traffickers either producing crystal methamphetamine or converting liquid methamphetamine into crystal methamphetamine in Southeast Asia in order to defeat law enforcement scrutiny.

Regional drug flow in Asia moves primarily across the land borders between Southeast Asian countries and in to Southern China. Methamphetamines and other drugs are also transported by maritime cargo, fishing vessels and by couriers traveling on commercial airlines.

## Cocaine Flow from the Western Hemisphere

Chinese-based and other TCOs, working with Asian distributors and drug suppliers from Latin American countries, traffic cocaine from the Western Hemisphere to the Asia-Pacific region via maritime commercial container shipments and/or small craft such as fishing vessels and private yachts. TCOs also use human couriers and exploit aviation and shipping sectors. Efforts to close existing intelligence gaps and disrupt the scope and magnitude of this drug trafficking activity continue. Despite increases in usage in recent years, cocaine is not expected to overtake methamphetamine and ATS in the foreseeable future as the drug of choice in the Asia-Pacific region.

## AA and Heroin Production/Distribution

Opium cultivation in Southeast Asia's "Golden Triangle" has declined dramatically in the last 20 years (decrease of approximately 85 percent) and shifted to Afghanistan, where the vast majority of the world's opium is grown (United Nations, 2012). In Afghanistan, the proceeds from heroin production and trafficking help fund and sustain the Taliban. Who have reportedly earned up to \$1.6 billion from heroin in the last decade. Asian producers and distributors of acetic anhydride (AA) fuel Afghanistan's massive heroin production. China and India are significant sources for AA in Afghanistan. Although Afghanistan has no legitimate industrial use for AA, as much as 1,500 metric tons of AA is consumed annually in that country for the production of heroin. Traffickers rely on weak regulation and enforcement capabilities present in the various countries within the USPACOM AOR to circumvent barriers to consumer markets abroad. Transshipment points of interest within the region include South Korea, Japan, Pakistan, India, Nepal, and Bangladesh.

## Countering the Threat

While DOD lacks law enforcement authorities to counter TOC, it does possess certain counternarcotics authorities to assist law enforcement agencies in the fight. In the USPACOM AOR, Joint Interagency Task Force West (JIATF West) uses those authorities to apply DOD capabilities in a whole of government approach to combat transnational crime.

As USPACOM's executive agent for counternarcotics, JIATF West plays a key role in achieving the USPACOM Strategic End State and supporting national policy goals throughout the region. JIATF West conducts operations and activities to disrupt and degrade the national security threats posed by drug trafficking, piracy, transnational organized crime, and threat finance networks reasonably related to illicit drug trafficking activities (DOD Counternarcotics, 2011, pp.4-5).

Although limited to a counternarcotics nexus, JIATF West's approach has been to focus on disrupting the drug-related TCOs, while also shaping the environment to enable partner nations to assist in the global effort against them. Taking the whole of government approach in support of law enforcement agencies has helped build a cooperative partnership of networks to counter transnational organized crime.

## Chapter 1 D: Transnational Organized Crime: A USSOUTHCOM Perspective

Ms. Renee Novakoff et al.

[renee.novakoff@hq.southcom.mil](mailto:renee.novakoff@hq.southcom.mil)

USSOUTHCOM

### Introduction

In broad terms, TOC represents a threat to our national interests. This day-to-day, low-level insidious and pervasive criminal activity slowly penetrates societies and ultimately threatens governance and security. This is a global threat that impacts every geographic combatant command but in this hemisphere the criminal activity—which is more than narco-trafficking, also includes gang activity, special interest alien trafficking, money laundering, and arms trafficking—has direct links to the U.S. In addition, in this region TOC is both a cause and effect of broader issues that have the potential to destabilize the region. Weak government institutions, under-resourced and hampered by corruption, have limited reach into the furthest corners of society, allowing TCOs to operate with impunity. Weak government presence and scarce legitimate economic opportunities entice citizens to cooperate with TCOs for security and economic well-being, further eroding legitimate governance and social and political foundations. We could be left with a blend of a criminal organization de facto running a weak state on our southern flank.

The convergence of TOC and asymmetric threats is a critical U.S. national security concern. The potential exists for cooperation between TCOs and terrorist groups. Without a doubt, the degree of overlap between TCOs and terrorist organizations is difficult to determine. There is not sufficient evidence of on-going cooperation between these two groups. Nevertheless, it is clear that the region's terrorist groups, such as the FARC, are involved in TOC as a way to generate revenue, even though they do not necessarily intend to directly target the U.S. Department of Treasury has also designated individuals in this hemisphere who are associated with Hezbollah as drug kingpins, underscoring the ties between terrorist and drug trafficker.

Current trends show TOC groups and networks growing in power and becoming national security threats throughout the region. This is not a force on force threat but one that is more insidious. These borderless groups infiltrate government institutions to create, for themselves, space from which to carry out illicit activities. These networks threaten to destabilize regional governments not by direct means but through behind the scenes attempts to gain space to develop their illegal businesses. These networks also have ties to the U.S., threatening its citizens by bringing violence to the streets of the U.S. and potentially its economic infrastructure by infiltrating illicit activities into American banking and business systems. The scale of TOC enterprises, the impact they have on legal economies, and their prospective continued growth argues for sustained national and international attention and resources (Farah, 2012). To understand and counter these threats, the U.S.

government will need to work across interagency lines. This will take new organizational constructs and relationships that are not wedded to parochial border norms.

## Background

Over the past ten years, TCOs have grown in importance and influence globally, including throughout Latin America and the Caribbean. Moises Naim, in his book *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy*:

Today more than ever, these structures have the capacity to operate on a global scale, connecting remote places of the planet and the most cosmopolitan cities, above all, with accumulated political power. Never have criminals been so global, so rich, or have so much political influence.

In Latin America, TOC networks will continue to grow and, in the worst cases, work with and corrupt government institutions to form an alliance that gives the TOC space to do business, significantly affecting societies. Public insecurity is pervasive, growing and supportive to further TOC encroachment. In nearly every country in the region, polls have shown that the population considers personal security as its number one concern. Across the region, murder rates are generally higher than they were ten years ago. The relationship between TOC and gangs is growing and is challenging nascent democratic institutions across the region.

As the only producer of cocaine in the world, and the primary transshipment zone for illicit trafficking to the U.S, and South and Central America is the epicenter of transnational crime activities. The problem is particularly acute in the “Northern Tier” countries of Honduras, Guatemala, Belize, and El Salvador, where criminal networks exploit weak rule of law, corrupt officials, and porous borders to traffic in drugs, precursor chemicals, weapons, people, and bulk cash. In all four countries, gangs and other violent criminal groups are contributing to escalating murder rates and deteriorating citizen security. This has overwhelmed civilian law enforcement departments and court systems, many of which are chronically under-resourced and challenged to develop practiced transparency and credible prosecution records.

Challenges faced by the “Northern Tier” countries are further exacerbated by the economic power wielded by criminal groups. The value of cocaine destined for sale dwarfs the security and defense budgets in the sub-region and allows significant criminal penetration into governmental organizations, including security forces and judicial systems, as well as legitimate financial networks. The overall value to these criminal networks from the cocaine trade alone is more than the gross domestic product (GDP) of every country in Latin America except Brazil.

Criminal networks’ access to regional governments is gaining momentum and even leading to co-optation in some states and weakening of governance in others. The nexus in some states among these networks and elements of government and big business figures threatens the rule of law. New

communications technologies have led to new criminal business models of widely distributed, constantly shifting networks of personal contacts and fleeting alliances to produce, market, transport, or distribute illegal trade. These networks are willing to deal in drugs, human beings, sometimes extortion, kidnapping, counterfeiting or whatever activity turns a profit (Killebrew).

### Pushing Back on TOC

The 2010 National Security Strategy acknowledges the challenge these organizations pose and that combating transnational criminal and trafficking networks will require a “multidimensional strategy that safeguards citizens, breaks the financial strength of criminal and terrorist networks, disrupts illicit trafficking networks, defeats transnational criminal organizations, fights government corruption, strengthens the rule of law, bolsters judicial systems, and improves transparency.” (National Security Strategy, 2010, p. 49) To help mitigate transnational crime in this hemisphere the U.S. needs to help improve Latin American and Caribbean domestic institutions and coordination across all their institutions—ranging from the law enforcement and judicial sectors to education.

A key to countering TCOs is to understand associated networks or the supply chain. Major crime groups such as Mexican cartels or Colombia’s FARC contract with smaller, local criminal organizations that move goods. These are important elements of the network but little is known about them. These franchises operate in, and control, specific geographic territories, which allow them to function in a relatively safe environment. These pipelines, or chains of networks, are adaptive and able to move a multiplicity of illicit products (cocaine, weapons, humans, and bulk cash) that ultimately cross U.S. borders undetected thousands of times each day. The actors along the pipeline form and dissolve alliances quickly, occupy physical and cyber space, and use both highly developed and modern institutions, including the global financial system, as well as ancient smuggling routes and methods (Farah, 2012). They are middlemen who have little loyalty to one group and often have no aspiration to develop their organization into a major trafficking network. They make a living by moving goods and ensure which families are safe from the TOC group who threatens to kill those who do not assist them.

More so than any other problem the U.S. faces, this particular challenge blurs the line among U.S. institutions. The size, scope, and reach of transnational criminal networks far surpass the ability of any one agency or nation to confront this threat. In Central America, increasing military involvement in domestic security is a reality, at least until this threat is degraded and the capabilities of civilian police institutions are expanded. This effort will require the commitment of Latin American governments and their societies to build the capacity of their law enforcement, judicial, and penal organizations. It will require their commitment to address endemic corruption throughout their societies. Moreover, it will require their commitment to engage regional and international institutions to enhance coordination and cooperation—supporting the development of national and regional security plans, enhancing regional defense and security institutions, and building capacity to operate in accordance with human rights principles.

Further, it will take concerted collaboration and sustained commitment by the U.S. and the international community—both governmental and non-governmental organizations—to address this complex problem. Innovative approaches, creative public-private collaborations, and synchronization of efforts between numerous U.S. federal agencies—DOD, Department of State (DOS), DEA, United States Agency for International Development (USAID), and DHS—will be necessary to create a cooperative national and international network that is stronger and more resilient than any criminal network. Key to success will be information sharing within the U.S. interagency community and with our partner nations.

### **A Way Ahead**

The 2011 national strategy to combat TOC applies all elements of national power to protect citizens and U.S. national security interests from the convergence of twenty-first century transnational criminal threats. This strategy is organized around a central unifying principle: to build, balance, and integrate the tools of American power to combat TOC and related threats to national security and to urge foreign partners to do the same.

Operations that create a vacuum in TOC operations and businesses should be paired with aggressive non-law enforcement engagement and social services in a coordinated fashion. This type of coordination requires agencies beyond law enforcement and DOD, from both the country itself and from international contributors.

### **Role of DOD in Combating Transnational Organized Crime (CTOC)**

First, DOD is a supporting agency to the interagency. DOD is the lead in detection and monitoring of illicit trafficking but can also offer significant advantage in terms of building partner capacity and network analysis. DOD nests many of its activities within the Central American Regional Security Initiative (CARSI) framework, directly supporting the disruption of criminals and trafficked contraband through detection and monitoring, interdiction support, training and equipping of partner nation militaries, network analysis, and information sharing. Specifically, the DOD's Counter Narcotic and Global Threats (CN&GT) Strategy outlines DOD's roles in countering illicit threats, including illicit trafficking and TOC. The strategy outlines several strategic goals and objectives in which DOD—as the single lead federal agency for detection and monitoring of aerial and maritime transit of illicit drugs in the US and an important contributor to national efforts to counter TOC—conducts operations and activities to disrupt and degrade the national security threats posed by drug trafficking, TOC, and threat finance.

DOD's role in C-TOC generally falls into the following supporting lines of effort includes the following.

- Detection & Monitoring
- Counternarcotics training
- Counternarcotics support
- Defense Equip (FMF/FMS)

- Defense Training (IMET)
- Defense Institution Building
- Human Rights Training
- Multinational Training Exercises
- Defense Engagement
- TOC Network Analysis and information sharing.

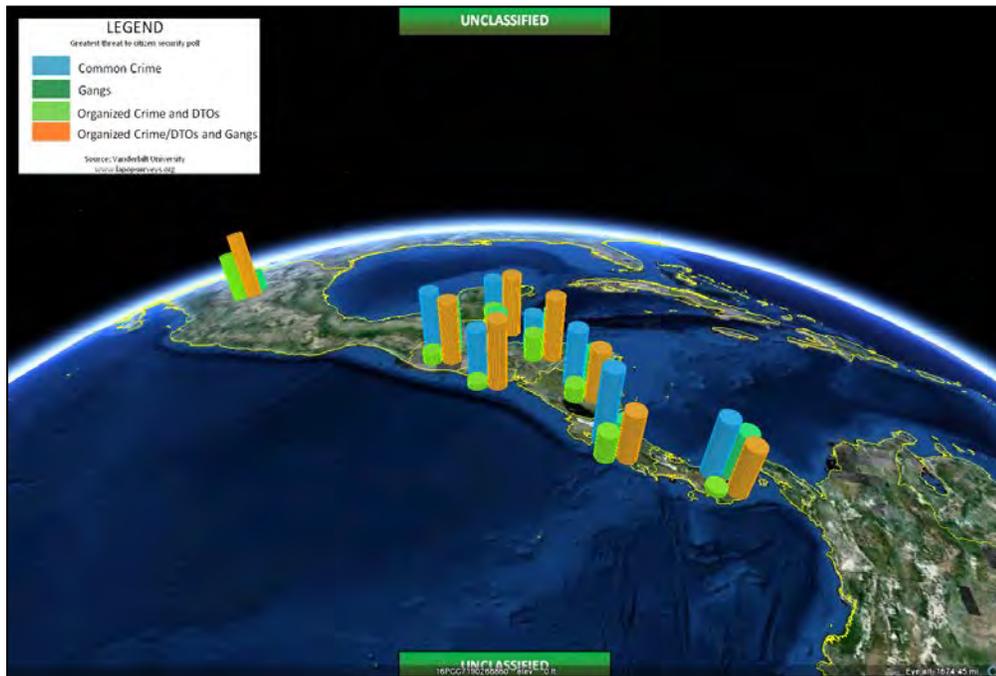


Figure 1: Example of WISRD layer. Depicts violent crime throughout Central America and Mexico

With the exception of the first mission set, helping partner nation's build and sustain their security capacity is *one* key component of all DOD C-TOC efforts.

### **SOUTHCOM's Approach to Countering Transnational Organized Crime (C-TOC)**

In accordance with the objectives outlined in DOD's CN&GT strategy, SOUTHCOM supports U.S. government efforts to:

- Reduce the quantity of illicit drugs entering the U.S. through Central America;
- Disrupt illicit trafficking and TCO operations in Central America; and
- Work with other government agencies and Departments to build the capacity of Western Hemisphere partners to deny TCO's the use of their territory, airspace, and surrounding sea lines of communication.

Since January 15, 2012, Joint Interagency Task Force South (JIATF-S), in support of U.S. Southern Command, has been leading Operation MARTILLO, a Western Hemisphere and European partner

nation effort that aims to shift maritime illicit trafficking away from the Central American littorals. To conduct this operation, U.S., Partner Nation, and allied forces' ships and aircraft are providing persistent presence in select maritime zones.

The need to help partner nation's build capacity cannot be overstated. There are significant capacity problems that can be addressed by military engagement and cooperation, which can have substantial short-to-mid term impact in creating conditions for deeper reform and progress. These would include improving border security and improving partner nation military capacity to support law enforcement to disrupt and interdict movement and transfer of illicit products.

Finally, one of the continuing and important roles of the U.S. military in supporting the effort to CTCO networks is intelligence analysis and information sharing throughout the region. The U.S. Southern Command's Whole-of-Society Information Sharing for Regional Display (WISRDR) program was developed to create a whole-of-society, enterprise process capability that provides participating organizations with a comprehensive common visualization of the TOC environment to satisfy a range of agency information requirements. WISRDR promotes the "responsibility to share" not only with the U.S. interagency but allows users to reach out and share information with non-traditional "whole-of-society" partners to include the academic and business communities. The WISRDR environment brings a more holistic approach to understanding the criminal activities.

## Summary

TOC is a global threat and a direct threat to western hemispheric stability and therefore a threat to U.S. national security interests. The U.S. needs to continue its efforts of thwarting the negative influence of TOCs in the region. DOD has an important supporting role in this effort. Building the capacity of American partners to exercise their territorial sovereignty is crucial. The improvements need to be targeted holistically from civil law enforcement and judicial reforms to the capability and capacity of their respective defense organizations. In addition, information sharing in the U.S. and among its partner nations will be a key facet of countering these groups. Stove piping information helps the enemy. The U.S. government must develop a new prism from which to confront this new type of enemy that has no boundaries.

## Chapter 1 E: Stronger Together: Building EUCOM's Network to Combat Organized Crime in Europe

BG Mark Scraba

Mr. Todd Trumpold

[todd.r.trumpold.civ@mail.mil](mailto:todd.r.trumpold.civ@mail.mil)

Joint Interagency Counter Trafficking Center, USEUCOM

### The New Face of an Old Enemy: the Impact of Organized Crime on State Security in Eurasia

Although TOC has been a recent topic in national security circles, the threat posed by organized criminal organizations is not new to U.S. European Command's (EUCOM) area of focus.<sup>12</sup> Located at the heart of a historic crossroads between Europe, the Middle East and Asia, this region has been both a key global transit zone and destination for illicit trafficking in drugs, weapons, human beings, and a host of other illicit commodities for centuries. Indeed, the Sicilian Mafia—synonymous throughout the world with organized crime—began here nearly 200 years ago (FBI, February 2013).

Since the early 1990s, however, globalization has turned the region into critical “turf” for some of the world's most powerful organized criminal organizations. Italian organized crime syndicates, such as the Sicilian Mafia, Camorra, Ndrangheta, and Sacra Corona Unita, have expanded their activities. The Federal Bureau of Investigations (FBI) estimates that these four groups have 25,000 members and 250,000 affiliates worldwide (FBI, February 2013). In addition, new, powerful organized criminal groups have emerged out of the former Soviet Union and Eastern Block countries. Recently, the U.S. Treasury designated several members of one of these groups, “The Brothers’ Circle,” for sanctions under E.O. 13581 (Treasury, 2012). Lastly, EUROPOL has reported an increase in Mexican drug cartel activity in Europe, as European organized criminal organizations are seeking ways to facilitate the movement of cocaine into Europe (European Monitoring Centre for Drugs and Addiction, 2013).

The growth of organized crime in Europe has been fueled by Europe's role as a central hub in the global economy. The volume of commercial goods transiting Europe every year is staggering. For example, over 15,000 container ships moved over 182 million tons of cargo through the port of Antwerp, Belgium, in 2011 (Port of Antwerp). Increasingly, many of these containerized shipments contain illicit drugs. EUROPOL has reported an increase in the use of containerized shipments for both heroin and cocaine smuggling (European Monitoring Centre for Drugs and Addiction, 2013). Indeed, in October 2012, Belgian authorities seized one of the largest shipments of cocaine to Europe: 8,000kg of cocaine valued at €500 million was concealed in a shipment of bananas from Ecuador (The Holland Times, 2012). As EUCOM's Commander, ADM James Stavridis has stated, these activities represent the “dark side of globalization” and signal a security issue for EUCOM.

---

<sup>12</sup> EUCOM's area of focus (also referred to as area of responsibility) covers 51 countries spanning Europe, Russia, and the Caucasus, including Israel, see <http://www.eucom.mil/mission/the-region> for more information.

The price for illicit drugs sold in Europe is as startling as the volume. A kilo of South American cocaine may cost three times as much on the wholesale market in Europe as in the U.S. (Keefe 2012). The United Nations Office on Drugs and Crime (UNODC) assesses that the average price for a kilo of cocaine in Europe was approximately \$53,000 in 2010 (Cocaine and Heroin Prices in Europe, 2013). Drug trafficking organizations can make a substantial profit at that price when one considers that the same kilo of cocaine may cost only \$2,000 in Columbia or Peru (Keefe, 2012).

Although the sale of illicit drugs is the most lucrative activity for organized crime, it is not its only source of revenue (UNODC b). In recent years EUROPOL has noted a trend in organized criminal groups diversifying their illicit activities (EUROPOL, 2011) For example, organized criminal groups are heavily involved in human trafficking—the financial exploitation of men, women and children for forced labor or prostitution. UNODC estimates the trafficking of women and children in Europe for sexual exploitation generates \$3 billion dollars annually and involves approximately 140,000 victims at any one time (UNODC b). In addition, the illegal smuggling of immigrants from Africa to Europe brought in approximately \$150 million dollars in 2008 (UNODC b).

The proceeds from the illicit activities of organized crime are significant. UNODC estimates that TOC generates approximately \$870 *billion* a year, which is equivalent to 7 percent of the world's exports in merchandise (UNODC b). Just one of the organized criminal groups in Italy, the Camorra, is assessed to earn roughly \$25 billion a year (U.S Department of Justice, 2008). Moreover, the revenues from illicit activities fund other groups, which pose threats to national security. For example, a 2011 UN estimate indicated that the Taliban made more than \$150 million in 2009 through the sale of opium (UNODC, July 2011).

Indeed, it is the magnitude of these illicit revenues in Europe that poses the greatest national security threat. How these proceeds create a national security threat is discussed in greater detail elsewhere in this publication, but perhaps the important aspect of this financial activity is the ability of organized crime to use these funds to foster the spread and development of further illicit activity (UNODC, 2010 at 99). A study of criminal cases in the Netherlands found that criminals “reinvested” 25 percent of their revenue from illicit activities in other irregular business activities and an additional 57 percent in “conventional investment (real property, securities, etc.) (UNODC, 2010 at 99). The impact from the flow of these illicit funds is extensive and varied. Not only does it allow criminal organizations to fund other illicit activities, such as cyber crime, the investment of illicit funds distorts prices, consumption and exports, as well as skews competition (UNODC, 2010 at 109). Most importantly, organized crime's ability to control these substantial sums of money promotes corruption, which can destabilize governments and undermine the rule of law. As an example, in 2012, the Italian cabinet invoked its special powers to dismiss the entire city government of Reggio Calabria, a provincial capital of approximately 180,000 residents, after it was discovered that several members of the council had ties to the Ndrangheta, one of the most powerful organized crime groups in Italy (Donadio, 2012).

The scope and magnitude of the threat posed by TOC demands a transnational, cross-organizational response. No longer can local or national law enforcement agencies address the threat alone. Data

from a variety of organizations across the globe must be shared to identify criminal networks and activities. Moreover, intelligence and law enforcement actions must be coordinated between organizations and across jurisdictions to efficiently counter organized crime's global activities. DOD should be a key contributor to this whole-of-government response, given its global reach, as well as its unique and substantial resources. The challenge remains how best to integrate it.

### **Expanding the Alliance: Establishing U.S. Military-Civilian Collaboration Against Organized Crime in Eurasia**

To address the rising threat posed by organized crime, as well as the issue of illicit trafficking, EUCOM established the Joint Interagency Counter-Trafficking Center (JICTC) in September 2011 (U.S. European Command, 2013). Comprised of military and civilian program managers and analysts, the JICTC's mission is to support U.S. Joint Interagency and U.S. embassy country team efforts to counter transnational illicit trafficking and to assist European and Eurasian nations in building counter trafficking skills, competencies and capacities to defend the Homeland forward. The JICTC is the only U.S. Interagency-DOD organization in Europe dedicated to implementing the President's Strategy to CTOC.

Despite consensus on the need for cooperation, U.S. military collaboration on issues pertaining to organized crime is challenging in the EUCOM focus area. The initial task of determining where to employ JICTC's limited resources can be overwhelming. The EUCOM area of focus— comprised of 53 countries—is a patchwork of national, state and local law enforcement organizations. The JICTC's ability to assist law enforcement at each of these levels and in each of these countries varies greatly and is influenced by a wide range of factors, such as partner nation laws, capabilities, willingness to combat organized crime, corruption, and political relations with the U.S. In addition, there are legal and cultural restraints in Europe to U.S. military assistance to European law enforcement. As in the U.S., combating organized crime is primarily the mission of law enforcement, but because of the domestic activities of some European militaries during WWII, there is reluctance in many countries for military assistance in law enforcement activities. In some instances, there are even statutory limitations regarding military involvement in domestic.

For these reasons, the JICTC operates in partnership with and in support of other U.S. government agencies and organizations. These organizations include the DOS, U.S. Treasury, FBI, DEA, Homeland Security Investigations (HSI), CBP, DOJ, Department of Energy (DoE), and USAID. In addition, the JICTC works in support of Country Teams at U.S. embassies as well as with U.S. government representatives at other locations, such as CBP officers located at key European ports of entry. These representatives typically can identify more easily how the JICTC can support efforts against organized crime. This is in large part because their organizations are already engaged with partner nation law enforcement on these issues. Moreover, these representatives can serve as the "face" of JICTC efforts, interfacing directly with their law enforcement counterparts and acting as a conduit for JICTC support, such as training, funding and analysis.

In its first two years of operations, the JICTC has had success in two broad areas of activities:

1. Collaborative partner capacity building efforts; and
2. Analytical support to U.S. law enforcement investigations and administrative actions.

JICTC partner capacity building efforts have focused on training partner nation law enforcement organizations and improving partner nation facilities and technical capabilities. Some of examples of recent JICTC capacity building projects include the following.

- The JICTC and CBP have worked together to train law enforcement organizations in border security techniques and to improve partner nation border management systems.
- The JICTC and the Justice Department's International Criminal Investigative Training and Assistance Program (ICITAP) have trained law enforcement organizations on the collection of evidence for criminal investigations, informant management, as well as surveillance techniques.
- The JICTC has provided analysts and translators to support law enforcement investigations against transnational organized crime, which resulted in the arrests of transnational organized crime members.
- In Romania, the JICTC sponsored the renovation of the Southeast European Law Enforcement Center (SELEC) to support collaboration between regional law enforcement agencies.
- The JICTC is supporting ICITAP in developing a new crime laboratory computer Information Management System for a law enforcement organization in Eastern Europe.

JICTC's analytical products are narrowly tailored to meet the ongoing efforts of other U.S. government organizations, in particular U.S. Treasury, HSI, and DEA. JICTC analysts provide information, build nomination packages for administrative actions, and secure the release of information to partner nation law enforcement organizations. Over the past two years, the JICTC's analytic activities have included:

- Supporting U.S. Treasury investigations to track and stop illicit fundraising;
- Creating nomination packages on drug kingpins and criminal organizations for U.S. Treasury sanctions and seizures of assets; and
- Providing Homeland Security Investigations information on the possible procurement of U.S. technologies that are prohibited from export.

As the organization matures and expands its network, JICTC continues to identify new areas in which it can assist in building partner capacity and providing analytical support. In the coming years, JICTC expects to focus its efforts on the Balkans and the flow of drugs from Central and South America to Europe.

## Learning to Play Their Game: Developing the Tools, Practices and Authorities to Combat Organized Crime

America's War on Drugs, and more recently the War on Terror, have gone a long way to prepare DOD for a larger role in supporting efforts to counter organized crime, but improvements in at least three key areas are needed for DOD to fully apply its capabilities. First, training programs should be developed to educate DOD analysts and planners on how organized criminal groups operate and how law enforcement and other governmental groups counter organized crime. Over the last decade, DOD has developed numerous programs and systems to perform social network analysis in order to identify and map terrorist networks. But, organized criminal organizations and terrorist groups are different. At the most fundamental level, organized criminal organizations are motivated primarily by profits, and terrorist groups are motivated by ideology or political agendas. Moreover, international efforts to counter organized crime differ from counterterrorism efforts. Broadly speaking, individuals supporting activities to counter organized crime must be more familiar with the needs of and limitations on law enforcement organizations, such as the criminal code and rules of criminal procedure. For DOD analysts and planners to best support these efforts, they must understand the motivations, structures, and tactics of organized criminal groups and rules by which law enforcement organizations operate. UNODC's website provides some good examples of the types of information important to countering organized crime (Authier, 2012).

Second, more representatives from U.S. government agencies and organizations involved in combating organized crime could be assigned to DOD organizations, such as the JICTC, to facilitate the employment of DOD resources. As discussed above, other U.S. government organizations, such as FBI and DEA, are better suited to work with partner nations in Europe on issues pertaining to organized crime. Although the number of representatives stationed in Europe from these organizations has increased substantially since 9/11, many of these representatives are focused primarily on counterterrorism. Additionally, they are too few in number to both advise DOD on appropriate support activities and engage with their partner nation counterparts. Thus, if the number of personnel assigned to work with DOD from other U.S. organizations was increased slightly, it would likely increase DOD's contribution by guiding and facilitating DOD efforts.

Third, authorities pertaining to DOD's support to law enforcement as well as regulations regarding the sharing of intelligence information should be reviewed and streamlined for DOD to most efficiently and effectively support the President's Strategy to CTOC. A labyrinth of rules and regulations pertaining to counternarcotics or counterterrorism operations largely governs DOD's support to CTOC activities. Even though DOD's authorities to support law enforcement have been expanded by several statutes and executive orders since 9/11, several of the key DOD regulations pertaining to these authorities, in particular DOD Reg. 5240.1-R (Intelligence Oversight) have not been updated. As a result, DOD regulations are not optimized to guide DOD in providing the full extent of support authorized by law (Authier, 2012). Moreover, because DOD authorities and regulations do not specifically address support to CTOC activities, but rather pertain to counterterrorism and counternarcotics, DOD must limit its support to those categories of organized criminal activities. Although DOD can frequently tailor its support to these categories, specifically due to

organized crimes' involvement in narcotics trafficking, DOD could be much more efficient and effective if the boundaries of its support to CTOC were expressly stated.

### Conclusion

Through the creation of the JICTC, EUCOM has taken a critical first step in supporting interagency efforts to combat organized crime in Eurasia, but challenges still lie ahead. Although the nature and gravity of the threat is broadly recognized, key enablers are not yet in place to optimize DOD support. Measures should be taken now to facilitate CTOC efforts at the CCMDs. These measures should include development of training programs, streamlining of authorities, and strengthening of working relationships with U.S. agencies and organizations that are leading the fight against TOC. In a period of declining budgets, these comparatively cheap measures would enable organizations such as the JICTC to provide DOD support more effectively and efficiently. In the meantime, the JICTC will continue to expand its partnerships and seek to identify ways in which DOD skills and resources can strengthen the network of organizations combating transnational organized crime.

## Chapter 2: Interagency Cooperation for Major Multijurisdictional Operations

Ms. Lauren Burns, Mr. Joseph D. Keefe, Mr. James H. Kurtz, Mr. William B. Simpkins, Mr. Christopher S. Ploszaj

[lburns@ida.org](mailto:lburns@ida.org)

Institute for Defense Analysis (IDA)

Col Tracy King

USMC

### Introduction

In 2010, the DOD directed the CCMDs to establish a dedicated counter threat finance (CTF) capability that would integrate intelligence and operations, analyze financial intelligence, and coordinate the execution of DOD CTF activities in accordance with existing authorities, regulations, and combatant command initiatives. USNORTHCOM requested a series of studies to help guide the command's CTF activities, focused on TCO operating in Mexico. One of those studies, conducted by the Joint Advanced Warfighting Program at the Institute for Defense Analyses, under the sponsorship of the Joint Staff Directorate for Joint Force Development (J-7), focused on lessons learned from 22 multijurisdictional, interagency operations that took place in the USNORTHCOM area of responsibility between 1996 and 2011 (Burns, et al., December 2011). These operations were directed against the command-and-control and the financial networks of Mexican TCOs, and were, arguably, the largest of their kind conducted by the USG against Mexican TCOs. The study, from which this paper is drawn, provided USNORTHCOM with insights into long-standing mechanisms for interagency coordination as well as into previous efforts to counter Mexican TCOs.

The DEA Special Operations Division (SOD) coordinated each of the operations. To identify the lessons learned, the study team conducted a series of structured interviews with SOD's lead Staff Coordinators responsible for coordinating each of the 22 operations.

### Special Operations Division

Established in 1994, SOD is a multi-agency division staffed by investigators, analysts, attorneys, military representatives, and support personnel from more than 20 interagency partners. SOD's mission is to establish, coordinate, and support law enforcement strategies and operations aimed at dismantling TCOs and narco-terrorist organizations. SOD places special emphasis on those TCOs and narco-terrorist organizations that operate across U.S. and international jurisdictional boundaries. SOD identifies and coordinates overlapping investigations conducted by disparate agencies and facilitates information sharing among all concerned (Maltz, 17 November 2011).

SOD uses sophisticated technology and synchronizes the resources of participating agencies. The Division works jointly with federal, state, and local agencies as well as with foreign counterparts in support of multijurisdictional and multinational investigations to target the TCO's command-and-control and financial networks (Maltz, 17 November 2011).

SOD shares critical information with a wide range of law enforcement, defense, and intelligence agencies, and works to expand the scope, breadth, and depth of multijurisdictional, interagency operations. SOD also works to discover and understand how TCOs and narco-terrorist organizations adapt to the interagency efforts directed against them (Maltz, 17 November 2011).

## Methodology

Before the mid-1990s, the Mexican TCOs, for compensation, transported cocaine into the U.S. for Colombian TCOs that oversaw distribution of the cocaine to various U.S. affiliates including other Colombians, Dominicans, and major U.S. gangs. By 1996, Mexican TCOs had expanded their own drug distribution networks throughout the U.S., in effect replacing the Colombians as the primary distributor of cocaine sold in the U.S. To counter their activities, SOD began to focus on attacking the command-and-control and financial networks of the Mexican TCOs. To identify a set of multijurisdictional, interagency operations that targeted Mexican TCOs between 1996 and 2011, the study team and SOD personnel jointly selected the 22 operations listed at the end of this chapter.

After the operations were selected, SOD identified the lead Staff Coordinator for each one. All lead Staff Coordinators were Supervisory Special Agents at the GS-14 or GS-15 level when they coordinated the operation. The study team developed a set of 16 questions that the study team used to conduct structured, not-for-attribution interviews with each lead Staff Coordinator.<sup>13</sup> The questions focused on lines of inquiry that would help identify the most important lessons learned.

## Tactics, Techniques, and Procedures used in Operations

The interviews revealed that the operations often involved a variety of tactics, techniques, and procedures (TT&P), which included, but were not limited to:

- Electronic surveillance—domestic and foreign;
- Fixed, mobile, aerial, and maritime surveillance;
- Cooperating individuals;
- Undercover federal agents;
- Undercover state and local law enforcement personnel;
- Undercover bulk cash pickups;
- Undercover bank accounts;
- “Walled off” seizures of drugs and currency;<sup>14</sup> and
- Federal drug laws.

---

<sup>13</sup>Comments about the operations are not associated with the name of the lead Staff Coordinator or the specific operation because the interviews were not for attribution.

<sup>14</sup>“Walled-off” seizures are planned and executed in such a way to lawfully preclude or diminish the ability of a trafficker(s) to identify the origin of the investigative activity that led to the seizure.

The interviews made clear that the TT&Ps used by field investigators when a particular investigation began were almost invariably expanded and adjusted once SOD identified cross-jurisdictional or interagency implications. At that point, the operations benefited from having a coordinated, interagency approach. Often, the expanded effort involved overseas investigation that included participation of foreign counterparts, DOD and U.S. Intelligence Community. Those adjusted approaches regularly reset targeting priorities and courses of investigative action, which usually resulted in more productive operational outcomes, for example, more arrests, drug seizures, and asset forfeitures, and greater disruption to the TCO.

Operations varied in scope and complexity, but were always framed in a set of goals and objectives designed to deter, disrupt, and dismantle TCOs' command and control and financial activities. Actions that SOD coordinated included arrest, extradition, prosecution, seizures of cash, and forfeiture of assets, both domestically and overseas. Regardless of the scope and complexity of the operations, detailed laws, regulations, guidelines, and policies governed the TT&Ps used. The specifics of the applicable laws, regulations, guidelines, and policies are too numerous and detailed to describe in this paper; however, it is important to emphasize that multijurisdictional, interagency operations are conducted with rigorous internal and external oversight.

## Lessons Learned from the Interviews

### *DOD Capabilities*

Among the lead Staff Coordinators interviewed, there was a general lack of knowledge regarding capabilities available from DOD and how to request those capabilities to support operations against Mexican TCOs. In the few years since DOD began assigning liaisons to SOD, Staff Coordinators have been gaining a better understanding of DOD capabilities. For example, Staff Coordinators believe DOD could support law enforcement agencies with tracking the movement of and interdicting precursor chemicals. This effort would be in accordance with the 2010 *National Drug Control Strategy*, which outlines DOD's role in the effort to prevent precursor chemical diversion.

Precursor chemicals are essential for the clandestine manufacturing of synthetic drugs, such as methamphetamine. The ability to track the flow of these chemicals would greatly enhance the U.S. Government's and its foreign partners' ability to deny TCOs the ability to manufacture the drugs. A few of the operations involved the clandestine manufacturing of methamphetamine in Mexico. In these operations, the U.S. agencies could track the movement of the precursor chemical pseudoephedrine from Bangladesh through Belize en route to Mexico, and from India and China to Mexico.

### *Money Movement*

The interviewees identified bulk cash as the most common method TCOs used to move money within the U.S. and into Mexico from the U.S. The Mexican TCOs accomplished this, for example, by placing the money in secured traps the traffickers had built into automobiles or trucks, or concealing it within a cover load of legitimate products. Individuals walking across the border carried smaller quantities of cash. In addition, the TCOs would pay independent organizations and individuals to transport the

currency into Mexico. Once the TCOs got their bulk cash to Mexico, it was difficult to track the money flow, even when Mexican authorities helped.

Some operations identified businesses and companies in Mexico that various TCO leadership either did business with or owned a share of. As a result of receiving this type of information, the Staff Coordinators started working more with The Department of the Treasury's Office of Foreign Assets Control, and now work with the office regularly when conducting multijurisdictional, interagency operations. Combining the financial sanctions authorities of The Department of the Treasury with law enforcement's criminal authorities is an effective way for the USG to target the TCOs and their assets.<sup>15</sup> In operations that identified TCO bank accounts and other illicit assets in the U.S., federal prosecutors pursued asset forfeiture proceedings to block the bank accounts and seize the assets.

Some interviewees who were responsible for later operations said that an emerging trend among the Mexican TCOs was to use trade-based money laundering schemes, particularly through China. With this scheme, Mexican TCOs sent money to China to purchase goods that they then shipped to Mexico and resold on the open market. Although this way to launder money is common, the volume of trade-based money laundering activity running through China concerned the interviewees because it was unusually large.

### *The Role and Importance of Coordination Meetings*

All operations were an amalgam of anywhere from 30 to 380 separate investigations, which, through analysis, SOD discovered were connected in ways that had previously not been apparent to the offices and agencies conducting the individual investigations. Once the multi-agency connections were established, SOD coordinated the operations by bringing together the investigators, analysts, and prosecutors for meetings. These meetings always included U.S. partners and, when appropriate, foreign partners. The goals of these meetings were to share information and develop effective strategies for attacking the targeted TCO(s).<sup>16</sup>

Investigators, analysts, and prosecutors were more supportive and motivated when they fully understood their role and how it contributed to deterring, disrupting, or dismantling the targeted organization. According to one Staff Coordinator, at the beginning of the operation, coordination meetings were used to form the "collective we" to help ensure that all field investigators, analysts, and prosecutors worked together under an agreed upon strategy with common goals.

---

<sup>15</sup>Treasury, through the Office of Foreign Assets Control, is the primary US Government administrator and enforcer of economic and trade sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, proliferators of weapons of mass destruction, and other threats to the national security of the United States. This office acts under Presidential national emergency powers and possesses the authority granted by specific legislation to impose controls on transactions and freeze assets under US jurisdiction (United States Code, 21 U.S.C. '1901-1908, 8 U.S.C. '1182; Code of Federal Regulations, 31 C.F.R. Parts 536 and 598; White House, 21 October 1995; White House, July 2011).

<sup>16</sup>A typical multijurisdictional, interagency operation might last 18–24 months and involve 3–5 coordination meetings. In addition to having large meetings, the SOD Staff Coordinators and analysts were in constant communication with participating field offices and, as necessary, would convene smaller meetings.

At the meetings, each investigation was briefed by the lead investigator/analyst to delineate how individual investigations fit within the larger, strategic effort against a TCO. Staff Coordinators learned that it was important to have broad levels of attendance at the meetings, because no matter how detailed or limited an attendees' information was about the subjects being investigated; the smallest tip could lead to major results. These meetings also served as training venues to educate investigators, analysts, and prosecutors on SOD's capabilities and capacities.

All the interviewees emphasized that the coordination meetings were "critical" in identifying, avoiding, and resolving interagency conflicts. The Staff Coordinators stated that a byproduct of the meetings was the development of trust among the participants as well as the recognition that no preferential treatment was given to any one agency or jurisdictional venue over another.

The coordination meetings also gave the prosecutors a forum to debate which judicial district would charge which violator(s) for which offense(s). Without the meetings, issues regarding prosecutorial decisions would not have been resolved as effectively. The meetings were helpful in gauging the various participants' commitment and interest in the others' endeavors. Finally, the coordination meetings helped to identify where the greatest effects could occur and served as a platform to discuss new and emerging trends in transnational criminal activity.

All interviewees agreed that having investigators and analysts co-located was critical to an operation's success. The interviewees further emphasized that when investigators and analysts worked together in one location—both at SOD and in field offices—they were better able to gather intelligence about the targeted organization's structure and successfully identify links to other investigations.

### *Foreign Involvement*

Foreign involvement in the multijurisdictional, interagency operations against the Mexican TCOs evolved. The earliest operations had limited foreign involvement, but as the multijurisdictional, interagency operations grew in size (i.e., both the number of separate investigations and agencies involved), SOD recognized the need for foreign counterpart involvement in addition to that of Mexico in order to amplify the effects the operations had on the Mexican TCOs.

Concerns about corruption in Mexico affected engagement with Mexican counterparts (Silver, 27 May 2010). Over time, experience showed that "when they [Mexico] are brought into the operation, the results improved significantly." For example, during one operation that targeted the Amado Carrillo Fuentes TCO, the Government of Mexico (GoM) executed some of its first judicial wire intercepts, which eventually led to the seizure of more than \$250 million in assets, as well as the collection of documents that SOD exploited to further its intelligence on the organization. There were a number of other examples in the 22 operations studied where SOD needed the GoM's support to affect the activities of the TCOs in Mexico. In one example, involving the transshipment of drugs, the Staff Coordinator reported that "the key corridor for the operation was between Nuevo Laredo and San Antonio up the I-35 to I-10, so we had to bring in the Government of Mexico."

One challenge prevalent in many operations, despite the success of past operations using judicial wire intercepts, was the GoM's preference for intelligence wire intercepts over judicial wire intercepts. Fewer

restrictions exist to initiating intelligence wire intercept than a judicial wire intercept. The difference may not seem significant, but which kind of wire intercept used matters if U.S. law enforcement is going to use them in a U.S. court. Under U.S. law, U.S. law enforcement agencies can use host-nation wire intercepts as evidence only if the host nation's judicial system authorizes the intercepts, and they meet the guidelines approved by DOJ.

A second challenge is with the GoM's prosecutorial system. As has been widely reported, Mexico's judicial system has a low conviction rate.<sup>17</sup> Even if the GoM improved this record, a fundamental challenge of trying to convict major TCO members in the Mexican system, which is based on the Napoleonic code of justice or "inquisitorial" system, versus the accusatory or "adversarial" system used in the U.S., would still exist.<sup>18</sup> This difference is important because under the Mexican system, prosecutors and defense attorneys file their complaints and defenses, respectively, in writing. A judge then adjudicates the case without being required to share the evidence with either the prosecution or defense, and does not have to justify his/her decision. The challenge with this system is that it is not transparent and is primed for corruption.

In addition to its inquisitorial system, the GoM also struggles with convicting TCO members because Mexico has weak conspiracy laws (Brewer, 2011). Without sufficient conspiracy laws, law enforcement officials have a difficult time effectively targeting a TCO's command-and-control and financial networks. This is especially true for extending legal cases to include corrupt government officials. Conspiracy laws are important because they give law enforcement officials broader authority to prosecute those involved in a crime even if the individuals do not directly handle, to cite one example, the drugs being trafficked or the money derived from the criminal activity.

The operations often needed the GoM's involvement to target more effectively the Mexican TCOs. To decide who to work with, and what information to disclose, the Staff Coordinators used people with the most knowledge about the TCO members in Mexico: the lead agency's country office(s).<sup>19</sup> "The negative effects of corruption are diminished by working through the country office because the assigned personnel know who can and cannot be trusted, and whom SOD can target without risking compromise," said one Staff Coordinator.

In dealing with the counterparts in Mexico, the Staff Coordinators all realized the importance of working through the country office(s) within the host nation to better appreciate the political dynamics (including corruption). As one Staff Coordinator said about taking the lead for operations involving Mexico, "understanding the Government of Mexico's law enforcement structure and strategy on drug trafficking before starting the operation would have been helpful." This education comes from the

---

<sup>17</sup>Non-governmental organizations have reported that Mexico's conviction rate is between 1 and 2 percent (Department of State, 11 March 2010). According to other estimates, between 75 and 96 percent of crimes between 1996 and 2003 went unpunished (Franco, 20 April 2005).

<sup>18</sup> Reforming this system is a central pillar of the US Merida Initiative (U.S. Agency for International Development, August 2011).

<sup>19</sup>The various country offices are nested under the authority of the U.S. Embassy in Mexico City as part of the U.S. Country Team.

personnel within the country office who work with the GoM daily and have the greatest appreciation for the political sensitivities that affect the operating environment.

### *Technology and Adaptation*

Some of the lead Staff Coordinators agreed that the TCOs' use of technology always changes after large seizures. In addition to adapting the technologies they had, the TCOs also stayed current with evolving technologies. The TCOs' successful technological adaptation caused one former Staff Coordinator to urge that reporting on technology be made a standard deliverable of every investigation.

The same former Staff Coordinator believed studying demographic patterns would lead to insights into the TCOs' adaptation. Specifically, he discussed the Mexican TCOs' strong foothold in Atlanta, Georgia. He believes the legitimate construction business before the Atlanta Olympics brought an influx of Mexican workers that afforded the Mexican TCOs an opportunity to assimilate into the community, and later to use the community to disguise their activities. He said, "They [Mexican TCO members] worked construction during the day and at night met with hillbilly methamphetamine users...over night, Atlanta's meth users went from being serviced by local dealers to being serviced by Mexican TCOs."

Once the Mexican TCOs gained this foothold, they expanded their business in the area to include cocaine and marijuana distribution. A similar migration occurred in North Carolina and Wyoming where the Mexican TCOs followed the flow of migrant workers to areas where thinner law enforcement presence meant the TCOs could easily assimilate into the local population. According to one Staff Coordinator,

All the cartels are setting up shop in smaller areas with farming communities because there is less law enforcement presence. They are using these areas as bases versus big cities. We are initiating wire-tap investigations in Casper, Wyoming...ten years ago, this was unheard of.

To try to mitigate the need to adapt or find new ways of doing business, Mexican TCOs worked to protect their investments. For example, during one operation's takedown, the leader of a U.S. drug trafficking organization affiliated with the Arturo Beltran-Leyva TCO managed to evade capture in the U.S. While still a fugitive in the U.S., he contacted his connections in the Arturo Beltran-Leyva TCO, seeking assistance to flee into Mexico. The Leyva TCO sent a plane to Las Vegas to get the leader of the U.S. trafficking organization and flew him to Mexico. According to the Staff Coordinator, "the Leyva drug trafficking organization offered to do this because they knew who was making them their money in the United States and wanted to protect the relationship." While in Mexico, with the assistance of the Leyva organization, the leader of the U.S. trafficking organization began to identify individuals he suspected of being informants and began to order "hits" to clean out his organization. Eventually, the GoM arrested the U.S. trafficker and assisted in his transfer back to the U.S. for prosecution.

Interviewees indicate that TCO members in the U.S. adapt often, even during ongoing operations. In contrast, those interviewed did not observe the same frequency of adaptation with the TCOs' command-and-control in Mexico. They believe this is because the TCOs never had the level of pressure exerted by the GoM that created that necessity. According to one interviewee, still involved in

operations against Mexican TCOs, the pressure exerted by the GoM on the Mexican TCOs in the past couple of years has forced the command-and-control to adapt, in varying degrees.

## Summary

The multijurisdictional, interagency operations reviewed grew in size and effects achieved (e.g., more arrests, drug seizures, asset forfeitures, and greater disruption to the TCO). Part of that success came from lead Staff Coordinators taking the time to learn from the previous Staff Coordinators and the operations they coordinated. In this regard, the lead Staff Coordinators interviewed recognized the importance of the following.

- Interagency coordination meetings that bring together all relevant players regardless of how small their role may appear initially; sometimes the smallest piece of information can lead to great effects.
- Collocation of investigators and analysts to streamline the investigative and analytical requirements and permit constant crosstalk.
- Input from the country team with respect to its knowledge and understanding of foreign counterparts, to include how to engage the host nation before, during, and after operations in a politically tenable manner as well as who to work with to mitigate concerns about corruption.
- Encouraging and assisting the GoM to enact conspiracy laws in Mexico that enables more effective targeting of the command-and-control and financial operations of Mexican TCOs.

The lead Staff Coordinators also highlighted many areas where multijurisdictional, interagency operations could improve. First, the lead Staff Coordinators appreciate that DOD has capabilities to support law enforcement efforts; however, they lack specific knowledge of those capabilities and the processes to use to obtain them. Second, the U.S. Government has an opportunity to disrupt the drug trade of Mexican TCOs if it could find consistent means for tracking and seizing precursor chemicals through enhanced global partnerships. Currently, the efforts are piecemeal and opportunistic. Staff Coordinators welcome DOD support in disrupting the illegal flow of precursor chemicals.

Finally, to counter the Mexican TCOs more effectively, the USG needs agile means to recognize how the TCOs are implementing and using evolving technologies to protect and facilitate their command and control and financial operations. This is an area where DOD support might assist law enforcement as it confronts the issues associated with evolving technologies.

Table 1: Results of the 22 Operations Examined

Operation	Arrests	Currency and Assets	Cocaine (kg)	Marijuana (lbs)	Methamphetamine (lbs)	Heroin (lbs)	Firearms	Federal Involvement	State and Local Involvement	Foreign Involvement
1	41	>US\$11 million	7 metric tons	2,800				DEA, US Customs Service	Several agencies	
2	48	US\$7,395,579	4,012	10,846				DEA, Several US Treasury Agencies (including IRS and US Customs Service)	Several agencies	
3	123	US\$19,031,751	12,434	6,177				SOD (DoJ, DEA, FBI, US Customs, IRS)	Several agencies	Government of Mexico
4	>122	US\$10,890,295	5,266	9,708				SOD (DoJ, DEA, FBI, US Customs, IRS)	Several agencies	Government of Mexico
5	>100	US\$4.2 million and assets		34,000				SOD (DoJ, DEA, FBI, US Customs, IRS)	Several agencies	
6	>261	US\$12,481,585	8,732	27,738				SOD (DoJ, DEA, FBI, US Customs, IRS)	Several agencies	Mexican Law Enforcement (Organized Crime Unit)
7	>240	>US\$8.3 million	11,759	24,409	108	1		SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 67 agencies	Mexican and Colombian police
8	94	US\$10.6 million	1,407	523	10			OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 24 agencies	Mexico; Colombia; Guatemala; El Salvador
9	196	US\$5,487,307	1,074.50	4,404		19.4	13	OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 38 agencies	
10	64	US\$2,351,849 \$136,394 (other)	461.1	13,116.80			18	OCDETF and SOD	LA District Attorney's Office; California Highway Patrol; LAPD; North Carolina State Police; Greensboro, NC Police Dept; Arizona Dept of Public Safety; Phoenix Police Dept	Mexico and Bolivia
11	17	US\$5.3 million \$5.7 million assets	632					OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 5 agencies	Mexican Federal Police (AFI)
12	26	US\$1,462,110	309	689	34			OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	Houston HIDTA and Willowbrook Police Dept (Chicago)	AFI; Colombian National Police; Panamanian National Police
13	59	US\$3,916,364 CAD\$2,500	90		155	30 oz	43	SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 13 agencies	Government of Mexico

Operation	Arrests	Currency and Assets	Cocaine (kg)	Marijuana (lbs)	Methamphetamine (lbs)	Heroin (lbs)	Firearms	Federal Involvement	State and Local Involvement	Foreign Involvement
14	48	US\$2,910,000	13,624	2,303	26.3		4	OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	Several agencies	Mexican, Colombian, Peruvian, and Ecuadorian National Police; Chilean Navy
15	37	US\$4,701,629	1,943		246			SOD (DoJ, DEA, FBI, US Customs, IRS)	South Metro Drug Task Force, Arpada Police Dept; Denver Police Dept (New Bedford, CT)	Government of Mexico
16	300	US\$38,495,708 \$5,050,000 assets	4,041	23,758	673	8	70	OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 68 agencies	Mexican Attorney General's Office, AFI; Dominican Republic
17	42	US\$48,607,010	2,422	61,793,500	14			OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 13 agencies	5 agencies in Mexico; DAS in Colombia; Venezuela
18	507	> US\$60 million and assets	16,711	51,258	1,039	19	168	SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 137 agencies	Guatemala, Colombia, Panama, Mexico, Special Operations Group (Rome, Italy)
19	781	US\$61,013,308 \$10,520,000 assets	12,611	17,611	1,263	8	191	OCDETF and SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 102 agencies	Procuraduría General de la República (Mexico); Royal Canadian Mounted Police; Combined Special Forces Enforcement Unit (Canada-BC); Indian Narcotics Control Bureau
20	865	US\$60,074,809 (US\$ and assets)	1,908	15,383	1,800	13	243	SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 182 agencies	Government of Mexico
21	1,837	US\$148,016,951 \$7,053,300 assets	4,969	135,118	1,245	1,318	360	SOD (DoJ, DEA, FBI, US Customs, IRS)	approx. 94 agencies	Government of Mexico
22	73	US\$6.5 million	6,782	572	37			DEA, IRS, ICE	several agencies	Mexico, Ecuador, Colombia, Canada, Costa Rica, Panama, Dominican Republic

## Chapter 3: The Intersection of Crime and Conflict

Ms. Gretchen Peters

[Peters\\_Gretchen@bah.com](mailto:Peters_Gretchen@bah.com)

George Mason University/Booz Allen Hamilton

### Introduction

From Thucydides to Hobbes, some of the most revered scholars of conflict have argued that war destroys markets. They were wrong. Conflict actually transforms markets, creating new winners and losers. It is true that production generally decreases in war zones; commercial manufacturing declines or even stops, investment founders, agricultural activity is interrupted, and often the populace suffers from widespread scarcity. However, conflicts typically create rich economic opportunities for a minority of actors, even as they destroy them for the majority (Collier 1999). It is possible to do very well out of war, in particular in civil conflicts and insurgencies.

One can find examples of this phenomenon in conflicts around the globe, and throughout history. In Afghanistan, war profiteers—both within the Taliban and the Kabul government—have benefitted handsomely from smuggling heroin out of Afghanistan and transporting goods into the NATO Coalition. Liberian warlord Charles Taylor enriched himself off diamond mines, while fomenting widespread brutality. New scholarship even shows that America’s Founding Fathers became wealthy, and were able to defeat Britain, then the world’s greatest power, because they ran lucrative smuggling networks that exported New World commodities and imported weapons and ammunition (Andreas, 2013, pp.3-4). Indeed, the first signatory to the Declaration of Independence was Boston’s premier merchant smuggler, John Hancock (p. 5).

### Insurgency and Crime

Rebellions have a strong tendency to become involved in black and grey market activity because they cannot openly fund-raise nor participate in the state-regulated licit economy. Since the end of the Cold War, and the broad decline of state sponsorship for insurgent proxies, illegal activities have provided critical revenue streams for insurgent groups around the globe, helping them to survive much longer than they could have without them. One Stanford University study found that conflicts in which the actors depended upon “valuable contraband” lasted five times longer than other conflicts on average, making it pertinent for military commanders, diplomats and scholars alike to gain a better understanding of the economic drivers that can prolong conflict (Fearon, 2004). Organized crime not only sustains insurgencies from a financial standpoint, it also supports their asymmetric warfare campaign by spreading fear and insecurity, frustrating efforts to establish rule of law, limiting the emergence of a healthy, commercial economy and contributing to public perceptions that the state is corrupt and incapable of countering the rebellion.

The intersection of crime and war can reshape wars, which come to be driven less by “the Clausewitzian logic of forwarding a set of political aims, but rather by powerful economic motives and agendas.” (Berdel and Malone, 2000, p. 23) There are numerous examples, from the Irish Republican Army to the Revolutionary Armed Forces of Colombia, or FARC, of rebel groups first motivated to action for political reasons, who later found benefits in illicit enterprise—and therefore an additional reason to continue fighting. Insurgent groups will typically deepen their involvement in organized crime over the course of an armed struggle both as new opportunities for profit emerge, and as resources become scarcer (Zartman, 2005). One group that followed this trajectory is the FARC, the Marxist peasant army, which first taxed coca farmers to raise revenue, later began taxing cocaine labs, still later became involved in cocaine processing, and now exports cocaine to multiple international destinations. Analysts and Colombian officials alike believe the FARC has become disconnected with its original leftist aspirations.<sup>20</sup>

Illicit earnings can also provide insurgent groups, or factions within insurgencies, with a means of breaking free from state sponsors or leaders whose support may be dwindling or politically conditional. A shift in generation, brought on by the death, capture or retirement of a former commander, often marks a critical juncture in an insurgent group’s criminal involvement, usually marking a shift when a group deepens its organized crime activities, or expands into new illicit sectors. A good example of this phenomenon is the Haqqani network, which expanded into new criminal sectors including kidnapping and construction when the clan patriarch retired, and his son took command of the group.<sup>21</sup> Perhaps most importantly, involvement in smuggling brings insurgents into contact with TCOs, sometimes for enduring business partnerships, in which they learn from each other and make other contacts.

Protracted conflicts, such as the wars in Colombia and Afghanistan, can produce what Zartman (2005) has termed the “Robin Hood Curse.” (p.269) Life at war becomes sustainable—even highly profitable—for insurgent leaders, while an end to the conflict would likely produce a decline in wealth and power for “the Merry Men.” This is particularly true in places where insurgents gain funding from narcotics trafficking, because the high profits generated by the drug trade tend to wash away whatever ideological objectives caused the group to take up arms in the first place. Illicit profits thus generate a collective action logic to sustain war and instability, and a concrete financial incentive to spoil any peace process (Olson, 1965). Once a war enters this phase it is typical to see insurgents collaborating with their enemies on organized crime, proving that profit eventually trumps politics. There’s another side to the curse; Williams (2012) has shown that an insurgency can lose both its standing with the population and its internal sense of political identity as a result of criminalization. In other words, a highly criminalized insurgency faces strategic vulnerabilities, which could be exploited in a counterinsurgency campaign that protects the populace and attacks the rebels using tactics that are typically applied against organized crime networks.

---

<sup>20</sup> For detail see: [http://www.start.umd.edu/start/data\\_collections/tops/terrorist\\_organization\\_profile.asp?id=96](http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=96)

<sup>21</sup> For more on this see: Gretchen Peters “The Haqqani Network, the Evolution of an Industry,” *Combatting Terrorism Center*, USMA, July 2012. [www.ctc.usma.edu/posts/haqqani-network-financing](http://www.ctc.usma.edu/posts/haqqani-network-financing)

## TCO and Conflict Zones

Conflict zones are also attractive to TCOs, which gain comparative advantage from doing business in unstable, chaotic environments. In the last two decades, organized crime has globalized just like other industries, moving into weak states, conflict zones and lawless regions, where the cost of doing illicit business is lower. Major TCOs like the Sinaloa Cartel of Mexico, Pakistan's D-Company, Japan's Yakuza, and Lebanese Hezbollah now operate across dozens of countries, and can have as many "employees" as large multinational firms. As they seek out new geographic markets to do business, they look for certain conditions, including the following.

- A location along a critical trade route, or near a major consumer market.
- A low rank on the United Nations Human Development Index, with social indicators, education levels and economic conditions that are among the world's worst.
- A youth bulge, high unemployment and widespread scarcity.
- Weak, corrupt and under-resourced governments, with a history of political and civil strife, and perhaps an insurgency or two along porous borders.

Such conditions typically scare off commercial and portfolio investors, but for organized crime, it is an attractive investment climate.

In conflict zones and fragile states, TCO networks forge alliances with insurgent, terror groups and gangs, simultaneously corrupting elements of national governments and using the power and influence they gain from capturing state institutions to further their criminal activities. This process is tremendously corrosive and also self-reinforcing; in other words, it gets harder to pull a country or region out of the downward cycle once it begins. Not only is corruption difficult to fight, but distortions to the economy and financial system caused by organized crime make it complex for the commercial economy to recover. For example, a number of narcotics-producing countries have suffered from what is generally known as "Dutch disease," in which there is a stagnation or even contraction of other, non-drug-related sectors, making their economies even more dependent upon the single illicit commodity (Economic and Social Consequences, 1998). Afghanistan is a good case study of this phenomenon, where opium has represented as much as 50 percent of the country's Gross Domestic Product. The drug trade there has contributed to soaring real estate and commodity prices, while insecurity and corruption have frightened off investors, thus preventing the emergence of a healthy licit economy. Crime and violence is also expensive to combat. For example, the World Bank estimates that Central American states spend as much as eight percent of their GDP on law enforcement, citizen security and health care costs resulting from soaring crime and violence (Crime and Violence in Central America, 2011).

As Colombia and Afghanistan have demonstrated, fostering the emergence of a capable, responsible, and responsive state and a stable civil society is challenging in such environments, but not impossible. A continued state of insecurity tends to richly benefit a small number of elites on both sides of the battlefield, giving both corrupt state actors and insurgent leaders a financial incentive to sustain the disorder, regardless of whether their wider political and other goals have been met. Attempts to eliminate illicit behavior, such as the eradication of narcotics crops, often serve only to stoke the flames

of the insurgency, especially when the populace depends on criminal proceeds to survive. Efforts to combat the insurgency can boost demand for criminal actors who supply the insurgents and bribe corrupt local officials. This cycle is difficult to break, and it often takes decades to observe real, lasting progress.

### **Reshaping Intelligence and Forging More Effective U.S. Interventions in Conflict Zones**

Before deploying to unfamiliar territory, any prudent war fighter will study the physical terrain, seeking to identify potential danger zones and pitfalls, so as not to stumble blindly into peril. In the last decade, U.S. military commanders have come to appreciate the importance of understanding the human terrain, so as to better navigate cultural, historic and religious sensitivities, as well as complex tribal and clan politics. However, in a world where crime and conflict increasingly intersect, the U.S. military needs to get better about understanding the economic terrain in conflict areas. Millions of dollars disbursed by American forces in Iraq and Afghanistan have distorted local economies, shifted the balance of power and, in many cases, inadvertently enriched and empowered the very adversaries and predatory powerbrokers that U.S. forces sought to defeat.

Counterinsurgency doctrine identified money as a weapons system, but it is a dangerous weapon when the barrel is pointing back at you. In Iraq and Afghanistan, there has been frighteningly little oversight of U.S. development aid and payments to local transport and security networks. In many cases, well-intentioned aid money has ended up funding the insurgency, through extortion rackets or front companies, resulting in the unintended consequence of U.S. funds being used to directly support militants who could fund attacks against American troops and the civilian populace. Moreover, U.S. troops have at times been dangerously oblivious to the black and grey markets hiding in plain sight that have supplied and sustained the enemy with critical resources, ranging from telecommunications services to IED components. The U.S. must not repeat these mistakes as we confront new problem sets in the Mideast, Latin America, and West Africa.

As military strategists prepare for a world where IW will in fact become the norm, it is imperative to develop a framework for collecting, analyzing, and utilizing economic data in irregular warzones. For example, it is critical to learn, and then disrupt, the logistical and financial channels that supply and sustain the adversary. In most cases, significant portions of that supply chain and financial infrastructure will exist outside the warzone, and may be highly globalized. U.S. military operations should be supported by a team of globally focused financial and fraud investigators to follow the illicit money supporting TCO and insurgent networks that the U.S. is combatting. That team would need to work in close partnership with the U.S. Treasury and U.S. law enforcement, since they have the relevant authorities for pursuing illicit financial activity and for sanctioning banks, businesses and the underworld facilitators, such as Dawood Ibrahim and Viktor Bout (who is serving a 25-year U.S. prison sentence for weapons smuggling), who support and supply terrorist, insurgent and criminal elements.

In addition, military planners would be wise to develop doctrine for stabilizing territories plagued by the crime-terror nexus, putting a focus on de-conflicting the work of disparate U.S. agencies, and crafting holistic strategy. As Williams (2008) has written: "In a world where the United States seeks to combat

extensive disorder and restore stability, military, economic, and diplomatic power have to be targeted in ways that create synergies rather than seams, that reinforce rather than undercut, and that provide maximum efficiency and effectiveness.”(2008) Much lip service has been given to interagency cooperation and the so-called “whole of government” approach, but in practice stability operations in Afghanistan and Iraq were often badly stove-piped. A better approach would be to create trans-agency teams for specific mission that would integrate military forces, diplomats, reconstruction and development specialists and legal experts into a team tasked with reestablishing the authority, legitimacy, and effectiveness of the state in a target zone (Williams, 2008, p. xi). Ideally, these teams should remain loyal to their mission rather than their parent agency, and committed to that mission for longer periods than currently typical in diplomatic and military foreign service.

Most importantly, in conflict zones, U.S. officials, whether military, law enforcement or diplomatic, must be intolerant of corruption and criminal behavior on the parts of their local counterparts. As Afghanistan has illustrated, we ensure our own defeat when we turn a blind eye as local partners and the recipients of U.S. aid steal development money or engage in organized crime. Accommodating corruption costs the United States more in the long run, because ultimately we fail to foster the emergence of stable, self-sustained states that can become durable partners. Colombia shows us that a country can fight back against a deeply entrenched criminal economy and criminalized insurgency, but when it does, that fight will be bloody and slow-going.

## Conclusion

The intersection of crime and conflict is not a new phenomenon, but globalization and communications technology have provided insurgent and terror networks with the capacity to expand their operations and connections far beyond the boundaries of their given conflict zones. The nexus of TCO and conflict represents an urgent threat and an ever-changing problem set for U.S. policy makers and military planners, one that necessitates a fundamental rethink of the way the U.S. government organizes itself and approaches stability operations.

## Chapter 4: The Connected Illicit System: A Glimpse at the Illicit Superhighway

Dr. Scott Helfstein

[scott.helfstein@gmail.com](mailto:scott.helfstein@gmail.com)

Combating Terrorism Center, West Point

### Introduction

The convergence between criminal and terrorist elements has been the subject of much debate over the last decade.<sup>22</sup> Some have argued that the process of convergence has continued apace, and that the interconnected network presents a unique problem threatening national security (Sanderson, 2004; Killebrew and Bernal 2010). Others have argued that the convergence thesis is overblown and that temporary marriage of convenience that often arises is disconcerting but far from a significant national security threat (Dishman 2001). This paper uses a unique dataset developed by West Point's Combating Terrorism Center to offer an empirical assessment of global connectedness and examine the structural relationships between criminals and terrorists in the network. The analysis of almost three thousand individuals operating across one hundred and twenty countries suggests that global connectivity is quite high. It also offers insight into structural aspects of the network and a novel rationale for convergence.

The research presented here on transnational illicit networks, in some ways the first of its kind, helps to get traction on the issue of convergence. With that in mind, it is also important to recognize that there are limits to this exercise. Astute analysts that have unpacked the idea of convergence suggest that one must look across different axes. The most common distinction is that convergence in activity versus convergence in organizations (Williams 1998; Kenney 2007; Lowe 2006). Activity convergence occurs when terrorists use criminal activities or criminals use terrorist tactics in pursuit of their respective political and economic ends. One might think of this as activity appropriation. Organizational convergence occurs when terror groups and criminal enterprises work together. Activity appropriation is commonly seen as terrorist groups rely on criminal activity to fund their activities. While many people generally overlook criminal use of terrorism, it is actually a common tool for organizations looking to manipulate politicians, law enforcement and the public (Makarenko, 2004). Organizational convergence in cases like Haqqani network relationship with al-Qaeda and D-Company's relationship with Lashkar-e-Tayhbah (LeT) occurs with some frequency, but it may short-lived.

This project adopts a slightly different method in assessing convergence. Rather than focus on activities and organizations, though they are considered, the network is built by mapping individuals and their relationships to others. Studies of organizational convergence frequently find it challenging to bin the groups and identify where one ends and another begins.<sup>23</sup> For example, an individual like Illyas Kashmiri

---

<sup>22</sup> For a summary of this debate see John T. Piccarelli, "A Brief Discussion of the Nature and Convergence of Transnational Organized Crime and Terrorism," A paper prepared for the Trans-Atlantic Dialogue on Combating Crime-Terror Pipelines, June 25-26, 2012.

<sup>23</sup> For a discussion on the breakdown of hierarchies and how that complicates understanding of illicit networks see Chris Dishman, "The Leaderless Nexus: When Crime and Terror Converge," *Studies in Conflict and Terrorism* Vol. 28, No. 3 (2004), 237-252.

reportedly had relationships with Harkat-ul-Jihad al-Islami (Huji), LeT, al-Qaeda and D-Company. Affixing him to any one of those entities risks underestimating convergence, but considering him as a part of all entities complicates topology. It also allows one to examine convergence without having to address some of the topological issues tied to activity appropriation. For example, it is difficult to determine whether beheadings conducted by Mexican cartels are terrorist or criminal actions. Both the activity and organizational approaches to understanding convergence are critical, but these difficulties also suggest that they should be augmented with alternative approaches as well. By focusing on the base unit, individuals, we can develop a picture of the global interconnectivity between terrorists and criminals.

The empirical assessment is built on open source reporting and court records in over sixty languages gathered for financial compliance. It reveals that interconnectivity is greater than one might have predicted. At the outset of the project, there was good reason to assume that the study would reveal parallel but unconnected clusters of individuals in cells unique to regions and activities. Instead, the study shows that there is one big connected network as opposed to many smaller networks. Terrorists and narcotics dealers play a critical role in connecting disparate parts of the network. While conventional wisdom suggests that criminals want little to do with terrorism, the structural analysis suggests that terrorists are likely to act as brokers linking unconnected groups.

The rest of the paper will proceed as follows. The next section will summarize the methodological approach and the pseudo-experiment that generated dataset. This will be followed by a description of the network and then there will an empirical assessment of convergence. The paper will conclude with some brief policy considerations.

## Method

Many studies of crime-terror convergence have relied on case studies that reflect aspects of organizational ties or operational similarities. Some of the work pushes beyond case studies to map specific networks and then uses a comparative analysis to explain how convergence differs across contexts (Clarke and Lee, 2008; Rollins and Wyler, 2010). Thus far, there are few studies that rely on quantitative assessments, in part because of data availability.

This study of transnational illicit networks is one of the first open source large-scale assessments, and it leveraged a data source developed for financial compliance. The proprietary data was drawn from a number of open source platforms that included court documents, designation files, and media reporting. The data source held information on individuals and entities in dossier format. One of the data fields, common in law enforcement, included known associates. The research team specifically focused on connections, activities and geographic areas of operation. This data was then structured to conduct network and econometric analysis.

The project started with a simple question: how often do terrorists enter the transnational criminal network and in what types of numbers? The researchers designed and conducted a pseudo-experiment to answer this question. Since the emphasis focused on the convergence of criminal terrorist connections, and specifically the prominence of terrorist ties to criminal networks, the first step involved developing a list of major transnational smugglers. This initial list targeted individuals operating in the areas of narcotics, arms, and people smuggling. This exercise leveraged a wide range sources to include DEA briefs, media sources, and reports produced by non-governmental organizations focused on major smugglers, or kingpin-type characters, operating over the past decade.

Many studies of social networks rely on a method commonly referred to as a snowball sample (Tichy, Tushman, and Fombrun 1979; Moore 1979). In traditional snowball experiments, respondents are asked who they know, which provides the raw data for an “ego network” that puts a single person in the middle. The list of people around the central node or person is referred as the first-degree connections. Experiments then frequently build on that baseline by asking each of the first-degree connections who they know. Like a snowball, the further one goes from the first individual at the center of the ego network the larger the network graph usually becomes. While snowball method does not produce a random and representative sample that serves as a cornerstone of experimental methodology, it does provide an effective approach to building out a network map.

By selecting forty different individuals to use as “Node-0,” the project tried to minimize the problems usually associated with snowball sampling. In a sense, the team began rolling forty snowballs with major transnational smugglers at the center of each. Using the data on known associates, the team generated a social network that incorporated the associates of the major figure (first degree connections) and the associates of those associates (second degree connections). This process is reflected in Figure 2.

The data source used in mapping the social connections also coded the individuals’ illicit activity that led to their inclusion. Individuals are coded for their involvement in terrorism, narcotics, organized crime and financial crime. Other designations include political figures, diplomats, military leaders, and suspicious individuals. People are only included in the database when there is an official designation, a court proceeding or there exists sufficient evidence to warrant doing further due diligence on financial accounts. Each individual in the database received a single designation for their activity, which is most frequently derived from legal designations and filings. The coding of illicit activity in the database serves as a method of generating a blind experiment. Those involved in this research did not code the individuals in the database, instead using the designations upon the conclusion of the network mapping.

Figure 2 shows how the network sample was derived. The forty transnational smugglers that served as the departure point connected to 754 individuals. Of that group, eighty-six were coded as terrorists and 221 were involved in narcotics. There was little surprise that major transnational crime figures would have more criminal than terrorist connections, but the eighty-six still represents 15 percent of the connections. Those 754 individuals in the first degree connected to a further 1,942. Among that group, the number of terrorists spiked sharply adding an additional 404 compared to 392 involved in the narcotics business. The number of terrorists increased at a rate of 370% compared to the growth rates of 158 percent and 77percent for the entire network and narcotics smugglers, respectively.

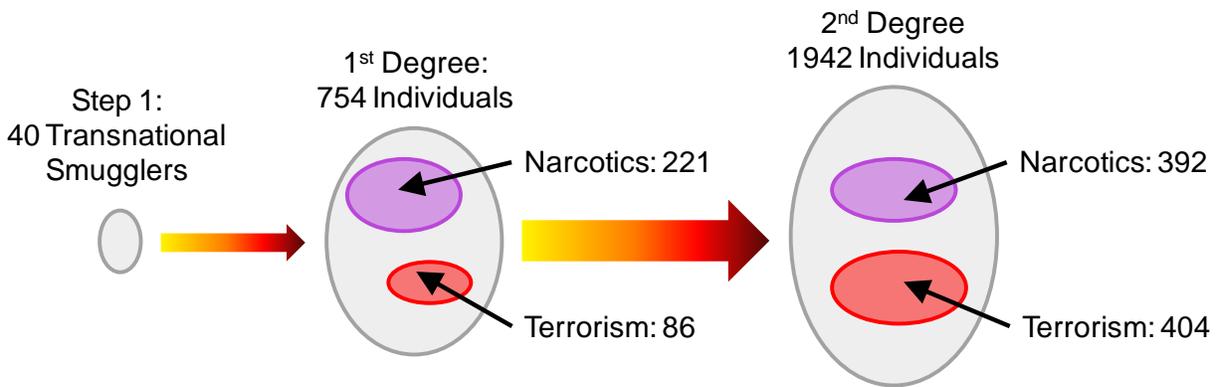


Figure 2: Network Construction

The final component leveraged for this analysis was the geographic distribution of the actors in the illicit networks. The individuals in this study operated across 122 countries spanning every continent. Approximately one-third of the people in the study operated in more than one country, with some moving between as many ten different countries. There are some actors whose locations were simply identified as unknown, however, this only represents about 5 percent of the sample.

### Unexpected Patterns in the Illicit Superhighway

At the outset of the project, there was no reason to assume that the forty individuals on the initial list were part of a common network. For example, individuals involved in the narcotics business in South Asia might not be connected to those selling narcotics in Latin America. There was also little reason to assume that individuals involved in narcotics, arms or human smuggling would be part of the same network. A reasonable assumption would predict modest interconnectivity based on industries and geographic centrality. One could predict that narcotics smugglers in Afghanistan or South Asia were part of the same network just as those involved in the Latin America narcotics trade might be connected. This reasoning led to a prediction that the forty smugglers would be allocated across a series of parallel networks based on geographic centers of gravity and the nature of illicit activities.

The results of the mapping experiment, when the network was completed, were surprising to say the least. The parallel networks converged into an almost fully connected system. Narcotics smugglers in South Asia were linked to narcotics smugglers in Latin America, and were often separated by only a single degree or relationship. These individuals might be connected by narcotics smugglers in North America, terrorists in Africa, arms dealers in Eastern Europe or financial criminals in Europe or offshore safe havens just as an example. In many cases, individuals were linked by multiple relationships. Figure 3 shows how the networks developed, beginning with the initial list of transnational smugglers (window 3a), progressing to the 754 first degree connections (window 3b), and finally the full sample of individuals (window 3c).

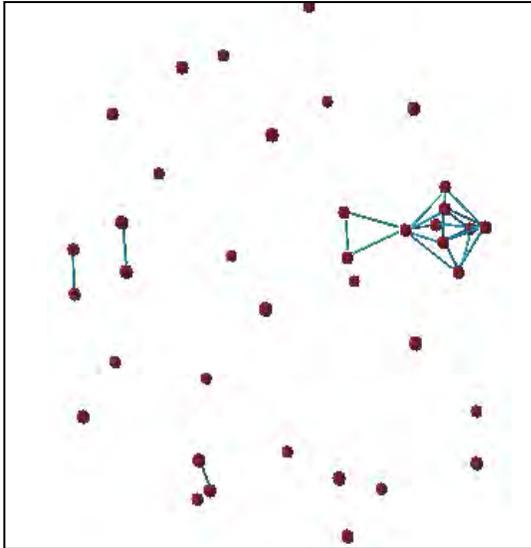


Figure 3a: The big 40

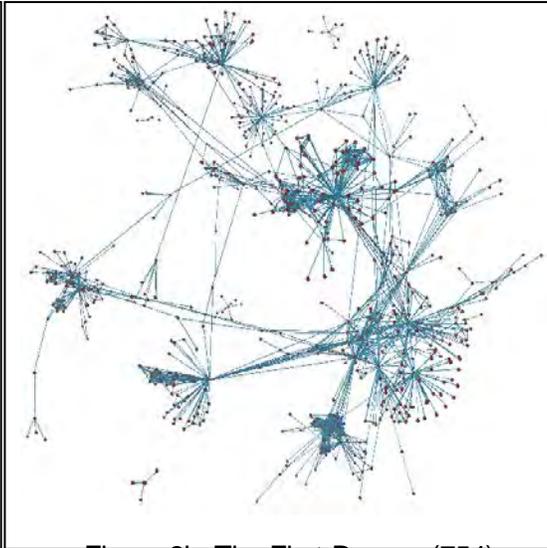


Figure 3 b: The first degree (754)

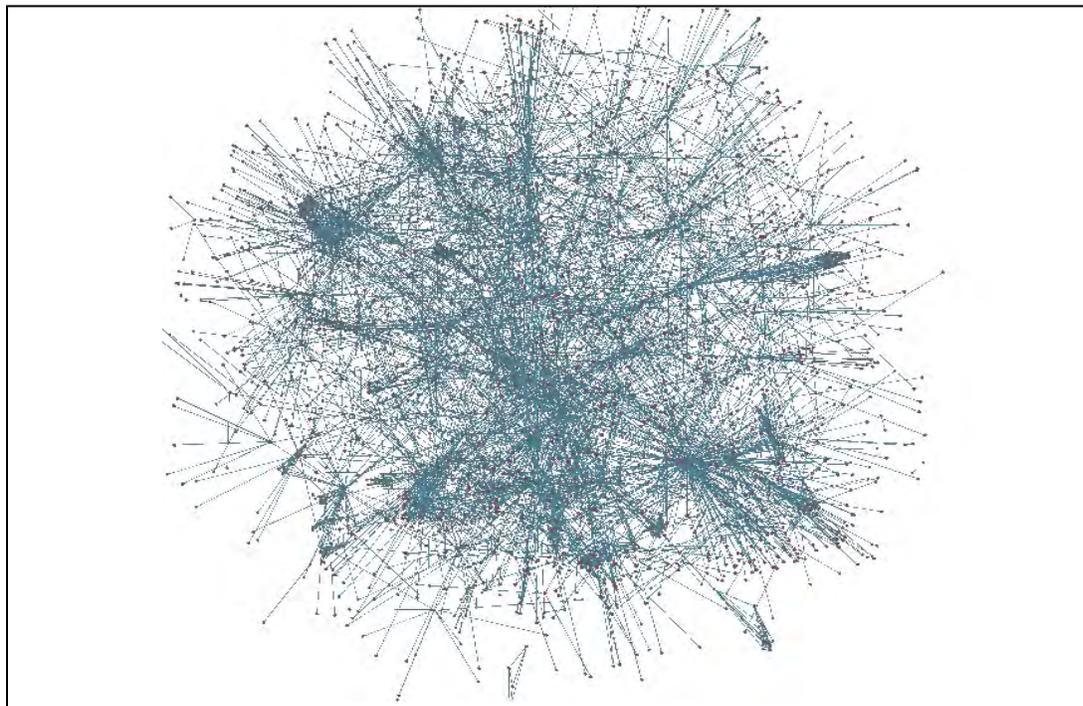


Figure 3c: Connected network (2739)

Figure 3: Evolution of Network Map

At the outset of the mapping exercise, window 2a, parallel networks seemed possible or likely. There was one connected group of ten individuals, and three smaller components that each comprised of two individuals that worked with one another. The remaining sample, which included more than 50 percent of the original list, is unconnected to other kingpins or top smugglers. It would be reasonable to assume that many of these individuals run networks that might remain unconnected, thus giving rise to parallel networks of illicit activity. This expectation collapses by moving a mere step to include the known associates of the kingpins. Figure 3b shows that the vast majority of the unconnected individuals in window 3a are actually linked together by common associations. There are nine components, meaning

nine parallel networks, as opposed to twenty or thirty. Almost 700 individuals are subsumed within the largest of the parallel networks. This 700-person cluster is often referred to as the giant component.

The existence of parallel networks collapses almost entirely when the next step of known associates is mapped out, often called the second degree of separation. The second-degree network includes more than 2,700 individuals and eight parallel components or unconnected networks. The fascinating part is that the second largest of these parallel networks is merely eighteen people. The third and fourth largest parallel networks are nine and eight people, respectively. The rest of these smaller networks includes just four and five people. That means a mere fifty-three individuals of 2,739 were unconnected to the larger network. Approximately 98.1 percent of the individuals were a part of the connected network, separated by a single associate (first degree) or an associate of an associate (second degree). This does not mean that everyone in the network is two degrees removed from the other, but that two degrees of separation was sufficient to connect a large number of major illicit figures operating across functional domains and geographies.

It is important to recognize that a graph connected by two degrees of relationships does not mean that everyone has access to one another through one or two individuals. Two degrees was sufficient to link 98 percent of the individuals, but many of them may be quite (socially) distant. Figure 4 helps to shed light on the nature of connectivity of the global illicit network mapped and studied here. The graph in Figure 4a shows the distribution of connectivity within the network. More than half of the participants, 1,676, link to only a single individual. This is not uncommon in many networks. Studies across the social and biological sciences suggest that many networks are characterized by a large number of actors with relatively few connections, say one or two, and a smaller number of well-connected nodes (Barabasi, 2003). Thus, the large number of individuals with a single link to the illicit network is not surprising. The nature of the data collection may also inflate that number, since the network mapping stopped with at participants two degrees removed from the top forty individuals. Mapping out an additional series of relationships would likely cut the number of individuals with a single connection.

While the distribution of connections in the network is consistent with studies of network structure across many other fields, it does differ in some important ways. An examination of the path length to move between any two individuals, often called the geodesic or social distance, suggests that the vast majority must travel through four to nine other individuals for an introduction.<sup>24</sup> As mentioned above, the network may be almost fully connected by looking at the associates of associates, but almost 10 percent of participants would have to connect through as many as fourteen other participants before getting an introduction. Only about 3 percent of the network could reach anyone directly or through a friend. The presence of large path lengths also reveals something important about structure that serves a slight deviation from many networks.

---

<sup>24</sup> See Stephen P. Borgatti, "Centrality and Network Flow," *Social Networks* Vol. 27, No. 1 (Jan. 2005), 55-71.

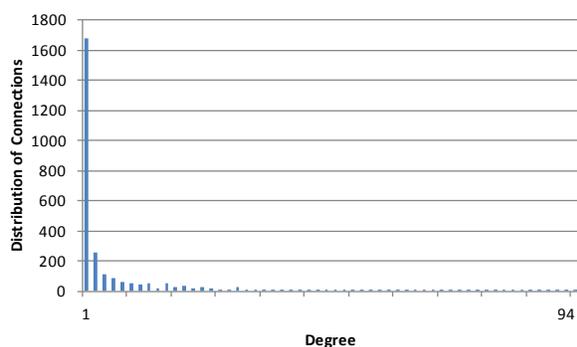


Figure 4a: Degree distribution

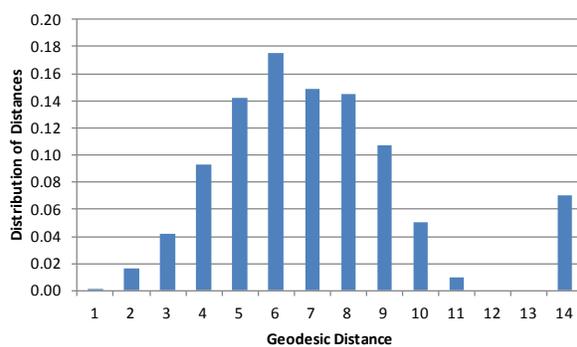


Figure 4b: Shortest paths

Figure 4: Network Connectivity Characteristics

Many studies of network science across disciplines find a hub-and-spoke structure, characterized by the few very well connected and the many peripheral individuals. Often these networks follow an 80-20 rule where 80 percent of the connections are held by 20 percent of the participants (Barabasi, 2003). This type of hub-and-spoke structure often explains the efficiency through which materials and information pass through a network since the relatively well connected can move things to participants in relatively few steps. The existence of long-path lengths, those above seven, suggests that there is shortage of hubs. An analysis of the Lorenz Curves associated with the network shows that it falls short of meeting an 80-20 rule (Newman 2005). Approximately 20 percent of the participants account for 65 percent of the connections. While this still has some of the characteristics of a hub-and-spoke network, it reflects the absence of a few super-connected individuals or a shortage of modestly connected individuals.

The details of the network analysis may seem esoteric it actually reveals some insights with policy implications. The network may experience inefficiencies in moving materials and information between distant parts despite being connected. Those that link these disparate groups are particularly important. More so, it suggests that the distribution of relationships is such that it is difficult to disrupt the activities of the global network by targeting a few kingpins. Such a strategy would work if there were a few hyper-connected individuals, but the relative shortage of these super-connectors means that the network is likely to withstand their removal. There is a similar though more extreme finding on terrorist networks (Helfstein and Wright 2011). The analysis shows that there are almost 11,000 relationships in the network, and the average participant knows four other individuals. There is a significant spread of connections despite the fact that a large number know only a single individual. Policies aimed at complicating business activities, particularly those across groups, geographies and activities may consider ways exploiting the presence of social distance and perhaps consider ways of disrupting flows by making them longer. This of course is only based on an assessment of network structure and it is important to consider additional insights drawn from incorporating activities and geographies.

### Illicit Activity and Geographical Spread

The network here includes individuals involved in different types of illicit activities. It is possible that these groups, despite being connected in the network in figure 3c, are quite segregated. This would be consistent with many of the arguments that counter convergence (Naylor 2002). These different illicit industries might occasionally work together through intermediaries, but their separation might be the

reason behind social distance. The data here are amenable to addressing just such an issue. By color-coding the different nodes in the network based on the illicit activity they are associated with, it is possible to explore the relative degree of segregation and convergence. A high degree of segregation would be marked by a network with patches of different colors in each quadrant of the graph. For example, all the terrorists colored red might reside in the upper right, while purple narcotics smugglers exist in the upper left and organized criminals in the lower right portion. Figure 5 provides little evidence of segregation.

The network in Figure 5 seems to reflect a reasonable degree of convergence between terrorists and those involved in other types of illicit activity. The visual evidence suggests that terrorists are distributed throughout the network. In some cases, there might be one or two individuals involved in terrorist activity subsumed in criminal networks, but in other cases, there are large clusters of terrorists with multiple connections to criminals. Empirical analysis of the networks show that 46 percent of terrorists' connections link to those involved in activities other than terrorism, and those involved in other illicit activities link to terrorists 35 percent of the time. This latter statistic is telling, since it challenges the conventional wisdom that most criminals eschew relationships with terrorists to avoid drawing the ire of national and international authorities. Almost 20 percent of all the connections identified cross the criminal-terrorist boundary, and more than one-third of criminal social connections tie to terrorists. Terrorists are also a party to 43 percent of total social connections in the network, which indicates that they are prominent social connectors in the network. Their relations are not restrained to fellow terrorists since those links only account for 54 percent of their connections.

Table 2 shows the summary statistics across individuals involved in different activities. One interesting finding is that the network is saturated with almost as many terrorists as those involved in narcotics, and the number of those involved in terrorism significantly outweighs organized and other types of criminality. That is a significant finding since the initial targets of the inquiry were all criminals. Despite the initial focus on transnational smuggling, the network is nonetheless populated with a number of people designated as terrorists.

The table also shows existence of some substantive structural differences across individuals based upon their activities. The average individual in the network was connected to four others, but those involved in narcotics and terrorism are substantially more connected than others. The average degree measure shows that narcotics had the highest average connectivity with individuals linking to almost six others followed by terrorists with an average connectivity score of almost five. Interestingly, organized and other criminals were on the low end of the connectivity scale.

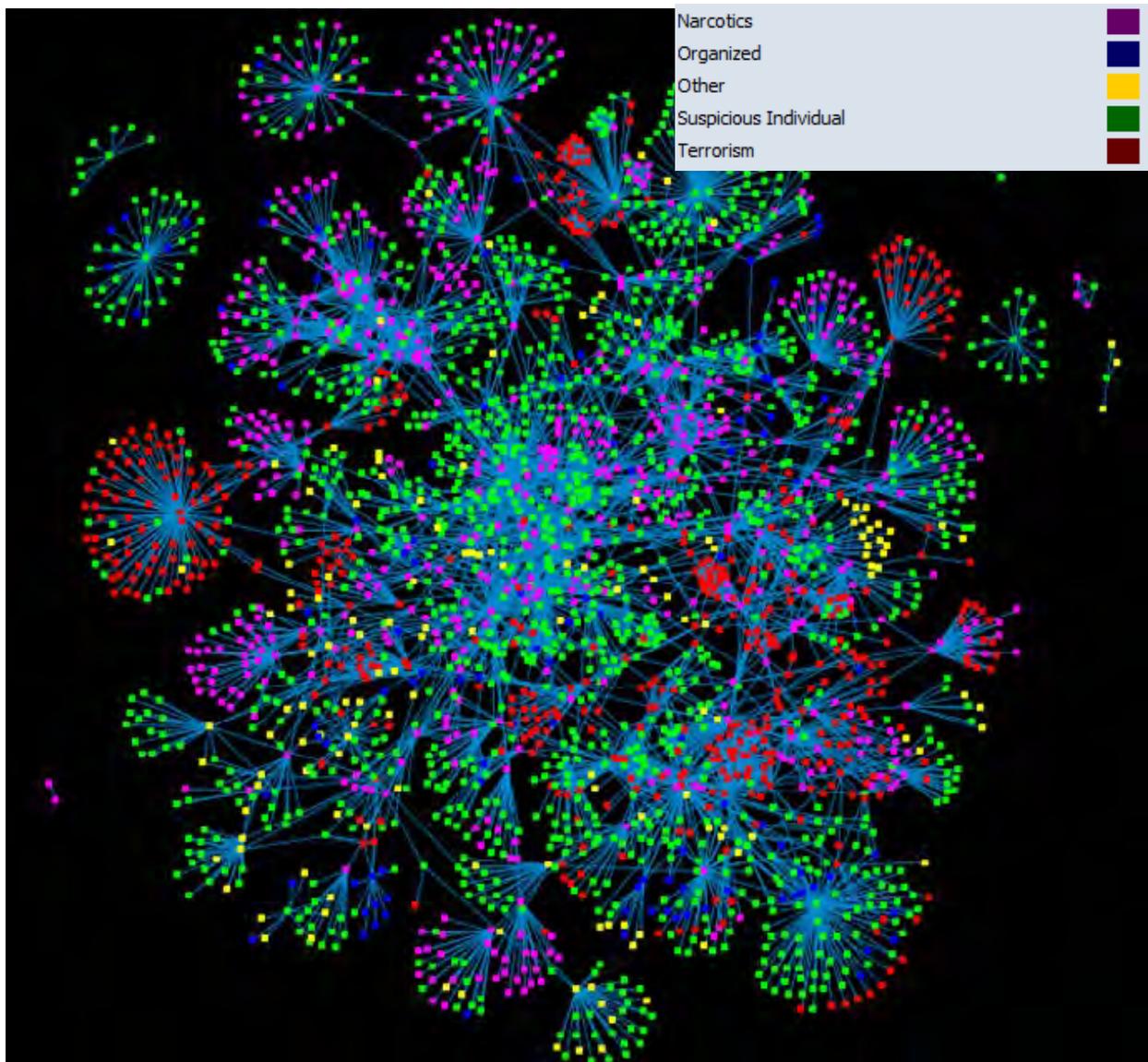


Figure 5: Network with Activities

Table 2: Summary Statistics by Illicit Activity

<b>Activity</b>	<b>Individuals</b>	<b>Average Countries</b>	<b>Average Degree</b>	<b>Average Betweenness</b>	<b>Average Closeness</b>
Narcotics	633	1.34	5.941	0.502	0.959
Organized	77	1.30	2.973	0.125	0.918
Other	121	1.25	2.934	0.044	0.867
Political	68	1.20	3.426	0.129	0.959
Suspicious Individual	1343	1.18	3.015	0.055	0.919
Terrorism	497	1.65	4.881	0.204	0.962
<b>Total</b>	<b>2739</b>	<b>1.30</b>	<b>4.037</b>	<b>0.189</b>	<b>0.935</b>

The number of connections an individual has is the most common way of conceptualizing connectivity and network structure, but there are a number of other measures utilized. Those with high betweenness scores link disparate parts of the network and has led some to describe the role of those people as boundary spanners (Freeman, 1977). In the illicit world, individuals with high betweenness are those like

Ilyas Kashmiri, Monzer al-Kassar and Victor Bout who connect with people from different social spheres around the world. Those involved in the narcotics trade have the highest average betweenness scores, but surprisingly, terrorists had the second highest average. This further challenges the idea that others in the illicit world eschew terrorists because of their stigma or the related security concerns. The analytics suggest that terrorists actually play a reasonably important role linking disparate cells and groups to one another. Those involved in drugs and terrorism are the most likely boundary spanners.

Another way of thinking about connectivity uses a measure called closeness, which examines how many links must travel through to reach others (Rowley, 1997). The higher the score the closer an individual is socially to everyone else making it easier to connect with others or funnel resources. Unlike the betweenness scores, which showed some significant deviation, the average closeness scores of the six groups are relatively similar. Terrorists are actually the closest to others in the networks followed by those involved in narcotics and political crime. Criminals classified as other had the lowest score, but the difference between the highest and lowest scoring was less than 0.1. The closeness scores suggest that the network is reasonably close, though the distance analysis suggested that there is more complicated connectivity story.

The network analytics suggests that terrorists are no more or less operationally secure than other criminal enterprises. They are deeply imbedded in the larger criminal network, they span boundaries to link otherwise separate clusters or organizations, and they are relatively close to others in the network. These results might be interpreted to suggest that the most effective means of countering such a global illicit network involves a mixture of tools used to counter criminal activity in conjunction with those used to counter terrorism.

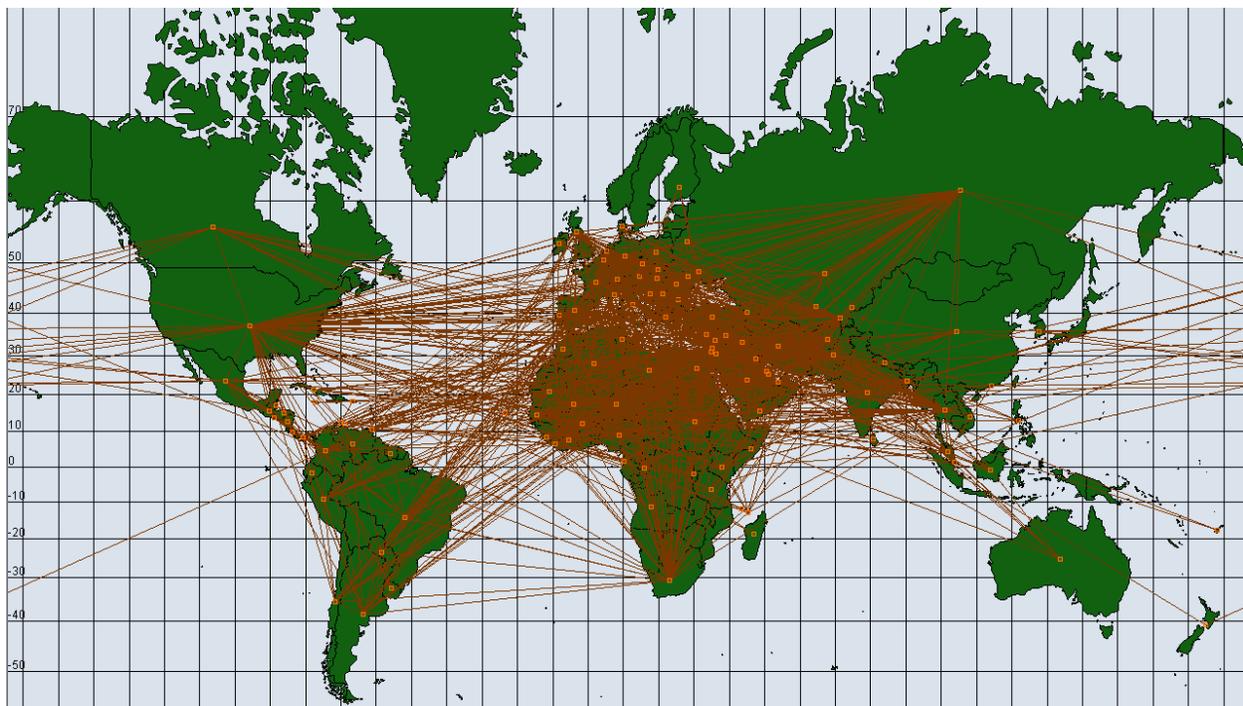


Figure 6: Country Connectivity

The network spanned 122 countries and there are some interesting aspects associated with connectivity across geography. Figure 5 offers a visual assessment of inter-country connectivity. While one could generate a geospatial network analysis of individuals, the sheer size of the network with 2,700 people operating in 3,600 places linked by 15,000 connections, the actual map would be blocked out by lines. Instead, Figure 6 summarizes the transnational relationships by looking at which countries have illicit connections to other countries. The node markers for each country are center-mast, and it shows the global reach of the network under study. There are over 1,000 country-to-country relationships spanning the globe.

While the map offers visual representation of the network, further empirical assessment helps draw insights that might otherwise be difficult to identify. For example, Table 3 shows the countries that have the most individuals and the most convergence between criminal and terrorist actors as represented by social connections. Countries with the most illicit actors tied to this network include Mexico and Columbia, due in large part to their narcotics business and terrorist groups. The U.S., as the world's largest consumer economy and a frequent target of illicit goods, also ranks high. It is followed by countries such as India and Pakistan with well-documented underworld economies that blend profit motives with ideological drive. There are also a number of countries that play an important role, often unwittingly, in facilitating illicit activity by providing sanctuary or access to the financial system.

The list of the countries with the most illicit actors is not quite the same as the list with the greatest convergence in criminal and terrorist relationships. It is also interesting to note that the list of countries with high convergence does not align with conventional wisdom. Generally, convergence is cast as a phenomenon in weak, failed or poor states.<sup>25</sup> The narrative behind this hypothesis is that governments are incapable of acting against the illicit activity, so criminal and terrorist elements have little to fear from working together. This type of collaboration is expected to be especially useful in poor countries where the combination of terrorism and criminal activity will allow groups to persist that might otherwise starve for resources in these meager environments.

Table 3: Prominent Countries

<b>Rank</b>	<b>Number of Individuals</b>	<b>Crime-Terror Convergence (by Link Count)</b>
1	Mexico	Colombia
2	Colombia	United Arab Emirates
3	United States	India
4	India	United States
5	Pakistan	Russian Federation
6	United Arab Emirates	Pakistan
7	Afghanistan	South Africa
8	Syrian Arab Republic	Liberia
9	Spain	Belgium
10	Argentina	Mexico
11	Korea, Rep.	Thailand
12	Brazil	Tajikistan
13	Iraq	Syrian Arab Republic
14	Saudi Arabia	Spain
15	Nicaragua	Panama

<sup>25</sup> For example, Rollins and Wyler, 2010 discuss the importance of ungoverned space in convergence.

The list of the top fifteen countries here, however, belies this thesis and suggests that the opposite may be true. Eleven of the top fifteen on the convergence list are among the largest 30 economies in the world. Approximately 70 percent of the countries where convergence is prominent are among the richest in the world. Only four, Liberia, Pakistan, Panama and Tajikistan, are examples of small or poor economies. While more analysis is needed to understand these patterns, initial analysis suggests that conventional wisdom about crime-terror convergence may be incomplete.

It seems as though convergence is most prominent in relatively wealthy countries, which by extension tend to have reasonably well functioning governance mechanisms. This may in fact help explain why convergence is more prominent in wealthy countries. Terrorist and criminal elements are only successful for extended periods of time when they can achieve negative political control, that is deny others the ability to govern certain space. That space may vary to include physical or legal spheres such as land or banking regulations. Generally speaking, poor countries already face a governance challenge, so it may be relatively easy for illicit actors to achieve negative political control. Groups may not need to work together and synergize in these environments. By contrast, denying governance in rich countries with capable government apparatus is likely to prove far more difficult, making potential collaborations across illicit elements more valuable.

### Conclusions and Implications

The analysis above provides an interesting perspective on global illicit activity. There are certainly limitations, as with any type of study delving into the clandestine. This analysis is static and therefore captures relationships that have been documented over time. Some scholars have correctly identified that groups or individuals might work together for certain periods of time and then terminate their relations (Picarelli and Shelly, 2002). This is true, and ideally a dynamic network might account for these, but it also shows that over time convergence between those involved in different activities across the illicit universe is not exceptional. It is a regular course of doing business for many. The high degree of connectivity is the first major conclusion that one should note.

While the prominence of connectivity is clear in this effort, it begs the question why this insight has up until recently eluded a community of interest deeply involved in addressing the issue. One reason lies in the distinction between means and ends. The policy community and by extension the analytical community have generally distinguished between illicit actors according to their ends. The economic ends of narcotics dealers and organized criminals are different than the political ends of the terrorists. At times, the violence associated with crime drove the government to pursue groups like the mafia and the Cali Cartel, but it is often treated as a law enforcement issue. Terrorists with their political ends may be a nuisance or may present a much greater threat depending on their ideology and capabilities. This distinction according to ends may have masked a convergence in means that is increasingly prominent.

While criminal elements seek economic profit, they usually require some sort of sanctuary to safely pursue and accrue the rewards. Governments have incentive to limit this operating capability, meaning there is a dispute over governance. Governments, in theory, aim to govern territory and apply their system of law and order, while major criminals often seek to deny others the ability to govern in certain physical or virtual spaces. It is in this denial of governance where criminals and terrorists converge most in means and ends. Terrorists, by many definitions, are trying to overturn the political status quo. At a minimum, they want to hamper government activities and ultimately deny them the capacity to govern

in the hopes of putting a new political regime in place. It is in this final step that terrorists are substantively different than most criminals, where the latter has no interest in governing. That said, hampering or denying others the opportunity to govern is an intermediate step for both criminals and terrorists. For criminals, denying governance is a step towards pursuing their illicit profits with less risk. For terrorists, denying governance is one step in the course of overturning the political status quo. It is in this intermediate step, denying governance or achieving negative political control, that terrorists and criminals are most likely to converge and work together despite different ends.

## Chapter 5: Analyzing and Evaluating Criminal Organizations

Daniel J. Mabrey, Ph.D.

[dmabrey@newhaven.edu](mailto:dmabrey@newhaven.edu)

Richard H. Ward, D.Crim.

[rward@newhaven.edu](mailto:rward@newhaven.edu)

University of New Haven

### Introduction

In announcing the nation's new strategy to combat TOC, the National Security Council identified ten areas that pose strategic threats to the United States and its interests abroad. Common to all these areas in the strategy is a focus on identifying and disrupting criminal organizations and the networks that support and enable them. Much of the literature—scholarly and professional—has focused on disrupting criminal organizations. Important contributions like Dr. Michael Kenney's book *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* make insightful observations about the nature of organized crime and the ability of government to counter and disrupt these agile adaptive networks. Indeed many analytical approaches to understanding organized crime focus on the structure, topography, and features of the networks. These approaches are not misplaced; understanding the structural dynamics of criminal networks through modern analytical techniques is definitely important and necessary.

The National Strategy definition of TOC refers to:

...those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.

Disentangling this complex definition reveals that organized crime is usually perpetrated by groups of all shapes and sizes. These groups are more easily understood as criminal organizations that are neither monolithic nor homogenous. COs run the gamut from small, sparsely connected clans and cells to wide-ranging bureaucratic organizations that more closely resemble multi-national corporations than gangs.

The emphasis in the scholarly and professional literature on analyzing network structures appears to be skewed toward the types of criminal organizations that lend themselves to these types of analyses—namely larger, hierarchically-organized groups like global TCOs with wide-ranging networks. Less emphasis has been placed on assessing and evaluating criminal organizations to understand the dynamics of the organization that affect, and sometimes drive, the network structures that are present. The literature that does address this topic tends to be concerned with developing threat assessment frameworks for prioritizing organizational resources to counter criminal organizations. The most prominent of these frameworks is the SLEIPNIR organized crime groups capabilities measurement matrix developed by the Royal Canadian Mounted Police to drive their intelligence-led policing model. In

SLEIPNIR, the RCMP uses a modified Delphi method to elicit expert opinions about the capabilities of organized crime groups in Canada according to a fixed set of attributes, which include the following.

- Corruption
- Violence
- Infiltration
- Money Laundering
- Collaboration
- Insulation
- Monopoly
- Scope
- Intelligence Use
- Diversification
- Discipline
- Cohesion

Whereas the SLEIPNIR model developed by the RCMP is widely documented in both academic and unclassified professional literature, unclassified research for this and other publications has not yielded a similar or comparable methodology in the United States.

This chapter discusses in greater detail some of the issues related to assessing and evaluating criminal organizations and concludes with a discussion of an approach developed by the Institute for the Study of Violent Groups at the University of New Haven to assess and evaluate criminal organizations worldwide. The approaches described here do not aim to replace or supersede analytical approaches to understand criminal network structures, but should complement these analyses with a systematic, structured understanding of criminal organizations.

### **Criminal Organization Hierarchy**

The National Strategy aptly pointed out that “there is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures. The crimes they commit also vary.” The amorphous and heterogenous nature of organized crime requires an assessment and evaluation approach that can be applied to all types of groups, regardless of size, structure, and criminal enterprise.

The Institute for the Study of Violent Groups (ISVG) has been researching terrorism, extremism, and transnational crime for more than 10 years and has compiled a comprehensive unclassified database of these groups and their activities. The database has more than 250,000 events since 2002 perpetrated by more than 4,000 organizations and more than 50,000 individuals. Through this database of networks and actors, ISVG has been able to develop an inductive understanding criminal organizations globally and how they are associated with terrorist and extremist organizations. In assessing criminal organizations worldwide, ISVG developed a criminal organization hierarchy that seems consistent across countries and over time.

This hierarchy has six levels is generally consistent with the description of transnational organized crime provided in the National Strategy. Figure 7 below presents the hierarchy below. The bottom of the

hierarchy represents the simplest and most common forms of criminal organizations while the top of the hierarchy represents the most complex and least common forms of criminal organizations. A discussion of this hierarchy is beyond the scope of this paper, but nearly all criminal organizations in a country can be classified into one of these levels.



Figure 7: Criminal Organization Hierarchy

Establishing this hierarchy does not fully assess or evaluate criminal organizations, but rather creates “bins” by which to organize the multitude of groups within a country. A group-level framework that can be systematically applied to any group at any level of the hierarchy is required to effectively assess and evaluate these criminal organizations.

### Analyzing and Evaluating Criminal Organizations

Aside from the SLEIPNIR measurement matrix developed in 1994 by the RCMP, the scholarly and professional literature on assessing/evaluating criminal organizations has been largely bereft of assessment or evaluation methodologies for criminal organizations. In 2012, the International Peace Institute (IPI) released a report titled “Spotting the Spoilers: A Guide to Analyzing Organized Crime in Fragile States”<sup>26</sup> that prescribed a well-rounded approach for analyzing criminal markets and the organizations that exploit these markets. In very plain and direct language, this guide provides a step-by-step guide for how policy makers and/or analysts can identify and measure criminal organizations in fragile states.

[I]dentifying and measuring hidden criminal activities is a significant challenge. Those involved generally don’t register what they are doing, and in countries that have just experienced conflict and where state institutions have been destroyed there would be few people with the means to record it, even if they were interested.

<sup>26</sup> See also [http://www.ipinst.org/images/pdfs/ipi\\_epub-spotting spoilers.pdf](http://www.ipinst.org/images/pdfs/ipi_epub-spotting spoilers.pdf)

Here lies the real challenge of the assessment. It will not be enough to label each problem as “serious” or of no consequence unless some hard data can be produced to back up the point. To be credible you need evidence, but because you are dealing with illicit activity in a fragile state, that evidence will be hard (and potentially dangerous) to find. But again, you are not trying to collect evidence to put someone on trial. You are trying to form a general assessment of organized crime and its impact on the society where you are trying to keep or build peace. So the challenge is to find enough dots, and then connect them.

In each of the thematic areas that you have identified for possible investigation you will need to think up and preferably write down a plan as to how you are going to find relevant data over a specific period (for example, volumes of seizures or number of convictions). This is not a question of finding one or two golden sources of numbers that can be used to judge the extent of the problem; rather, it will mean finding lots of different measures that can be compared and contrasted to enable you to understand what is going on. (pp. 14-15)

The report then provides an example of the thought processes and questions an analyst would need to answer for a specific thematic area – drug trafficking. The IPI framework differs from the SLEIPNIR and other “threat assessment” approaches because it focuses on understanding criminal markets, and the opportunities in these markets that can be exploited, rather than criminal organizations themselves. The questions posed in this framework are not dissimilar from how an analyst would assess or evaluate a criminal organization exploiting these markets.

### Order of Battle Analysis – Transnational Organized Crime in Mexico

The IPI framework published in 2012 is similar to a traditional military intelligence analytical approach called order of battle, which is the identification, command structure, strength, and disposition of personnel, equipment, and units of an armed force participating in field operations.

From 2008-2012, the ISVG at the University of New Haven performed order of battle analysis on TCOs operating along the US-Mexico border. ISVG worked with Mr. Thomas Davidson III, CW4 USA (Ret.) to modify the traditional U.S. Army order of battle approach to better understand and measure the capabilities of organized crime groups and then systematically applied to the largest cartels operating in Mexico including: the Gulf, Sinaloa, Juarez, and Zetas cartels. ISVG’s transnational organized crime order of battle includes the following sections:

- Area of Operation
- Background
- Firsts
- Links to Other Organizations
- Corruption
- Membership
- Tactics & Operations
- Training
- Weapons and Ammunition
- Funding/Money Laundering
- Effectiveness

ISVG’s complete order of battle for a cartel is usually 50+ pages of technical writing supported by graphics and visualizations. For this chapter, selected portions of the Los Zetas order of battle from December 2011 are presented here to illustrate the modified approach. Although applied to Los Zetas,

which is clearly a top-level group in the criminal organization hierarchy, this analytical approach can be applied to any criminal organization at all levels of the hierarchy.

### Areas of Operation

The geographic profile of the cartel; focuses on three primary measures – control, dispute, and presence— reported at cascading levels of geo-specificity. The geographic administrative features of Mexico that we used to assess area of operation are State (estado), Municipality (municipio), and Neighborhood (colonia). Presence indicates that a cartel has a reported presence in the area, but is not in control of an area or contesting control of the area with another organization. Dispute indicates that a cartel with presence in an area is contesting the control of the area with another group, usually through violence and intimidation. Control indicates that the cartel commands and directs the illicit activities within a designated area. Figure 8 provides an example of area of operations in Northeastern Mexico for 1 week in late 2011.

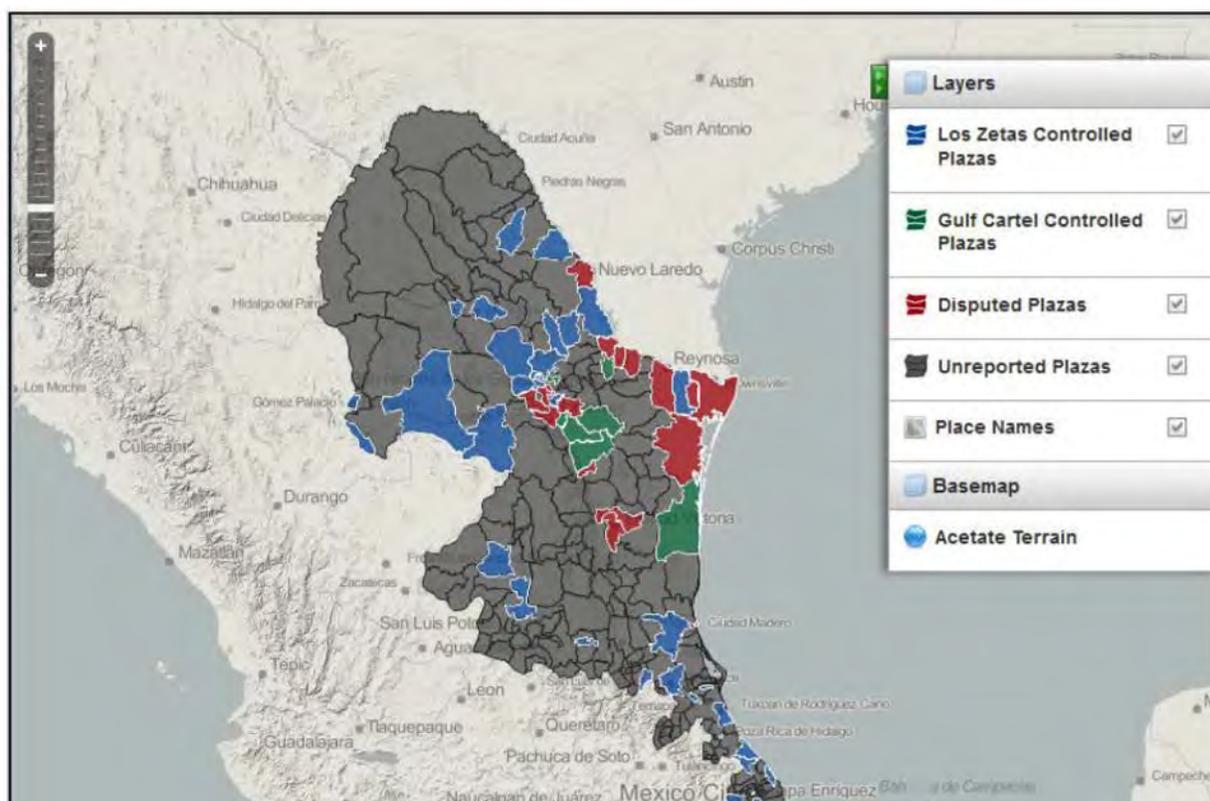


Figure 8: Areas of Operation for Los Zetas in Northeast Mexico in late 2011

### Background

This section includes basic information about a criminal organization’s composition, disposition, and strength. This includes a description of the organization’s headquarters, leaders, rank hierarchy, and history. Figure 9 provides an example illustrating the Los Zetas cartel’s leadership and hierarchy as of June 2011.

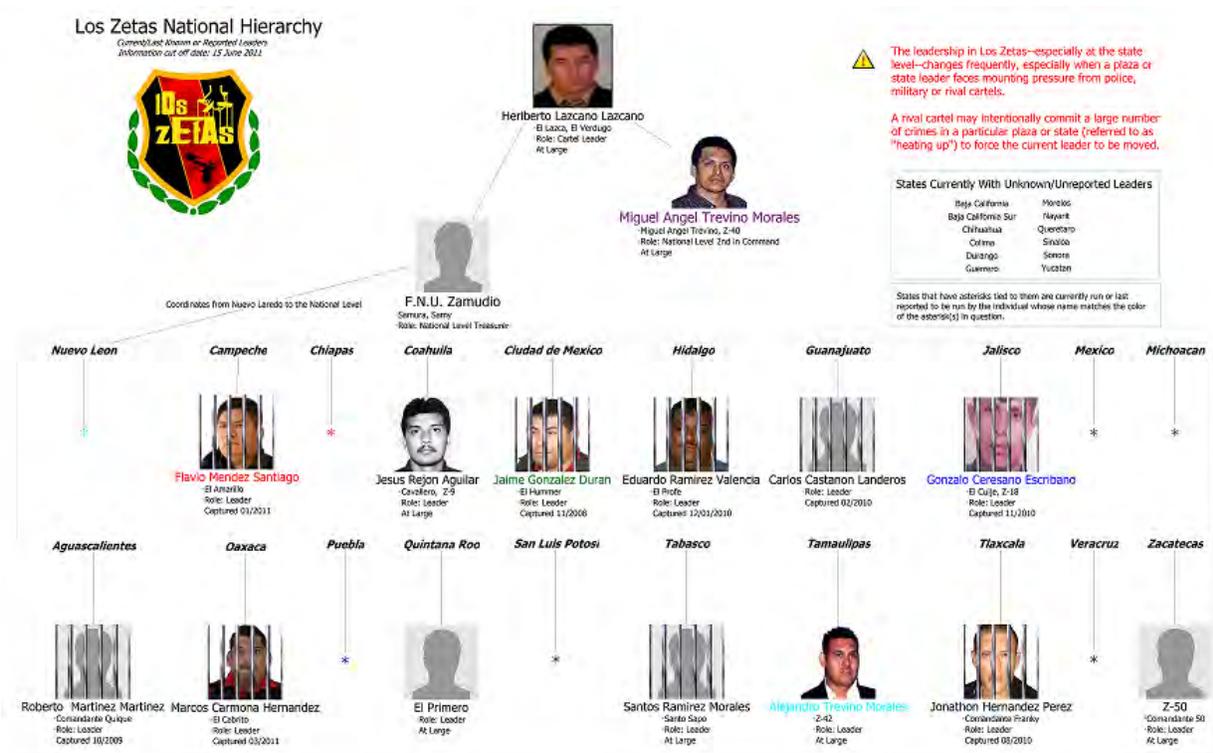


Figure 9: Los Zetas National Leadership and Hierarchy as of June 2011

### Firsts

Organized crime groups are highly innovative and adaptive organizations, capable of quickly transforming to out-manuever law enforcement and security organizations. This section chronicles the innovations and evolutions of a group to assist the analyst understand the impact of these adaptations on a group’s activities. An example of this for Los Zetas follows:

Los Zetas was the first cartel in Mexico to begin modifying vehicles to intimidate and enhance offensive capabilities. The first up-armored vehicles, so-called Monstruos, were recovered in 2010. Between 2010 and 2012, more than 10 versions of the vehicles were identified, most resembling crude tanks rather than regular armored vehicles. The wide ranging vehicle types and modifications suggest a trial and error development approach or even a specialization process in which different styles are utilized for different missions. The larger models appear to be capable of defending against larger munitions and delivering a large number of cartel members to a location under siege, i.e. personnel transport; smaller models have been designed to have armor designed to deflect more munitions than absorb them, i.e. operational attack/escape vehicle.

### Links to Other Organizations

Organized crime exists within communities and the larger political-social environments that require and ever-evolving number of relationships to other organizations. These relationships are often fluid, ranging from positive, to benign, to negative and back again. Understanding the capabilities of organized crime requires the analyst to track and evaluate the relationships for each group. This section chronicles these relationships, the nature, strength, and direction of these relationships.

### Corruption

Organized crime relies on corruption to enable nearly every aspect of their illicit activities. While corruption is usually pervasive, specific relationships are of interest for assessing the capability of

organized crime. Corruption of political officials, law enforcement and security officials, and community organizations are usually the most important indicators to track. This section chronicles evidence of corruption perpetrated by an organized crime group. Examples of Los Zetas capacity for corruption during 2011 are detailed below.

### *Politicians*

Former Cancun Mayor, Gregorio Greg SANCHEZ Martinez, was detained by federal police in 2010 on suspicions of money laundering and helping to protect both the Beltran Leyva and Los Zetas cartels. Sanchez was also accused of participating in the execution of former General Mauro Enrique TELLO Quinones, who was killed one week after taking his new position as the head of a police task force aimed at ending drug-related violence and crime in Cancun.

### *Law Enforcement & Security Officials*

Victor Emmanuel DELGADO Medrano aka El Chumil, after his arrest in March 2011, reported that several members of the Judicial Police (PJE) were on the payroll of Los Zetas in the state of Quintana Roo. El Chumil was a boss in the Quintana Roo state at the time of his arrest. Jose Idelfonso SAANCHEZ Chan, a first commander, was reported to be the go-between for the two groups, taking money in and dispersing to appropriate personnel. Municipal commanders Hugo GARCIA Quintal and Manuel OLIVERA aka El Primo, as well as homicide commander Hugo GONZALEZ Pamplona and theft commander Justo MORENO Lopez, are a few of the named police receiving bribes from Los Zetas (reportedly). The bribes provided were standardized based upon rank; commanders received 7,500 pesos and troops received 6,000 pesos. These were delivered in envelopes, as many as 80, and two envelopes reportedly contained 15,000 pesos, but the destinations of those were "unknown" to El Chumil. El Chumil reported that his knowledge of the bribes indicate it has been ongoing for at least several months. Reports have surfaced of PJE members asking Los Zetas for money for hospital bills for individuals injured in battles with Los Zetas. Los Zetas are known to keep reports and payrolls on who receives what "payments," some of these documents have been discovered and used to investigate corrupt officials. One such list had a reported 25 PJE members indicated.

In a Nuevo Laredo prison a recent breakout of 153 inmates was reportedly orchestrated by Los Zetas. All the prison employees working at the time of the breakout were arrested and are awaiting trial as it is reported the inmates walked past the guards and into waiting vehicles including a yellow school bus. One guard not working at the time confidentially reported the entire prison of 1,200 prisoners was controlled by Los Zetas and that even after the breakout was still under their control as several members were left behind to maintain that control. Prisoners are reportedly forced to pay a fee to Los Zetas for their safety.

Albino SANCHEZ Osorno aka El Babalucas, Abuit ESTUDILLO Ortiz aka El Eco 06, aka El M2, and Francisco Manuel MORA Lopez aka El Pinguino, all former members of the State Investigation Agency (AEI) of Oaxaca were charged for collaborating with Los Zetas by protecting the group in the cities of Istmo de Tehuantepec and Oaxaca de Juarez (the state capital) in March of 2011.

### *Community Organizations*

Churches in Mexico have been accused of accepting "narco alms" from known or suspected drug traffickers. One church even has a plaque dedicating the church to the now deceased leader of los Zetas, Lazcano, which states the church was "donated by Heriberto LAZCANO Lazcano.

### *Membership*

This section captures how organized crime recruits, structures, and maintains its membership and ranks. The complexity and detail of this section varies along the organized crime hierarchy. Generally, groups

at the bottom of the hierarchy have less complex organizational designs than organizations at the top. Los Zetas is clearly in the top tier of the organized crime hierarchy and has a very complex and multi-faceted membership structure. The following are excerpts from ISVG's analysis of Los Zetas' membership as of late 2011.

Los Zetas membership is made up of different operational levels. According to one report, Zetas members are sent to new areas in order to recruit "common" criminals into Los Zetas and they are then trained for a specific task/role, new members can advance to other positions. The tactic of recruiting criminals and military/police is reportedly used by many Mexican cartels now but was pioneered by Los Zetas. It is also reported that new recruits can be "promoted" all the way to the position of hit man, or operativo, in one month, a process that historically took as long as numerous years. This may be a result of rapid turn-over in personnel due to arrests and deaths, as well as an increasing presence in more locations requiring more members. A recent report suggested that Los Zetas had around 17,000 members, second most behind only the Sinaloa Cartel. The call sign of "Z" or "Zeta" is generally reserved for original or "near-original" members who were in the military where the call signal was used to designate rank. "L" is used for other members of note who cannot be designated with the "Z" call signal.

There is also evidence that members are transferred from plaza to plaza when particular areas become too "hot" for them. This suggests an extensive intelligence capability in which Los Zetas are retrieving information about which members are under the scope of the authorities. It has been suggested that rival cartels will intentionally "heat up" an area in order to force a member of the opposition to transfer to a new location.

### *Membership Levels*

- Zetas Viejos: Plaza leader, control operations of entire plaza from assaults, to drug trafficking, to bribery and intelligence gathering. Most Viejos were original members or have been in Los Zetas since shortly after the group's formation. Only those with military experience may be Zetas Viejos, cell and plaza leaders are, however, increasingly made up of non-military and/or non-original members due to the expansion of the group and the capture/death of many original members.<sup>87</sup> Members of this level refer to themselves as Licenciados (Lawyers/attorneys), Maestros (Teachers/masters) or Ingenieros (Engineers).
- Operativos (Operatives): Operatives pick up and kill targets, carry out missions
- Zetas Nuevos: "Shock Troops" are operativos who carry out particularly gruesome and bloody assaults. Zetas Nuevos are made up of those with military or police backgrounds almost exclusively.<sup>[87]</sup> Including Kaibiles from Guatemala.
- Cobras: Provide security for drug shipments and higher level members and leaders, often designated with the call signal "L," which stands for Levantones.
- Cobras Viejos: Experienced Cobras in charge of coordinating trafficking and security matters
- Halcones (Falcons): Monitor military and police activity, informants who most often have no criminal record
- Las Panteras (Panthers): A group of mostly women they perform several functions including; obtain safe houses, purchase provisions and clean/care for wounded. Their main role is to infiltrate authority figures and their organizations, contact police officers, military personnel, mayors and politicians, and civilians, who are targeted to assist Los Zetas. If the target refuses,

the women are trained killers and do not hold back their skills. This group was first noted in 2006 and was formed by El Lazca. Men in this group function mostly as body guards and hostage controllers. Panteras are known to use costumes and to change their appearance depending on their current mission. One Pantera recently captured was Gloria ROJAS Valencia, captured in Venezuela and turned over to U.S. officials, was known to have ties with and worked with Colombian drug cartel member Luis Frank TELLO Candelo, also recently turned over to U.S. officials. Ashly "La Comandante Bombon" NARRO Lopez and Yaneth DEYANIRA Cruz were known Panteras leaders who have been captured already.

- Accountants: Also, it has been reported that each plaza also, ideally, has its own accountant. The accountant is tasked with controlling all of the funding for their plaza and making sure all the members are paid as well as bribes paid and that payments are collected from merchants and others being extorted. The main accountant for the entire organization has been reported as Comandante Sol, who reports directly to El Lazca. When Carlos Adrian MARTINEZ Muniz, number 2 leader of a Los Zetas cell in Monterrey, Nuevo Leon, was arrested in October 2009, in addition to drugs and weapons he had deposit/payment slips for 7,150 different people.

### Tactics & Operations

This section captures the tactics, techniques and procedures that are unique to an organized crime group. Generally, this section analyzes the activities of a group in three dimensions:

- violence/intimidation activities;
- illicit activities; and
- communication/propaganda efforts.

### Training

This section describes how organized crime trains its recruits and maintains readiness among its membership. The following are excerpts from ISVG's analysis of Los Zetas' training as of late 2011.

- In 2001 the majority of training, while still operating for the Gulf Cartel, was transferred to Nuevo Leon. Specifically a ranch in China, Nuevo Leon, known as "Las Amarillas", and a ranch near San Fernando (along the Ciudad Victoria-Matamoros highway), served as the main training headquarters for the early members of Los Zetas.
- Currently there are still "ranches" designed to train recruits, however they know exist throughout their region and the recruits are trained near where they are recruited from until their training commanders believe they are ready.
- One report indicates training is currently around three months long and takes place at ranches known as Arroyos (Creeks) that are located in the states of Tamaulipas, Nuevo Leon and Coahuila. Training includes operational, survival, invasions and defenses. Also, the hierarchy is taught and maintained.

- A training facility in El Salvador was recently uncovered and with it over \$15 million (USD) in plastic containers has been uncovered with more expected to be located. In October 2011 it was reported that two former Colombian Army majors and two former non-commissioned officers are in Mexico training Los Zetas. It was reported that the four had been doing so since 2006.

### Weapons and Ammunition

This section captures the weapons and munitions used by an organized crime group. This information usually comes from reported seizures, arrests, or from videos/images from media or produced by organized crime groups themselves as propaganda. In addition to lists and descriptions of weapons and munitions, this section also captures details about how these items are procured and the origins of these weapons.

**Funding/Money Laundering** – This section captures the ways and means of organized crime to generate funds and for flowing funds through the organization. The following are excerpts of ISVG’s analysis of Los Zetas’ funding activities as of late 2011:

- Laundering of money takes place through a number of businesses including restaurants, car dealers and meat markets in the Northern Texas area. Laundering has been reported in Kansas, Minnesota, Atlanta and Chicago.
- A group of Los Zetas members were recently arrested, accused of dealing in stolen petroleum, the individuals were linked to bank accounts with over \$1.4(USD) million.
- Los Zetas charge "derecho de piso" or protection fees/dues to businesses. If the protection money isn't paid, the businesses are victimized, as are the owners. The dues vary from 2,000 to 50,000 pesos a month, varying with the business' success and size.

### Effectiveness

Organized crime thrives in fragile states/areas, usually where government functions have degraded or broken down completely. In many cases, criminal organizations engage in activities to perpetuate degraded government functions. This is above and beyond the violence and illicit activities that constitute the “business” of organized crime. These activities ensure the effectiveness of criminal organizations and generally fall into three categories: managing popular support, internal control mechanisms, and deterrence/intimidation.

Managing popular support can range from using public messages to “communicate” with the population to providing social and security services that effectively replaces the government functions in the areas of operation. Internal control mechanisms are protocols/procedures that criminal organizations implement to “harden” the organization to law enforcement and security organizations seeking to counter or disrupt them. Once a criminal organization controls territory and is effectively managing popular support, it needs to take steps to intimidate 3<sup>rd</sup> parties (usually the government, media, and/or other criminal organizations) from re-encroaching on this territory. These activities constitute a strategy of deterrence, usually through portraying superior force/strength and intimidation.

### Analytical Challenges

The transnational organized crime order of battle analysis provides a comprehensive framework for assessing and evaluating criminal organizations. It is not without its analytical challenges. Through the example of Los Zetas, this order of battle analysis was completed at the strategic level of the criminal

organization looking at the top-level leadership and hierarchy. This is an incomplete analysis though. In reality, Los Zetas is a transnational organization that operates across Mexico and abroad.

A complete order of battle analysis needs to be performed at the regional and sub-regional levels according to how each criminal organization constitutes its operations. In the case of Los Zetas, the cartel decentralizes operations to the State and Municipio/Plaza level. ISVG's complete order of battle analysis of Los Zetas was conducted and maintained at the national, state, and Plaza levels which provides a thorough and comprehensive assessment of the criminal organization.

Another shortcoming of transnational organized crime order of battle analysis is that it does not do a good job of tracking/visualizing the change or evolution of criminal organizations. Tracking and visualizing change usually requires the creation of repeated measures that describe aspects of a criminal organization that can be counted at regular intervals. These counts can then be quantitatively analyzed and visualized to evaluate the variances. Criminal organizations are clandestine by their very nature, but limits the types of information that can be reliably counted at regular intervals. So-called "count data" should be evaluated thoroughly for information validity, reliability, and appropriateness before incorporating repeated measures into an assessment and evaluation of criminal organizations.

## Chapter 6: The Contemporary Face of Transnational Criminal Organizations and the Threat They Pose to U.S. National Interest: A Global Perspective

Dr. Vesna Markovic  
[vmarkovic@isvg.org](mailto:vmarkovic@isvg.org)

Assistant Professor Henry C. Lee College of Criminal Justice and Forensic Sciences, University of New Haven, West Haven, CT and Program Manager, Institute for the Study of Violent Groups (ISVG)

### Introduction

Over the past several decades, transnational criminal organizations (TCOs) have represented an increasing threat to U.S. security and interests both domestically and internationally. TCOs are organizations that conduct and carry out criminal operations across international borders. This means that the planning or execution of a crime occurred in more than one country. TCOs include groups such as Mexican drug cartels including Los Zetas and the Sinaloa cartel, violent street gangs like MS-13, and other international criminal organizations such as the D-Company in Pakistan. Although the underground nature of these networks does not allow for completely accurate statistics, in 2009 the United Nations Office on Drugs and Crime (UNODC) estimated that profits from criminal proceeds exceeded \$2 trillion. These proceeds come from crimes such as drug trafficking, arms trafficking, human smuggling, human trafficking, counterfeit products, sea piracy, kidnap for ransom, and the illegal smuggling of commodities such as tobacco and oil, to name a few.

Traditional organized crime groups have consistently posed issues for law enforcement; however, the contemporary TCOs present an even greater security risk and threat. TCOs thrive in countries with a weak rule of law and present a great threat to regional security in many parts of the world. Bribery and corruption employed by these groups further serve to destabilize already weak governments. These TCOs also present a major threat to U.S. and world financial systems by exploiting legitimate commerce, and in some cases creating parallel markets ("Transnational Organized," 2011). Finally, one of the most significant threats posed by contemporary TCOs is their alliances and willingness to work with terrorist and extremist organizations. This paper will focus on contemporary TCOs by giving a brief overview of the most common criminal enterprises associated with these groups, the nexus between various TCOs, the nexus between TCOs and terrorist and extremist groups, case studies highlighting the nexus, and the threats they pose to U.S. national interests.

### Transnational Criminal Organization Activities

Drug trafficking has been and continues to be one of the most common criminal activities carried out by TCOs. It is also among the most profitable of the transnational crimes. A UN report (2012) estimates the worldwide illicit drug trade profits at \$322 billion a year. Every day, large quantities of drugs are shipped worldwide. This includes marijuana, which is the most widely used illegal narcotic, to cocaine, heroin, methamphetamines and their precursors, Ecstasy, and other synthetic drugs. TCO participation in the drug trade has increased levels of corruption, undermines the rule of law leading to greater levels of violence and instability in many regions, as well as the associated health and social issues it causes (Harrigan, 2011; Markovic, *i.p.*). Substance abuse of both licit and illicit drugs causes nearly 40,000

deaths in the U.S. each year and also leads to higher incidence of Hepatitis B, Hepatitis C, and HIV (CDC, 2011). Terrorist groups have also been known to use drug trafficking as a method of financing. The Taliban plays a role in Afghanistan's poppy/opium market, the FARC in the cocaine trade in Colombia, and more recently al-Qaeda in the Islamic Maghreb (AQIM) has been linked to raising fund through taxing and protecting cocaine shipments headed to Europe via Western Africa (Freeman, 2013).

The trafficking of small arms is another area of concern, since it fuels numerous conflicts around the globe. The trafficking of small arms, including rifles, pistols, and light machine guns, fosters violence and instability throughout the globe. Although the actual amount is not known, some estimates of the worldwide illicit trade in arms is somewhere between \$200-300 million, while some estimates believe it may run into the billions ("Small Arms," 2011). Arms and weapons that are trafficked may be stolen, obtained from licit sources but in violation of arms embargoes, arms for goods trades—such are trading drugs for weapons, trafficked from former high-conflict areas, and in rare cases manufactured by groups (Markovic, 2011). Small arms and light weapons are used worldwide in different theaters from civil conflicts to cartel wars. All forms of TCOs use small arms and light weapons in their operations, as do terrorist, extremist, insurgent, and rebel groups. Such weapons can help facilitate attacks such as the siege of the Amenas gas plant in Algeria by members of AQIM on January 16, 2013.

Another major criminal enterprise engaged in by TCOs is the smuggling and trafficking of human beings. The UN estimates global profits from forced labor to be over \$30 billion. This includes all forms of forced labor particularly sexual exploitation but does not include migrant smuggling. Human smuggling is the movement of people from one country to another by deliberately evading immigration laws. Human trafficking also contains a component of exploitation of those being moved, including forcing them to work in the sex industry, forced labor, domestic servitude, and other similar situations. Trafficking individuals for the purpose of forced labor is prevalent in the Middle East, Africa, South Asia, East Asia, and the Pacific while trafficking individuals for the purpose of sexual exploitation, which accounts for nearly sixty percent of all cases, is common in Europe, the Americas, and Central Asia ("Global Report," 2012). There are many estimates of the profits made from human trafficking and smuggling, as well as the number of people trafficked each year, however, they may underestimate the overall number due to the underground nature of the crimes. Various TCOs such as Mexican Coyotes, Russian mafia, snakeheads, and many groups in the Balkans all profit from trafficking humans (Markovic, 2011).

Product counterfeiting has also remained a major industry for transnational criminal groups. Virtually every product on the market can be replicated and sold on the black market at much lower than retail value (Markovic, 2007). As with many of the other criminal activities, the black market benefits from politically and economically unstable areas. Some countries do not have strong laws protecting against trademark and copyright infringement, therefore creating an opportunity for TCOs to capitalize. Another contributing factor is the demand for counterfeit products. Audio and video CDs and DVDs are some of the most popular items that are reproduced. TCOs also counterfeit software, electronics, and designer clothing and accessories such as purses, sunglasses, and watches. These products are easily reproduced, transported, and sold. Even currency, tax stamps, and other similar items may also be counterfeit. These products and currency can generate large profits for TCOs and terrorist groups as well. The trade in pirated music for example can be more profitable to a TCO than sale of cannabis. A kilogram of pirated CDs is worth almost \$4,000 per kilogram, while one kilogram of cannabis resin is only worth a little over \$1,300 (Interpol, 2004). The high demand for counterfeit product creates large

markets around the world. Another major incentive to TCOs is the fact that the penalties for drug trafficking are much harsher than for product counterfeiting.

Aside from the criminal activities mentioned above, TCOs are also involved in trafficking contraband items such as cigarettes, oil, precious metals and stones, timber, and other commodities. Sea piracy is another criminal activity that has grown over the past several years, although there was a major decrease in 2012. TCOs have been involved in various types of fraud as well. For example, criminal groups in Europe alone make nearly \$2 billion a year from credit card fraud (Europol, 2012). Regardless of which one of the criminal activities TCOs are involved in, they must conceal the origin of the illicit proceeds. This is done through both formal and informal money laundering, as well as, bulk cash smuggling. Bulk cash smuggling involves moving illegal proceeds, generally more than \$10,000 in cash, from one location to another by concealing it in some way. This is increasingly becoming a popular method used by TCOs, particularly those involved in the drug trade.

Formal money laundering operates through the regular banking system and attempts to conceal the source of proceeds that were obtained illegally. If the money is in cash, it is first put into the financial system; this step is known as "placement." The next step involves concealing the money by making multiple transactions to make it difficult to trace the origin of the money. This step is known as "layering." The more transactions made, the harder it is to trace the origin of the funds. Once the money is concealed through this method, it is ready to be used as legitimately earned money; this step is referred to as "integration" ("National Money," 2007). This means the clean money may then be used to purchase real estate, cars, businesses, or be invested in some other form. A major example of formal money laundering by TCOs involves the HSBC bank. In December 2012, HSBC was fined \$1.92 billion in a money laundering case tied to Mexican drug cartels (Hernandez, 2012).

Other forms of money laundering are the informal money laundering systems. *Hawala* is an informal money transfer system, which is based on trust. There are no formal receipts or statements of transaction, and no money ever crosses borders. Since no money is exchanged the debts between *hawaldars* can be settled through under invoicing, over invoicing, and debt assignment (Jost, 2001). Due to its favorable exchange rate, and low fees compared to bank transfers, it is a preferred method of transmitting money by immigrant communities particularly because no documentation is necessary to send money. Besides providing a cheap, fast, and reliable method of transferring money, the lack of a paper trail also makes this method favorable among criminal organizations. *Hawala* transfers can be an easy and effective method of transfer for terrorist groups, while making investigating these transfers difficult due to the lack of records. A prime example of the use of *hawala* by a terrorist group is the money transfer sent by Tehrik-i-Taliban (TTP) from Pakistan to Faizal Shahzad in April 2010, just one month before his failed Time Square bombing attempt ("Manhattan U.S.," 2010). TCOs also use *hawala*. Dawood Ibrahim is believed to be heavily involved in *hawala* money transmittal operations (Nanjappa, 2010).

There are also other variations of these informal money transfer systems worldwide. One popular method is the Black Market Peso Exchange (BMPE). It is used heavily in South America, especially in Colombia by businessmen who attempt to avoid remittance controls, and by TCOs who launder proceeds from drug trafficking operations. Just like formal money laundering, proceeds from illicit activities are moved via the BMPE and eventually end up back in the licit market, as if it were earned legitimately. Previously drug money was transferred back to Colombia on the same planes that brought

the drugs, and then exchanged for pesos at willing banks in Colombia, or the money was flown to off-shore banks in the Caribbean (Zill and Bergman, 2000). Law enforcement and government officials, based on information from various sources, estimate the total amount of money laundered through the BMPE at three to six billion dollars a year (White House, 2000; Zill and Bergman, 2000; Johnson, 1999).

If a TCO were smuggling proceeds of drug sales from the U.S. to Colombia using the BMPE, they would first contact a peso broker. The peso broker will arrange pick up of the money in the U.S. and then change the funds into money orders, purchase other financial instruments, or place the money directly into already established bank accounts. The broker then enters into contracts with businessmen in Colombia, who for a lower exchange rate, purchase goods from the U.S. These businessmen pay the broker in Colombia in pesos while the drug money in the U.S. is used to purchase the goods for the businessmen, which is then shipped to Colombia allowing for the drug proceeds to be laundered, and allowing the businessmen to make purchases at a lower exchange rate. The money can be exchanged at a rate that is discounted between 25 and 40 percent (Johnson, 1999; Zill and Bergman, 2000). As with the *hawala*, there are numerous variations of this scheme.

### Transnational Criminal Organization Networks

One of the most prominent threats posed by TCOs is their interest in the bottom line. This means that they are willing to work with any group regardless of their affiliations or ideologies. Many of these groups work together for the main purpose of making money. Of particular concern to U.S. interests is the collusion between Mexican drug trafficking organizations (DTOs) and various street gangs in the U.S. Mexican DTOs are making large amounts of money from drug trafficking and this fuels the ongoing violence in Mexico. Coupled with a high level of corruption, the problems in Mexico create a threat to U.S. cities around the country. Some have already witnessed an increase in cartel violence, such as in Atlanta and Chicago. There has been an increased presence in cartels in Chicago. The increase in murders in that city in 2012 has been directly attributed to fighting over drugs and territory. Battles for control over marijuana, cocaine, and heroin distribution by the Zetas and Sinaloa cartel and their violent street gang counterparts have been increasing (Keteyian, 2012).

Chicago is not the only city to witness the increase in violence due to these turf battles from the lucrative drug business. In 2008, approximately \$70 million in drug-related cash was seized in the Atlanta area alone because of its role as a distribution center for marijuana, cocaine, heroin, and methamphetamines for the eastern U.S. ("Mexican Cartels," 2009). These nationwide networks also include numerous street gangs. These street gangs assist in transportation, distribution, and sale of narcotics, and in some cases work as enforcers for the Mexican drug cartels. Figure 10 illustrates the relationships between some of the most active Mexican DTOs and street gangs. The figure only shows links with street gangs the DTOs have been aligned with, and not inter-linkages or rivalries between DTOs or gangs themselves. The chart shows just a handful of groups that have worked with or for Mexican DTOs. This poses a great threat to U.S. interests and the level of violence in cities around the U.S.

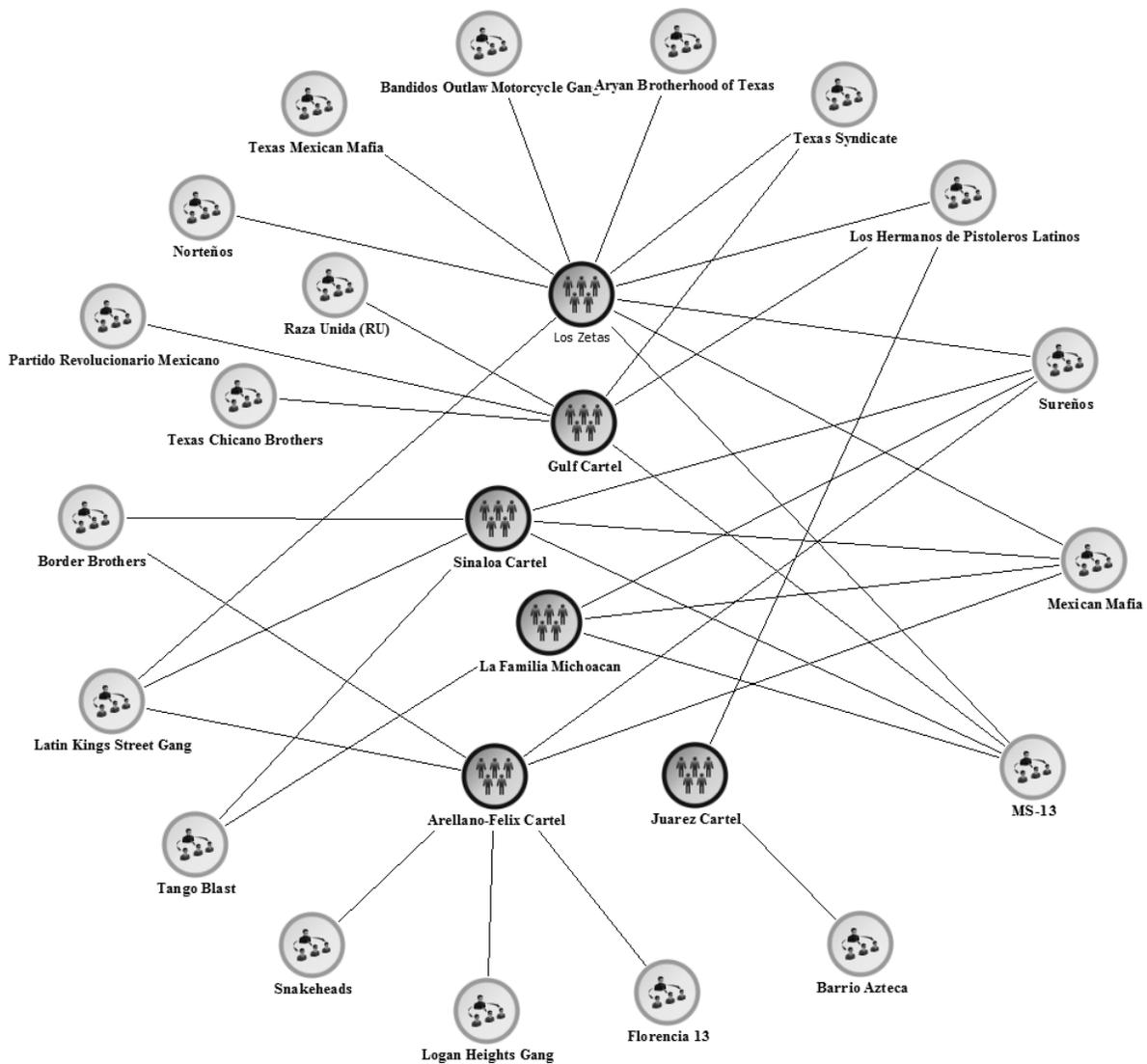


Figure 10: Major Mexican DTOs and Their Links with U.S. Street Gangs (ISVG)

### The Nexus between TCOs, Terrorists and Extremist Groups

Perhaps the most disturbing aspect of the contemporary TCOs is their willingness to work with terrorist and extremist organizations. Whereas traditional organized crime groups were viewed as having a nationalistic orientation, the contemporary TCOs often have competing interests with the State (Shelley, 2005). This presents a particularly troubling trend among the contemporary TCOs. Terrorist groups have also begun using tactics traditionally attributed to organized crime to finance their operations. These indicators include:

- Colluding with other terrorist groups to finance through organized crime;
- Working with TCOs in organized crime activities; and
- Overlapping networks between TCOs and terrorist groups (Markovic, 2011).

There have been many cases that illustrate the nexus between these groups. The following section contains three case studies that demonstrate the effectiveness and threats posed by such collusion.

## Case Study 1: Nexus between TCOs and Terrorist Groups

It is becoming more and more common for contemporary TCOs to collude with terrorist and extremist groups. In some cases the lines between terrorist/extremist groups and TCOs may be blurred. They may have overlapping networks and in rare cases the TCO is greatly involved in terrorist activities. A primary example of this is the D-Company, a TCO based out of Karachi, Pakistan run by Dawood Ibrahim. The group is engaged in many transnational criminal activities such as drug trafficking, human trafficking, extortion, gambling, Hawala, among criminal activities (Kaplan, 2005). The most troubling aspect is the group's continued collusion with terrorist organizations. For the past several decades, the D-Company has repeatedly engaged in relationships with terrorist and extremist groups worldwide.

In the 1990s, the D-Company smuggled heroin from Pakistan with the assistance of a Sri Lankan terrorist organization the Liberation Tigers of Tamil Eelam (LTTE) ("Dawood Inc.," 1997). These drugs were shipped overland through India to Colombo, Sri Lanka, where they were repackaged and shipped to Europe in ocean-liners, and to West Africa using cargo and container ships ("Dawood Inc.," 1997). This joint network also operated in trafficking arms to various areas. One intelligence report claimed that the LTTE used these networks in Karachi to transport an arms shipment to Northern Alliance Commander Ahmad Shah Masood in Afghanistan in 1995 ("Dawood Inc.," 1997). In an even more troubling example, some reports allege that Ibrahim granted permission to al-Qaeda to pay for use of D-Company's extensive smuggling networks (Raman, 2003).

D-Company has also been directly linked to terrorist activities, including providing logistical and material support to various terrorist groups in Pakistan. The 1993 Bombay (Mumbai) attacks, in which 13 bombs simultaneously exploded around the city causing over 250 deaths, were linked to Ibrahim (Kaplan, 2005). The 2008 Mumbai attacks carried out by Lashkar e Tayyiba (LeT), which led to the deaths of over 170 people, was also facilitated to some extent by Ibrahim. It is believed he provided the boat used and also provided material support to the group ("Dawood Directly," 2008). Moreover, Ibrahim has provided material and financial support to LeT and other groups such as the Students Islamic Movement in India (SIMI), Harkat ul Jihad-al-Islami (HUJI), and Tehrik Nifaj Shariat-e-Mohammadi (TNSM).

The willingness of TCOs to work with and provide logistical, financial and/or material support to terrorist or extremist groups makes these relationships very lethal, as exemplified by D-Company. The international reach of the group and its networks can potentially link a wide range of dangerous groups together. It can also help facilitate the movement of money and operatives to the many countries where D-Company maintains operations or network contacts. To illustrate the potential of this network, a social network chart of Ibrahim and D-Company was created using data from the Institute for the Study of Violent Groups (ISVG). Figure 11 shows direct and indirect links between Ibrahim and LeT, SIMI, Harkat-ul Jihad-al-Islami Bangladesh (HuJI-B), and al-Qaeda.

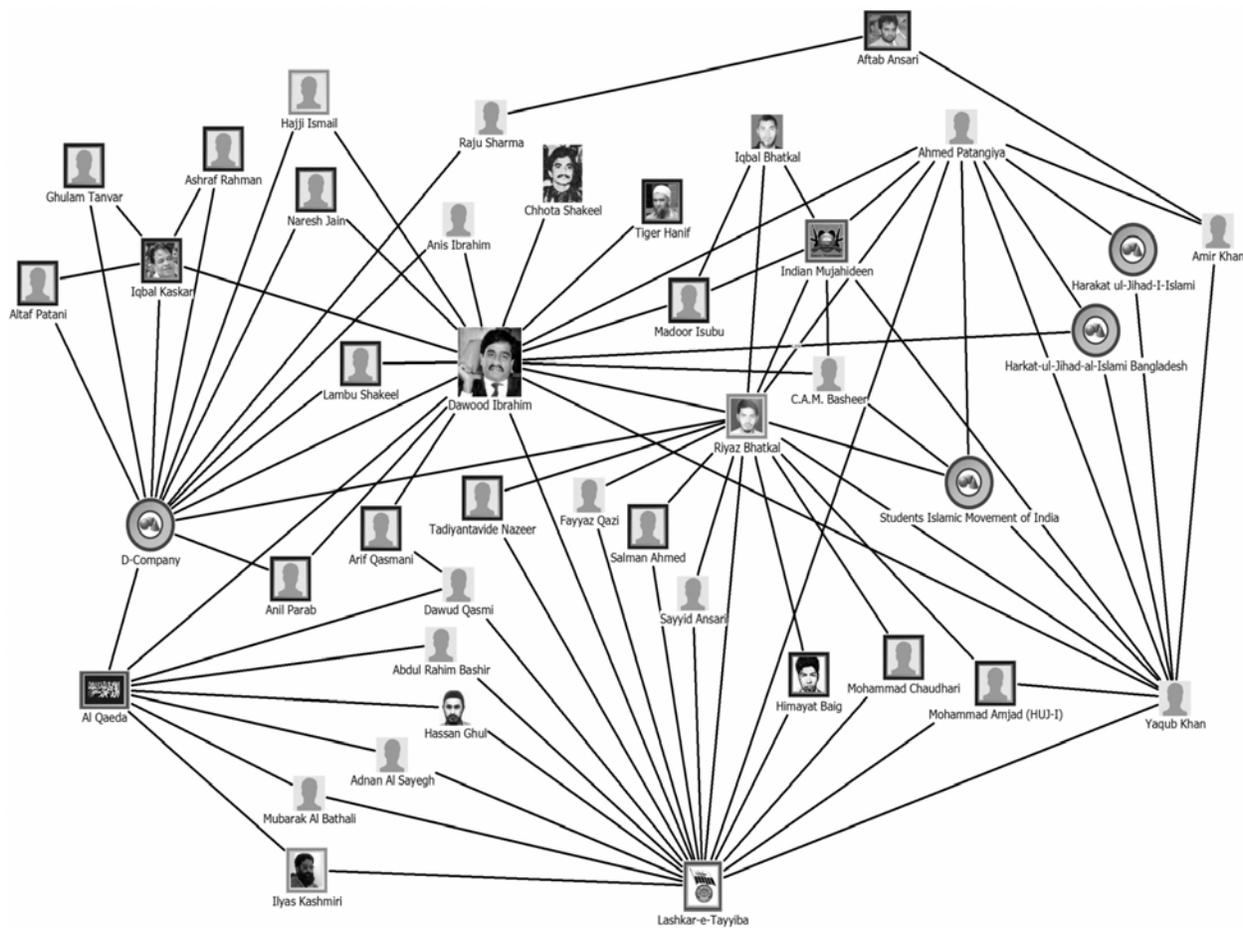


Figure 11: Social Network of Prominent Links of Dawood Ibrahim and D-Company (ISVG)

### Case Study 2: Nexus between Two Terrorist Groups

This second case study looks at the collusion between two terrorist groups. On December 15, 2009, Umar Issa, Harouna Toure, and Idriss Abelrahman were indicted on two counts for their role in a conspiracy to possess with the intent to distribute cocaine, and conspiracy to provide material support to a foreign terrorist organization (USA v. Issa, 2009). The men were linked to AQIM, formerly known as the Salafist Group for Call and Combat (GSPC), and were attempting to work with FARC to smuggle Colombian cocaine to Europe via West Africa. They were actually dealing with undercover agents, whom they believed to be members of the FARC. A confidential human source was introduced to Issa and began a series of meetings that would lead to the arrest of Issa and two accomplices.

The confidential human source (CHS) identified Issa as a member of a criminal organization that operated in Togo, Ghana, Burkina Faso, and Mali (USA v. Issa, 2009; Markovic, 2011). The indictment stated that the CHS met with Issa on September 14, 2009 in Ghana. This meeting was used to plan the logistics of transporting cocaine for the FARC via West Africa, to North Africa, with the final destination being the Canary Islands. During this meeting Issa stated that the shipment would have protection provided by AQIM and that they would be able to easily circumvent scrutiny at customs checkpoints in Mali. After this date, there were several phone calls made to arrange the logistics of transporting the cocaine, arranging transfers to Issa through Western Union in Togo. Further meetings took place in October in Ghana between the CHS and Issa at which point Issa introduced the informant to his boss

Harouna Toure. They would arrange for transshipment of the cocaine from Ghana to Mali, however they would enlist the support of AQIM from Mali to Morocco using Land Rover 4x4s. The cost negotiated to transfer the cocaine was \$2,000 per kilogram (Markovic, 2011). The arrangement was to transport between 500 and 1,000 kilograms of cocaine at a time.

During the meetings between the men and the CHS, Toure mentioned his connections to AQIM and other criminal activities he participated in to finance al-Qaeda operations, and supporting them by providing gasoline and food. This involved smuggling individuals from Bangladesh, Pakistan, and India into Spain. Other activities included collecting taxes from the wealthy in Mali, also allegedly carried out for AQIM. The kidnapping of Belgian citizens who were held for ransom was also for AQIM. Although the men were actually dealing with undercover agents, it showed the group members willingness to work with other terrorist groups to raise funds for their cause. In December 2009, the three men were arrested for their role in this smuggling plot.

### **Case Study 3: Terrorist Group Using TCO Tactics**

The final case study looks at one of the primary examples of terrorist groups employing methods traditionally associated with transnational organized crime groups. Although kidnap for ransom (KFR), and express kidnappings have been used by many criminal organizations - including those involved in sea piracy, KFR and kidnapping for political motives has also been widely used by many terrorist groups. Groups such as Abu Sayyaf (ASG) in the Philippines, Pakistani groups such as Tehrik-e-Taliban Pakistan (TTP), Lashkar-e-Jhangvi (LeJ), and Sipah-e-Sahaba (SSP), FARC, National Liberation Army (ELN) in Colombia, and al-Qaeda in Iraq (AQI) have also used kidnapping for ransom and political motives. One of the most prominent groups using KFR as a tactic is AQIM, formerly known as the Salafist Group for Preaching and Combat (GSPC), which originally primarily operated in Algeria. Since becoming an al-Qaeda branch, the group has increased its level of attacks, and spread its area of operation outside of Algeria. Kidnapping for ransom is one of the group's primary sources of funding. Since 2005, AQIM is believed to have earned \$65 million from kidnap for ransom ("Organised Maritime," 2011). AQIM has also used kidnapping to try and coerce concessions from foreign governments.

Although AQIM has used KFR for many years, the most recent incident involving the siege of the Amenas gas plant in Algeria has thrust them into the international spotlight. On January 16, 2013 approximately 30 militants using automatic weapons and grenades attacked the gas plant and rounded up hundreds of foreigners in a massive hostage taking. Some hostages managed to escape while others were shot while attempting to escape. According to Algerian officials, some hostages were strapped with Semtex bombs (Chrisafis, et. al., 2013). Mokhtar Belmokhtar, former Emir of AQIM, released a video claiming responsibility for the attack and called on France to stop airstrikes in Mali ("Qaeda Commander," 2013). Many foreign hostages were killed in the attack, including three U.S. citizens. The siege lasted for four days before intervention by Algerian security forces. As of January 21, it is believed 37 foreign hostages, and 29 militants were killed (Fleishman, 2013).

While the kidnapping at the Amenas gas plant was the most prominent incident involved foreign hostages, this is a very common tactic used by AQIM. On January 22, 2009, armed gunmen ambushed a group of Western tourists. While the first vehicle was able to escape, four Western tourists (German, Swiss and U.K. nationals) were kidnapped in Niger and taken to Mali ("Organised Maritime," 2011). It is believed that they were kidnapped by nomads and then sold to AQIM. One of those kidnapped was UK citizen Edwin Dyer. AQIM asked the government to release Abu Qatada, a Palestinian with Jordanian

citizenship, who at the time was incarcerated in London for his affiliations with al-Qaeda. The UK refused to release Abu Qatada. Their second offer was a €10 million ransom in return for his release ("Organised Maritime," 2011). Dyer was killed by AQIM on May 31, 2009 in Northern Mali. They then demanded €300,000 for the return of his remains, which was also not paid. The three remaining hostages were subsequently released. Although the specific terms of the release were not known, it is believed that some ransom was paid ("Organised Maritime," 2011).

### The Threat to U.S. Security and Interests

TCOs operate all over the world. Some countries are destination countries, while others are just used as transshipment points. Some of the major problem areas include Western Africa for the trafficking of cocaine to the European Union, the Balkan route, and of particular concern to the U.S., Mexico, Central America, and the Caribbean. What makes this problem more serious is the evolving nature of TCOs. The transnational nature of the criminal activity poses critical threats around the globe. These groups and their criminal activities perpetuate violence, serve to further destabilize areas with weak economies and institutions, lead to high levels of corruption, and pose a significant threat to U.S. interests both here and abroad. These groups that threaten U.S. interests have not only become more dangerous by increasing their capabilities of carrying out attacks but have also become more flexible because of their continuing ability to obtain support and raise funds, particularly through the use of traditional organized criminal activities. The recent attacks against foreigners at the Amenas gas plant in Algeria, provides a prominent example of the threat faced by the U.S.

Other major threats have arisen based on changes in TCO operational tactics. In order to avoid law enforcement and security forces, the groups have adapted and become creative in their methods of operation. One primary example is the increased use of self-propelled semi-submersibles, or mini submarines. These submersibles are used to traffic cocaine from South America to the U.S., and present a unique challenge in homeland security. They are generally built in FARC-controlled territories in Colombia, and can hold up to 10 metric tons of cocaine. They were made of wood, but have also been made using fiberglass and steel, and are equipped with sophisticated electronics to avoid detection ("All Hands," 2008). Although it is used specifically for trafficking cocaine, it can also be used to facilitate other transnational criminal activities and possibly terrorist acts. With a 10 metric ton cargo capacity used to ship narcotics, this space can also be used to carry explosives or even WMDs, and can possibly be used to facilitate water-borne attacks, which pose a direct threat to the national security of the U.S. ("All Hands," 2008).

The new TCOs are constantly expanding their operations and networks, and have diversified the criminal enterprises they are involved in ("Transnational Organized," 2011). Also playing a role in these expanding networks are individuals such as accountants, attorneys, bankers, and other facilitators who provide services to these TCOs ("Transnational Organized," 2011). These partnerships, along with the collaboration between TCOs and terrorist groups act as a force multiplier (Rollins & Wyler, 2012). The new TCOs are more apt and willing to provide weapons, logistics and other services to these groups. Also, as groups such as the Self Defense Forces of Colombia (AUC) turned to criminal activity after demobilization, or terrorist groups who use criminal activity as a source of funding, TCOs may also adopt political or ideological motivations and goals (Rollins & Wyler, 2012). The criminal organizations, such as Ibrahim's D-Company have already crossed the line from criminal activities to terrorism as previously

outlined. In order to disrupt these networks it is important to cooperate on an international level. It is important to strengthen the skills and capacity of weaker governments in battling TCOs.

# Chapter 7: The Threat of Pakistani Criminal Organizations: Assessing the Potential for Involvement in Radiological/Nuclear Smuggling, Collaboration with Terrorist Groups, and the Potential to Destabilize the Pakistani State

Dr. Amy Pate, Ms. Mila Johns, Mr. Gary Ackerman, and Ms. McKenzie O'Brien  
[apate@umd.edu](mailto:apate@umd.edu)

START/University of Maryland

## Introduction

This paper details a project designed to assess risks posed by criminal organizations operating in Pakistan. The START research team utilized openly available sources to identify criminal organizations active in Pakistan and to build qualitative profiles for 11 of the most significant criminal organizations. The Radiological/Nuclear Smuggling Threat Assessment Tool (RN-STAT), previously developed by START, was modified and extended to assess the threat individual criminal organizations posed in four arenas, including the following (Ackerman, 2011).

- The likelihood of engaging in RN smuggling in general
- The likelihood of engaging in RN smuggling for or with a terrorist organization
- The likelihood of forming a general cooperative nexus with a regional terrorist organization
- The likelihood of increasing the levels of instability within the Pakistani state

This modified threat assessment tool, renamed the Criminal Organization Threat Assessment Tool (COTAT), was applied to selected criminal organizations. A social network analysis was also undertaken for each of the profiled criminal organizations and their interactions with others in the Pakistani milieu.

The following paper first reviews the methodologies employed and then moves to a discussion of the findings of the threat assessment tool and the social network analysis. The conclusion highlights key findings and lessons learned, including potential insights for policy.

## Methodology

### Identification and Selection of Prominent Criminal Organizations in Pakistan

Researchers and student research assistants used open source search strategies to identify criminal organizations in Pakistan. In order to be considered for inclusion, the criminal organization had to be coherent enough in its leadership, membership, and/or behavior to be identifiable in open sources. Secondly, we limited our search to the time period 2009 to 2012. If the team could not identify criminal behavior by an organization during this time frame, we did not consider it for inclusion. Sources were identified through general Internet searches, academic databases, and news aggregators. Searches were undertaken primarily in English, with supplementary searches in Urdu. The team identified 68 criminal organizations through this open source searching and selected 11 to profile, based on the size and scale of their operations and/or influence in specific criminal markets. The groups selected were the Tehrik-e Taliban Pakistan (TTP), People's Aman Committee (PAC), Lashkar-e Jhangvi (LEJ), Lashkar-e Taiba (LET), the Haqqani Network, D Company, the Dons of Lahore, Harkat-ul-Jihad-al-Islamic (HuJI), the Imam Bheel Bizenjo Network, the Quetta Alliance, and the Islamic Movement of Uzbekistan (IMU).

## Profile Development

In order to produce a threat assessment, the research team undertook a comprehensive search of open source information available on the characteristics and behavior of the selected organizations. Data collection covered multiple sources, including those found through general Internet searches (e.g., Google), academic databases (e.g., EBSCO, JSTOR), and news aggregators (e.g., Lexis-Nexis).

The research team opted to develop qualitative profiles and then derive quantitative measures to provide maximum flexibility for further analysis. Additionally, the research team performed a social network analysis for each of the selected organizations. The profiles reflect a broad range of organizational and behavioral dimensions, based on a theoretically and empirically informed assessment of their potential contribution to risks for RN smuggling, engagement with violent extremists, and/or domestic instability. The profiles collected the following characteristics.

- History of the organization
- Markets Involved In
- Scope and Size
- Leader Characteristics
- Organizational Structure
- Identified Resources
- Networking and Social Capital – Prior/Existing Relationships
- Ideological / Ethnic / Familial Orientation (if any)
- Technical Sophistication
- Penchant for Innovation
- Antipathy towards the United States and/or a South Asian government
- Experience with Radiological and/or Nuclear Materials
- Potential for Causing Political Instability
- General Analytical Evaluations
- Other Notes

## Development of Tool

The research team was aware of only one tool in the open domain that was developed explicitly to assess the feasibility for criminal organizations to engage in specific behaviors. RN-STAT had been previously developed by START, including members of the current project team, but focused only on assessing the relative probability of TCOs becoming involved in radiological and/or nuclear smuggling. Thus, the team extended the existing tool to first, examine additional behaviors, and second, apply to criminal organizations that were not necessarily transnational.

The Criminal Organization Threat Assessment Tool (COTAT) was designed to address threat assessments of the four different behaviors, listed above, of criminal organizations (COs). The tool is grounded in a basic conception of threat, i.e., that any strategic CO behavior requires the presence of both **motivation capability**, and at times, of **opportunity**<sup>27</sup>, and thus assumes that these elements contribute to the overall magnitude of the threat posed by a particular CO.

---

<sup>27</sup> Traditionally, opportunity factors have often been subsumed within the capability factor by framing them under the group's capability to exploit such opportunities. However, because the factors that relate to the opportunity for acquiring and moving RN materials and destabilizing the state are specific to these types of materials, we have chosen to draw attention to them by emphasizing them as a separate part of the analysis.

Based on the existing RN-STAT and members' expertise, the research team then began to identify individual motivational, capability, or opportunity metrics that could be expected to influence the likelihood (either positively or negatively) that a CO might engage in each of the threat behaviors listed above. A total of 61 distinct metrics<sup>28</sup> were collected and categorized into one of the threat elements described above, with each metric assigned possible values for scoring.<sup>29</sup>

The team then developed several options for combining the metrics into a threat assessment score. In theory, as we are seeking to determine the relative threat posed by each organization, there should be no difficulties in simply adding up the corresponding threat scores and comparing them across COs, so long as each CO was evaluated according to the same metrics. There are, however, a number of conceptual issues, which complicate this basic form of aggregation, which led the team to develop three different methods of weighting the threat metrics. Additionally, the team developed two methods for dealing with uncertainty in the data collection process.

Overall, applying the three different weightings and two methods of treating unknown values yields nine different threat scores for each assessment. While none of these scores can be unequivocally said to be more accurate in general, they provide a useful range of values that can be compared across assessments for each CO and incorporated into the rankings, as described below.<sup>30</sup>

### Tool Implementation

The current version of COTAT was implemented in Microsoft Excel as a spreadsheet containing the metrics and drop-down menus for the critical values. Each of the 11 criminal organizations selected for profiling (as described above) was assigned to three START analysts: one of the primary investigators (PI), a Special Projects Division researcher, and a faculty research assistant. A separate version of the spreadsheet tool was created for each CO and each of the four threat assessments was conducted using the information contained in the CO Profile.

For the purposes of quality control, the assessments produced by each of the three analysts were compared. At a group discussion led by the other PI, the research team considered each metric where there was a discrepancy between coded values across analysts, dealing with each CO in turn. A consensus decision was formed for each of these cases and a "resolved" set of four threat assessments was produced for each CO.

For each of the four threat assessments, the following procedure was employed.

- The nine total threat scores obtained from the "resolved" assessments of each CO were collated into a combined spreadsheet listing all the COs involved.
- For each of the nine threat scores, the CO's were then ranked from highest to lowest score.
- At the same time a "gross average ranking" was obtained, by averaging rankings across all three weightings and both methods for dealing with uncertainty.
- Owing to the inexact nature of threat assessments of this type, the final analysis did not make direct use of any single threat score. Rather, the project team examined the threat scores and determined a final ranking, which took into account all nine conceptualizations of the threat score, as well as the gross average ranking.
- For the final rankings, there are several cases where COs are grouped together in a single ranking "level." This was done in cases where rankings oscillated widely across the different threat scores or where certain COs received threat scores that were very close to one another.

---

<sup>28</sup> This included 19 new metrics not used in RN-STAT.

<sup>29</sup> A breakdown of metrics and how each was measured is available upon request.

<sup>30</sup> A full description of the tool development process is available upon request.

- At the same time, a project analyst independently proposed an intuitive ranking, based on a qualitative reading of each assessment. As a further quality control measure, the earlier tool-derived rankings were compared with these impressionistic rankings to act as a “smell test” regarding the face validity of the quantitative findings. None of the tool-derived rankings was rejected based on this exercise.

## Social Network Analysis

The research team also performed a social network analysis for each of the profiled organizations. Links were identified through searching open sources, simultaneous with identification of sources for populating each organizational profile. For each link, the criminal organization (and specific individual or individuals, if identified) was listed, along with the entity to which it had a relationship (and specific individuals or individuals, if identified). The research team also noted the nature of the link, whether the relationship was cooperative or conflictual, the start date of the link (if known), the termination date (if known), the relative strength of the tie (strong, moderate, weak), and the directionality of the relationship. Social network analysis was performed using *Analyst’s Notebook 8*. Four specific measures of centrality were employed, including:

- Degree centrality: measures the number of direct links of a node or entity;
- Betweenness centrality: measures the degree to which the node or entity acts as a “gatekeeper” within the network;
- Closeness centrality: measures the degree to which an entity is near all other nodes in the network; and
- Eigenvector centrality: measures the importance of a node in a network.

## Results

### Threat Assessment

The final rankings for each of the four threat assessments are listed below, along with a discussion of the tool results.

The 11 selected criminal organizations were ranked for risks of radiological/nuclear smuggling, as follows.

1. HuJI
2. LeT
2. TTP
4. Haqqani Network
5. LeJ
6. D-Company
7. IMU
8. Quetta Alliance
9. Imam Bheel Bizenjo Network
10. PAC
11. Dons of Lahore

The final ranking identifies HuJI as the most likely of the COs to engage in RN smuggling with LeT and the TTP next most likely, although there is no evident hierarchy between them. It is interesting that the top five criminal organizations are actually hybrid criminal/militant groupings, thus confirming the widely-

held conception that militant organizations like terrorist groups are the most likely to seek to become involved with RN weapons or materials. The only non-militant CO that is ranked higher than a militant group is D-Company, which has already shown itself willing to engage in mass-casualty attacks. None of the remaining pure COs received a threat score of 0.5 or greater in the majority of threat conceptualizations.

The rankings for risk of involvement in radiological/nuclear smuggling on behalf of or in conjunction with a militant or terrorist organization are listed below.

1. LeT
1. HuJI
3. TTP
4. Haqqani Network
4. D-Company
6. LeJ
7. IMU
8. Quetta Alliance
9. Imam Bheel Bizenjo Network
9. PAC
11. Dons of Lahore

The ranking for the particular manifestation of RN smuggling where the CO is involved with a terrorist/militant organization is very similar to the basic RN smuggling assessment. In this case, the predominance of militant/criminal hybrids at the top of the list is even more unsurprising, since these types of groups inherently meet the criterion of terrorist group involvement. However, two major changes from the previous list should be noted. First, LeT and HuJI now share the top spot in the list and, second, D-Company has climbed to a higher rung, on a par with the Haqqani network and above LeJ. One of the main reasons for this is D-Company's larger opportunities for encountering RN materials and its greater scope of motivation to do so, which in a sense trumps the fact that LeJ itself is a militant group.

Hybrid organizations (those with both militant/terrorist and criminal characteristics) were dropped from the threat assessment of criminal organizations forming a cooperative nexus with militant/terrorist groups. The ranking of the criminal organizations is listed below.

1. D-Company
2. Imam Bheel Bizenjo Network
2. PAC
2. Quetta Alliance
5. Dons of Lahore

For the pure COs included in the assessment, D-Company was far and away judged to be the most likely to cooperate with terrorists, with the Dons of Lahore relatively unlikely, and the Imam Bheel Group, the PAC and the Quetta Alliance showing similar threat scores. It should be noted that when hybrid organizations were included in the threat assessment, they occupied the top six positions in the ranking.

The rankings for threats posed in destabilizing Pakistan are listed below.

1. TTP
2. Haqqani Network
3. D-Company
3. IMU
5. HuJI
5. Quetta Alliance
7. PAC
8. LeT
9. LeJ
10. Imam Bheel Bizenjo Network
10. Dons of Lahore

The TTP and the Haqqani network are most likely to significantly increase the levels of instability or fragility in Pakistan. These two organizations share a high motivation to destabilize the Pakistani state, coupled with the capability to do so. Furthermore, they frequently work cooperatively in operations that challenge significantly Pakistani state control in large swathes of territory. More interesting is the appearance of D-Company, a pure CO, at the third spot—while it does not have a very high motivation to destabilize the state, its capabilities to do so ensure its prominence. Conversely, LeT and LeJ feature further down the table due to lower capability, despite some desire to destabilize the state (although not as high as most of the other militant groups). The threat of these two groups is also lowered by their past dependence on Pakistani state structures, including the ISI.

A link chart of the 11 selected COs was created and analyzed to assist in determining the existence and significance of linkages between important actors in the region. The link chart visually reveals the complex relationships of these entities, highlighting the degree to which the profiled criminal organizations are often connected to one another, to various states and state institutions, and to terrorist or insurgent groups in the region. Four measures of centrality (degree, betweenness, closeness, and Eigenvector) were employed to identify key nodes in the social networks of the 11 profiled criminal organizations.

Degree centrality is the number of direct links of a node or entity. This type of measurement ranks all entities on the link chart in the order that identifies “the most active in the network based on the number of direct links to other entities. For inbound activity, the top organizations (based on current links) are listed below.

1. Islamic Movement of Uzbekistan
2. LeT
3. Haqqani Network
4. TTP
5. HuJI

For outbound activity, the top five organizations are listed below.

1. IMU
2. LeT
3. Haqqani Network
4. TTP
5. HuJI

The entities, most notably the IMU, LeT, the Haqqani Network, and the TTP, are identical for both most inbound and outbound activity in the network. These results suggest that these entities, not surprisingly, receive and direct the most activity, requests, or information from and to other entities in the network as a whole. If a target activity is deemed likely to be executed and/or assisted by the most active or directly linked actors in the region, then it is these entities that must garner the most attention.

Betweenness centrality is a measure that ranks all entities on the link chart in the order that they might act as “gatekeeper entities” in controlling the information flow between different parts of a network. In other words, these entities guide a significant amount of information and play powerful communication roles as nodes between significant network clusters. The five highest scoring entities are listed below.

1. IMU
2. Afghan Taliban
3. LeT
4. PAC
5. Haqqani Network

These entities represent the main intersections for information passing through the whole network. As a result of this information advantage, these entities possess considerable knowledge of how to carry out trafficking and/or insurgent activities.

Closeness centrality refers to the degree to which an entity is near all other nodes in the network. This type of centrality measures an entity’s “access to other parts of the network and the visibility of activities within the network.” (i2, 2010) Because these entities are close to everything else, they are in an excellent position to monitor information and events happening in the network as a whole. The SNA measured both direct and indirect closeness: “Direct closeness is when two entities are connected by a link. Indirect closeness exists when information can only pass from one entity to another via a path that runs through one or more entities.” (i2, 2010) The top five entities with outbound paths are listed below.<sup>31</sup>

1. Friends of Lyari International
2. Habib Jan Baloch
3. Abu Sukhayib Al-Ansari
4. Hossein Mosleh (Iran)
5. Ahmad Sharifi (Iran)

The results suggest that these entities might direct key information or activity to other parts of the network. Additionally, these entities would be particularly well placed to deliver disinformation or otherwise obstruct criminal activity.

Eigenvector centrality is a measure of a node’s importance in a network. This type of measurement ranks all entities on the link chart in terms of their “influence in the network due to their direct links to highly active or well connected entities.” (i2, 2010) The SNA again measures both inbound and outbound links, determining an entity’s role as an authority and hub, respectively. The top “authority” entities are listed below.

1. IMU
2. LeT
3. TTP
4. LeJ

---

<sup>31</sup> Inbound paths were also measured and are available upon request.

## 5. HuJI

The top “hub” entities are listed below.

1. LeT
2. Haqqani Network
3. TTP
4. IMU
5. Afghan Taliban

These results suggest that these entities, most notably LeT, TTP, HuJI, and the Haqqani Network, are the most connected to other significant or well-connected entities in the network, and as such, act as authorities to other entities or as hubs between them for information or resources. For the purposes of this study, these well-connected entities have a great deal of influence on the network as a whole, and therefore, could be entities that would be influential in criminal activity, as well as in abetting or hindering it.

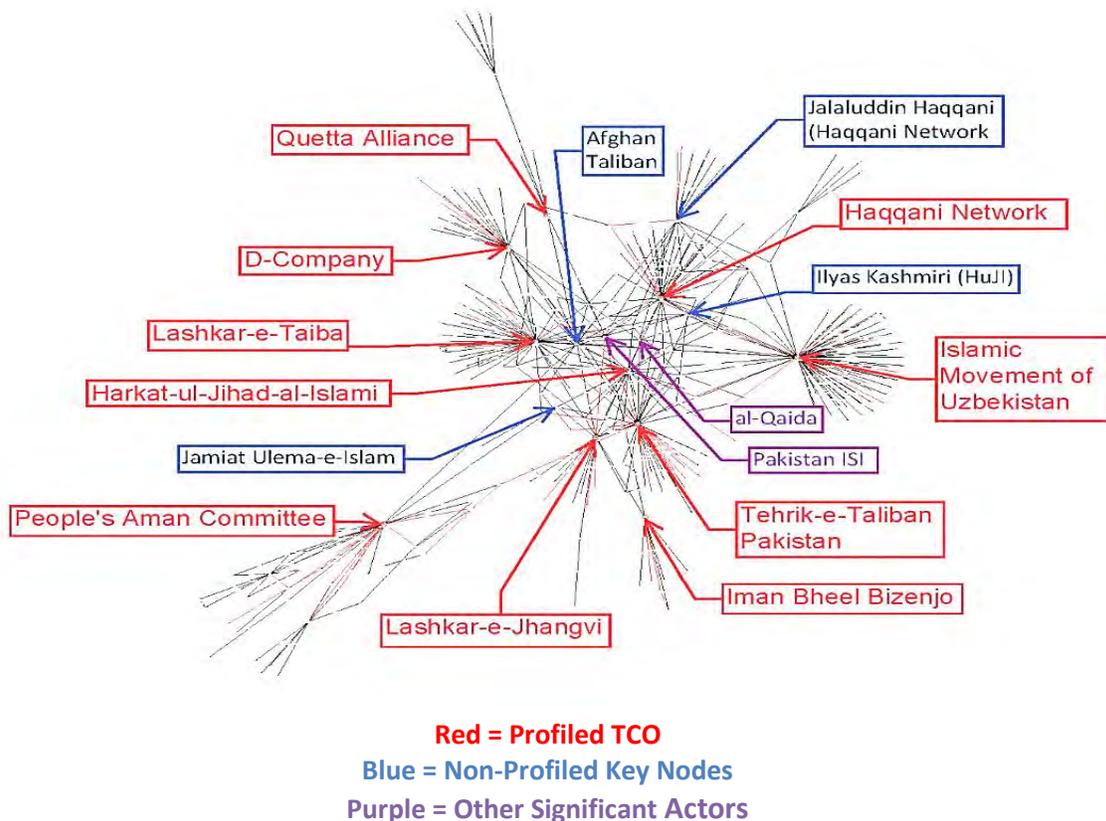


Figure 12: Snapshot of Current CO links

### Conclusion

Several conclusions may be drawn from the combined findings of the various threat assessments and the social network analysis. The overarching lesson derived from the various analyses is that hybrid organizations are more of a threat across threat domains (RN smuggling, RN smuggling with extremist organization involvement, nexus formation, and instability threat) than are the more purely criminal organizations. HuJI, LeT, the Haqqani Network, TTP, and LeJ are consistently in the top five for the various threat assessments. Furthermore, hybrid organizations are more central in identified social

networks, with the IMU, the Haqqani Network, LeJ, LeT, and TTP identified as the key nodes across methods. The only primarily criminal organization that emerges as significant in the threat assessments or in the social network analysis is D-Company, a criminal organization which has developed distinct ideological leanings and has at times engaged in politically motivated attacks.

Hybrid organizations (those that include both political extremist and criminal elements) have much higher motivations, in general, for engaging in RN smuggling (a high-risk activity with uncertain profit margins) and for creating an atmosphere of political instability. In particular, those hybrid organizations that have as part of their end-goals the transformation of the current Pakistani state into a Deobandi Islamist entity are highly motivated to generate and amplify political instability. In contrast, while criminal organizations may benefit from moderate levels of political instability, they are not motivated to foment instability directly. In general, the success and density of criminal organizations in Pakistan is as much a result as a cause of instability.

Four organizations emerge as clear threats for radiological and/or nuclear smuggling: HuJI, LeT, TTP, and the Haqqani Network. While the RN ambitions of HuJI and LeT are likely directed towards states other than Pakistan (India in particular), TTP and the Haqqani Network's ambitions are more likely directed at Pakistan's civilian government, in addition to Afghanistan's government. However, should Pakistan pursue a peaceful solution to the issue of Jammu and Kashmir with India's government (which would necessitate a more aggressive policy towards its former protégés in HuJI and LeT), the ambitions of HuJI and LeT could easily be redirected towards Pakistan.

Two of the organizations that are prominent risks for RN smuggling also top the threat assessment for political instability. TTP and the Haqqani Network, which frequently work in concert, are the two hybrid organizations that pose the highest level of threat to Pakistan's stability. This threat has been borne out in recent years, with both organizations stripping control of considerable swathes of territory from the Pakistani government.

Findings from the social network analysis largely reinforce the findings from the threat assessments, including the following.

- There is a relatively high degree of connectedness directly between the profiled criminal organizations.
- Several of the main entities are closely connected to various states and state institutions.
- There are close links between terrorist and criminal groups in Pakistan. Several of the profiled TCOs also function as terrorist organizations. Yet even the profiled organizations not themselves labeled as terrorist organizations generally have strong direct and/or indirect connections to terrorist or insurgent groups.
- As expected, the profiled COs appear to have a central role within the larger criminal network in Pakistan, especially the IMU, the Haqqani Network, LeT, LeJ, and TTP.
- While not always scoring high in the categories of centrality, the following entities have been identified as significant nodes in addition to the profiled COs: the Afghan Taliban, Jamiat Ulema-e-Islam (JUI), Jalaluddin Haqqani, and Ilyas Kashmiri.

The aggregated findings of the threat assessments and the social network analysis identify TTP and the Haqqani Network as the most critical organizations for which intervention strategies should be identified, evaluated and implemented. Additionally, strategies that address hybrid organizations in general are needed. Finally, D-Company emerges as the singular criminal organization that warrants specific attention. Its network, established not only in South Asia but also in the Middle East, presents particular difficulties that some of the more localized hybrid organizations (such as TTP) do not share.

## Chapter 8: Networking and Legitimization of Transnational Crime Organizations

Mary D Zalesny, PhD<sup>32</sup>

[mary.d.zalesny.civ@mail.mil](mailto:mary.d.zalesny.civ@mail.mil); [mary.zalesny@pnnl.gov](mailto:mary.zalesny@pnnl.gov)

Chief of Staff of the Army Strategic Studies Group  
Pacific Northwest National Laboratory

### Introduction

Enduring stereotypes of organized crime (e.g., Mafia gangsters in the early-mid 20<sup>th</sup> century) belie the scale of transnational organized crime (TOC) today and its cost to the global economy and human community (United Nations, 2004). Globalization, improved communication, and transportation technologies have benefitted both legal and illegal enterprises helping TOC become a potent financial and cultural force that undermines vulnerable state institutions and rule of law, and adversely affects millions of people. Accurate and consistent figures on the impact of transnational criminal organizations (TCO) are difficult to calculate and estimates vary across individual countries (Canadian Security Intelligence Service, 1999; Manwaring, 2007).<sup>33</sup> At least one estimate pegs the financial cost of TOC at \$870 billion annually (United Nations Office on Drugs and Crime, 2012). The profits from drug trafficking alone can surpass the gross national product of some nations. First and foremost, however, TOC is big business whose purpose is to make money. However, while criminal organizations make most of their money illegally without the constraints of laws and regulations, they also participate in legitimate businesses (White House, 2011). Both approaches give TCOs a competitive edge over legitimate businesses that operate within the confines of law.

The success of TCOs depends on their ability to provide desired goods and services to their customers, effective leadership, strong business-related networks and organizational processes that create advantages for thriving in a highly competitive global marketplace. Like any group, criminal organizations are created to accomplish tasks and objectives individuals could not achieve on their own. The complexity and magnitude of the task determines how large a group is required, what capabilities are needed, and the extent to which individual actions must be coordinated. Optimally, criminal groups should organize for efficiency and effectiveness alone. In reality, they may sacrifice some operational efficiency and effectiveness to avoid interference from authorities. Operational security is a fixed cost of doing business illegally and is achieved through stealth, co-opting or bribing officials, using well-placed insiders, and building networks that can be tapped for support throughout the group's operations. Operational security is also enhanced through investment in legitimate businesses that provide cover, legitimacy, and a vehicle for laundering profits from illegal activities.

This white paper is about networks created by TCOs to operate in and move across primarily geographical borders.<sup>34</sup> It summarizes the results of a recently conducted study that investigated criminal group involvement with local populations along U.S. borders and the network dynamics in two

---

<sup>32</sup> The author gratefully acknowledges the comments of Colonel Julian Tolbert, USAF, and Colonel William Zana, National Guard Bureau on an earlier draft.

<sup>33</sup> Estimates range from two percent (Canada) to 40 percent (Russia) of gross national product [GNP] and 14 percent of gross domestic product (Latin America).

<sup>34</sup> While this paper acknowledges the importance of the Internet as a highly attractive and still unregulated operating environment for TCO groups to reach across national borders, an in-depth discussion of TCO use of the internet is beyond the scope of this paper.

U.S. border areas.<sup>35</sup> The study focused on how known TCOs interact with two American Indian tribes whose lands straddle the U.S. border. Many of the geographical areas utilized by TCOs exist outside the effective control of authorities and allow the groups to operate with relative ease in staging illicit operations, meeting other illicit actors, and operating logistical hubs. American Indian reservations are controlled by sovereign nations and are home to local and accessible populations that provide potential recruits, specialized skills, and cover to hide from authorities. These facts have not gone unnoticed by TCOs, as evidenced by the following.

- Some TCOs reduce the risk of detection by transporting commodities and people across U.S. land and water borders that lie within tribal territory (DiFeo, 2009).
- There is a significant overlap between the locations of the most populous American Indian tribes in the U.S. and the locations of known Sinaloa drug cartel operations (Lamar, 2009).
- Other drug trafficking organizations are known to distribute drugs and other commodities using routes between American Indian reservations to major urban distribution hubs (Abreau et al, 2009).<sup>36</sup>

Factors critical to understanding TCOs, their networks and activities, and the local populations on US borders may not generalize to TCOs that operate elsewhere or to other local populations. However, an important element of research on TCOs is to determine which factors do generalize and under what circumstances. The research discussed here identified similarities between TCO and terrorist group structure and networks, and the similarities and differences between American Indian and Pashtun tribal philosophies that guide their members' behavior (Zalesny and Numrich, 2011). Primary research methods were expert solicitations and literature searches.

The study focused primarily on the southwest and northeast U.S. and the American Indian tribes whose lands straddle the U.S.-Mexico and U.S.-Canada borders. Information on tribes within 200 miles of the U.S. borders (land and water) with Canada and Mexico was also gathered. Importantly, a comparison of the characteristics that define the populations, practices, networks, and locations of interactions of TCOs that operate at U.S. borders with characteristics of terrorist and criminal groups that operate outside the U.S. was conducted. Rather than searching what distinguishes one TCO from another, the study looked for commonalities in organizing and operating strategies and practices among TCOs and with terrorist organizations.

Table 4 summarizes characteristics that appear to be common to both groups (United Nations, 2004; Gosselin, 2009; US Department of Justice, 2004.)

---

<sup>35</sup>The study was sponsored by Mr. Ben Riley, Principle Deputy, Rapid Fielding Directorate, Office of the Secretary of Defense.

<sup>36</sup> For example, the Yakama Indian reservation is a major distribution hub for drugs, including locally grown crops (often grown alongside legitimate crops that are a significant part of the region's economy).

Table 4: Similarities Between TCOs and Terrorist Groups

<b><i>Characteristics Common to Transnational Crime Organizations and Terrorist Groups</i></b>
Highly centralized structure and organization, but with greater use of more cellular structures and self-emerging cells
Strong organizational culture and strict norms, the violation of which could have serious or fatal consequences
Evidence of regional differences within the same organization
Multi-generational and lifetime membership
Observable adaptation to changing market factors (e.g., supply, demand, regulatory challenges, competition)
Increased outsourcing for specific capabilities
Increased use of cyber, but continuing reliance on low technologies to avoid detection
Creation of syndicates and alliances to further goals
Use of local populations to facilitate operations
Use of tribal lands to avoid detection and seizure of assets and to help with border transit

### Networks and Alliances

Criminal organizations have historically relied on networks to facilitate their illicit activities and have crossed tribal or state borders without regard to laws or restrictions. The networks they develop and rely on arise through various means and are often part of or extensions of broader, existing family, tribal or community relationships. Migrations and diaspora of tribal, kinship or ethnic groups have been cited as one of the key factors facilitating the spread of criminal groups beyond their home lands (DiFeo, 2009; Gosselin, 2009; Margolis, 2009). Like some political and business families, criminal groups develop relationships and marry strategically to gain entry into advantageous groups, networks, and locations they might otherwise not have access to (Thomas, 2009; Reina, 2009). Friendship and marital connections can facilitate acceptance of an outsider to a group, provide legitimacy and cover, and provide information important to criminal operations and security.

Networks are also increasingly used by TCOs over more traditional hierarchical structures as important organizing and operating platforms (United Nations, 2004). However, networks are not egalitarian. Status, trust, skills and operational security influence an individual's connectedness to other network members, especially TCO leadership (Manwaring, 2007). Interconnections among criminal networks that lead to the formation of syndicates and alliances can help supply needed or desired resources, skills, and further connections.

The use of existing, local networks by criminal groups for skills they need is logical. At a minimum, it is simply easier to engage a proximate group that criminal group members know and share characteristics or circumstances. Members of TCOs that operate outside of the group's home territory may assimilate into local, ethnic communities. Over time, they may come to rely on the communities for protection, recruits, and markets (OCTA, 2008). TCOs that develop from local gangs may already control neighborhoods in which members have been raised and can draw from the local population for recruits and other resources. A recent review of gangs in Central America (Manwaring, 2007) described some TCOs as the third generation of the "gang phenomenon" and a natural progression from first- and second-generation gangs when leadership and other circumstances are favorable. According to Manwaring, first-generation gangs are what most people think of as street gangs that develop and operate primarily in their own neighborhoods or turfs. Their crimes are usually opportunistic for personal gain and creating protection rackets. Most gangs remain at this level. As criminal activity takes on a greater business focus, gangs may progress to the second-generation. Under the right kind of entrepreneurial leadership, as criminal activities and their territory expands, their operations become

more sophisticated and they may enter into alliances with TCOs as service providers (e.g., enforcement, commodity transit). Second-generation gangs may also operate in several regions and across national borders. By the time some gangs reach the third-generation, they are indistinguishable from other TCOs. At each generation, gangs face a common challenge of controlling territory, people, and markets to allow unrestricted ability to achieve their objectives. Networks, alliances, bribery, intimidation, and violence are applied as tools of influence and control.

Because they are business organizations, TCOs often emulate successful, legitimate commercial organizations in their management and operational practices (Manwaring, 2007). For example, TCOs:

- Create or follow a business model to maximize profit;
- Develop and maintain clear business and accounting processes
- Conduct market research and cultivate markets;
- Attempt to control markets;
- Maintain internal discipline; and
- Support a learning culture (evidence of learning by doing) and organizational growth in personnel and capabilities (Miller, 2009; Margolis, 2009; Williams, 2009; Former VP Hells Angels, 2009).

Just as large commercial enterprises leverage their networks and influence to secure favorable locations for their operations (e.g., low taxes, adequate transportation infrastructure, access to customers, and markets), TCOs develop and leverage their networks. This includes ethnic, religious, linguistic, cultural, business, marital or ideological ties to local populations in order to find or develop favorable locations (or safe havens) from which to operate.

### Geography and Tribal Characteristics Matter

Differences in the geography of the southwest versus northeast U.S. border areas and differences in tribal characteristics affect how TCO groups operate and engage the local populations in each area. Both U.S. border areas contain well-used transportation and smuggling routes. However, the ability of outsiders to traverse the routes without assistance varies. On the U.S.-Mexico border, the line between countries is unmistakable, the soil is soft and the vegetation minimal making border violations (or evidence of violations) relatively easy to observe. The safest routes have been traversed for centuries and are well known. While the southwest border area presents its own challenges (e.g., heat, little water, flash floods, distances to population centers), it is relatively easy to navigate without assistance to reach the U.S. interior.

The Great Lakes and St. Lawrence River form a water boundary on the northeast U.S.-Canada border, making border violations more difficult to detect. Additionally, the rugged and forested land terrain is challenging to navigate beyond the patrolled and controlled border crossing areas. An alternative to the land border checkpoints is the St. Lawrence Seaway and the water routes used for decades by the St. Regis/Akwesasne Indians to smuggle commodities and people. The Akwesasne use boats when the water is flowing and snowmobiles and all-terrain vehicles when the waterway is frozen. The first land border off the St. Lawrence River is inside the Akwesasne Territory (Thomas et al, 2009). TCOs operating on the northeast U.S. border are more dependent on tribal members who know the water routes and the habits of both tribal police and Customs and Border Patrol agents than are TCOs operating on the southwest U.S. border (Lamar, 2009).

Tribal characteristics also influence how TCOs attempt to establish relationships with tribal members and develop networks to facilitate TCO operations. The Akwesasne's history of smuggling commodities, their skills in navigating the challenging terrain and water boundaries, and their aggressiveness in keeping the United States Government (USG) off the reservation make them an ideal local population

for TCOs to develop alliances with. However, the Akwesasne are also generally distrustful of all outsiders. Consequently, TCO members frequently make initial contact and develop friendships with tribal members in bars or gyms rather than on the reservation. Younger Akwesasne are recruited by older tribal members with TCO connections (rather than directly by TCOs) to work as mules. Part of the recruiting strategy assures the younger tribal members that any criminal charges they might incur as minors will be sealed and will not affect them once they turn 18 years of age. For these young tribal members, easy money without the usual risk is attractive.

Mules traffic commodities onto the reservation, then other tribal members move them to the interior on either side of the U.S.-Canada border (Thomas et al, 2009). This arrangement means that TCOs effectively lose control of their commodities from the time they enter the reservation until they reach their final destination in the U.S. or Canada, which may be considerable distances in some cases. A high degree of trust, strict accounting processes, and a clear understanding of consequences of not delivering a shipment are crucial to making this arrangement work. Among the TCOs that operate on the northeast U.S. border, each 'nationality' (e.g., Russian, Armenian, Salvadoran, etc.) may find a group of tribal members to work with on a continuing basis (DiFeo, 2009; Thomas, et al, 2009). The relationships and networks that develop can include generations within families.

On the southwest U.S. border, TCOs do not depend on local tribes to facilitate their operations, but utilize the knowledge and skills of tribal members for various activities including operational security.<sup>37</sup> Of American Indian tribes, the Tohono O'odham is considered especially hospitable. Historically, tribal members have helped anyone who needed or asked for help while traveling across Tohono O'odham Nation (TON) land.<sup>38</sup> In the recent past, however, sentiments have begun to change. Significantly larger numbers of people traversing the reservation, an increase in home burglaries, and a growing environmental disaster from the water bottles, garbage, abandoned cars, clothing, and other items transitors leave behind, have led to community efforts to police the reservation and to greater cooperation with U.S. agencies and state law enforcement. These efforts may create additional challenges for TCOs who use the TON lands to avoid detection from authorities.

Unlike groups operating on the northeast U.S. border, smugglers operating on the southwest border actively recruit on the TON reservation. Previously, only adult tribal members were involved with TCOs. However, criminal groups now frequently target young and much older tribal members. The recruiting pool from the large number of youth gangs on the reservation is attractive to TCOs. Given 60-70 percent unemployment of youth on reservations, the money is also appealing. Tribal members are employed primarily as scouts and lookouts and to help store commodities during transit. Interactions between TCOs and reservation youth often occurs through existing family ties (versus through non-family tribal members) and may include romantic involvements with young tribal women (e.g., common law marriages are recognized by tribal code). Some TCO members use their relationship ties on either side of the border in order to live legally on the reservation. Similar to tribal connections developed on the northeast U.S. border, relationships between TCOs and tribal families can endure for years—with both sides preferring to keep the relationship within the family. For some TON tribal members, family involvement in smuggling marijuana has become part of their way of life (Reina, et al, 2009).

## Legitimacy

Broadly, organizational legitimacy is the acceptance by a social system (e.g., society, community, neighborhood) of an organization's utilization of resources (e.g., human, natural, infrastructure) that

---

<sup>37</sup> According to tribal leaders and the Tohono O'odham Police, the Sinaloa drug cartel has majority-to-complete control over the Arizona border across the TON reservation.

<sup>38</sup> This is similar to one of the key elements of Pashtunwali tribal code of honor of protecting anyone on one's land asking for one's help.

could be used for other purposes (Dowling and Pfeffer, 1975). Organizations seek legitimization by justifying their right to exist to the communities in which they operate (Maurer, 1971). For legitimate organizations, common legitimization strategies include philanthropy, participation of senior officers on corporate and non-profit boards of directors, and scripted communications with stakeholders and to the public (e.g., annual reports, websites). TCOs also seek legitimization; social tolerance of their presence and activities allows TCOs to sustain operations (OCTA, 2008). Legitimacy makes it easier to justify one's illegal activities and violence that may harm members of the community and neighborhoods in which the TCOs operate. It also provides cover to authorities who receive benefits from TCOs for allowing them to operate outside of the law. Not surprisingly, achieving legitimacy requires some creativity by TCOs, but follows a similar strategy to legal enterprises.

Not all TCOs specialize solely in illicit activities. The connection of a TCO with a legal business operation lends an element of legitimacy to the group's other activities. Some TCOs operate legitimate businesses as front companies to help launder money associated with illegitimate activities (Margolis, 2009). Others invest in key sectors to control critical infrastructures or strategic materials, including oil pipelines and rare minerals, which provides cover and opportunities to influence important markets for their own gain (US Department of Justice, 2004). TCOs may also raid or take over a legitimate business, sometimes with the knowledge and assistance of corrupt government officials enriching both the criminal groups and the officials (US Department of Justice, 2004).

Relationships and networks that include a local population can also provide local or regional legitimacy and acceptance for a TCO. At a minimum, local or regional legitimacy and acceptance can reduce operational and organizational security risks and establish a safe haven for TCOs. On the northeast and southwest U.S. borders, legitimization activities by TCOs have included establishing business enterprises on the reservation and participation in community events. For example, one criminal group set up a cigarette manufacturing plant on the Canadian side of the Akwesasne reservation and employed locals to assist in smuggling the cigarettes produced on a reservation across the border for sale in the U.S. By placing the plant on the reservation and employing some tribal members, the group produced cigarettes legally, provided employment opportunities for some tribal members, and avoided taxes by smuggling the cigarettes into the U.S. (Thomas, et al, 2009).

TCO members, especially senior leaders, may participate in public or private political, charitable or social events attended by highly placed political, business, and community leaders. Appearing in published photos with respected individuals at these events creates the impression that TCO leaders are accepted and integrated into the inner circles of respectable society. Our study found that TCO members on the southwest U.S. border would occasionally attend church events on the reservation. Because these events are central to the tribal community and to tribal values and beliefs, attendance suggested shared values and beliefs by TCO members. These community events also turn out to be a good way to meet and become romantically involved with young tribal women (Reina, et al, 2009).

In some instances, TCO leaders are welcomed by local communities and political officials because the TCOs supplement inadequate public services or provide the only public or social services available in the community. They may also create order when weak, corrupt, or ineffective governments cannot (Marcella, 2009). Manwaring (2007) notes that some Jamaican posses (gangs) have accepted social responsibility to provide security to the residents in their territories and to help with education, health, and employment issues. In addition to developing support from the community, these gangs undermine the credibility and legitimacy of the state. Similarly, Hezbollah has a long history of providing social services directly (e.g., Hezbollah's Martyr's Foundation, Islamic Health Unit) or partnering with NGOs to provide health and social services to the poor and those affected by Hezbollah's military activities (Flanigan and Abdel-Samad, 2013). At the TCO senior leadership level, Pablo Escobar, considered the greatest Colombian drug lord, was loved and protected from authorities for the contributions he made

to improve the welfare of the poorest inhabitants of Medellin, Colombia (Bowden, 2002). In exchange for the schools, parks, recreational centers, and housing he built, the community overlooked Escobar's drug smuggling and violence. Escobar's election to the House of Representatives of Colombia's Congress can also be seen as testament to the legitimacy he created with the population of Medellin (Bowden, 2002).

The study could not document or confirm specific instances of TCO members becoming directly involved in tribal politics. However, there was evidence that TCO members established (or attempted to establish) relationships with tribal leaders or their families presumably to create opportunities for indirect influence in tribal decision making that could benefit their organizations.

### Implications for DOD, USG, and Law Enforcement

While traditionally considered a law enforcement issue, organized crime has developed into a powerful influence on the politics, economic viability, and governance of nation states. By virtue of their wealth, their ability to corrupt public officials at all levels, and their increasing control of legitimate markets, natural resources and key infrastructure, TCOs can distort global markets and threaten tightly linked economies.<sup>39</sup> The scope and consequences of the threat posed by TCOs may eventually exceed the ability of law enforcement to contain or prevent it.

Changes in the global environment and the expanding presence of commerce, public services and the social community in cyberspace are shaping the military's operational environment and will affect how and where the military protects national security. The focus on counterinsurgencies in the Middle East, repositioning toward Asia, and the creation of Cyber Command attest to the influence of the environment on military strategy and missions. As TCOs become more embedded in legitimate businesses, politics, and public services, they will become a larger and more persistent actor in that environment. U.S. national security strategy has acknowledged that the U.S. military should participate in counter-TCO efforts. In response, the DOD Counternarcotics and Global Threats Strategy (DOD CN&GTS, 2011) has directed CCMDs, the National Guard Bureau, and Defense Agencies to generate functional and regional strategies in their planning to primarily support interagency efforts and build capacity of partner nations. Although the strategy does not specify what actions and activities the military should take, it is clear that countering TOC will require a larger role for the whole of government, including the military.

The operational environment is changing. Assessments of key future trends which nations should recognize as signposts and should identify as opportunities for implementing change include the following.

- Diffusion of power across newer and different types on non-state actors including businesses and criminal networks and empowered individuals.
- Greater pressure on energy, food and water resources from economic and population growth.
- Greater potential for instability due in part to disaffected, unemployed youth.
- Increased potential for nationalization of resources.
- Increased migration into urban areas (National Intelligence Council, 2008, 2012).

Each of these trends represents an opportunity for TCOs to expand their influence on vulnerable states, and global economic and societal security. Criminal networks already use corruption as part of their strategy to control territory and markets. They have made inroads into the energy sector, taking

---

<sup>39</sup> Ongoing investigations are revealing organized crime involvement in Italian renewable energy projects, which receive large government subsidies. Similar instances of 'eco-corruption' have been discovered in Spain (Faiola,2013).

advantage of opportunities and government subsidies in renewable energy (Faiola, 2013), and will likely continue to leverage unemployed youth as part of their recruitment strategies. By controlling more critical infrastructure and resources (e.g., mining, wind farms), TCOs are likely to be active participants in regional and global conflicts over “public commons and goods.”

Another trend that must be considered is the rise of megacities. These highly populous areas stress public services and exacerbate the conditions that generate instability, violence and crime. This will only continue if rural populations continue to move into cities, as current trends suggest. Megacities will also create new definitions of urban warfare and challenge law enforcement and the military to innovate how they operate, use technologies and what equipment they employ. Because TCOs and local organized crime groups (e.g., gangs) are already skilled at instituting their own rule of law in territories they control, urban warfare in megacities that may have a significant TCO presence will present a new adversary with its own set of tactics and rules of engagement.

Finally, cyberspace will continue to be important. As TCOs expand into cyberspace, encounters between TCOs and the military (especially, Cyber Command) are bound to occur. Whether through disruption of service attacks, hacking critical infrastructure control systems, recruiting for specialized skills, or disabling military electronic systems and corrupting sensitive databases, future encounters between military cyber specialists and TCOs are likely to increase and become more complex. Preparation for a formidable new type of adversary begins with greater knowledge and understanding of who the adversary is and how it operates.

It is unrealistic to believe that TCOs can be eliminated. However, it is possible to significantly reduce their reach and impact. Effective strategies by the whole of government and law enforcement should begin with understanding the business models of TCOs and their business-related networks and alliances. Just as business organizations have experimented with different organizing structures and operating principles, TCOs are expanding beyond the business model and structure of La Cosa Nostra that criminal organizations have often emulated. Successful TCOs appear to adapt their operations to local conditions and geography. They utilize local resources and capabilities, outsource and enter alliances to further their interests, and rely on both local and global ethnic communities to network and operate.

The importance of acceptance by a community to TCO operations and security cannot be underestimated. Regardless of their occupation or criminal status, people are members of families, communities, ethnic, religious or tribal groups. Those connections partly define who a person is and provide a link that provides at least tacit acceptance into and legitimacy with a group. Migrations bring all members of a group or community, including the criminals, to a new location. Daily life, especially in a new location, is easier when surrounding others look and act similarly and share beliefs, values, and a common language. All of the law enforcement experts who participated in the study noted that criminals generally prey on their own families, ethnic groups and communities—at least initially. Moreover, criminals who are recognized members of a group are likely to be protected from outside authorities. Although the community may prefer to deal with them on their own, criminals can be an embarrassment to a newly established ethnic community (Gosselin, 2009; Reina, et al, 2009; Thomas, et al, 2009). Several of the experts we spoke with noted that one reason Mexican drug organizations often seek safe havens in American Indian communities is because they physically resemble the locals, can blend in more easily, and are less likely to be perceived as an outsider.

The recommendation to “think globally, act locally” appears to have been accepted by TCOs. Their reach, network, and the scope of their operations may be global, but they rely on networks at the local and regional level for much of their work. Having many local networks and alliances provides a measure of security against detection, but also provides greater flexibility to adapt to changing circumstances without adversely affecting operations. Reliability and customer satisfaction are as important to TCOs as

they are to a legitimate business to maintain market share in a highly competitive environment. Understanding the characteristics, organization and operations of the TCO adversary should be part of the military's preparation of the future battlespace.

## Chapter 9: The Symbiosis of Technology and TCOs and What that Entails for the Future

Dr. Valerie B. Sitterle

[Valerie.Sitterle@gtri.gatech.edu](mailto:Valerie.Sitterle@gtri.gatech.edu)

Georgia Tech Research Institute

### Introduction

Globalization, propelled by rapid technological advancement, presents unique and daunting security challenges for the U.S. and its partners. A tremendous and continually increasing degree of interconnectedness among financial systems, regulatory processes, markets, and communications intimately links societies across national and cultural boundaries. Global society is shifting from simple connectedness to true interdependency. Yet critical disparities persist across socio-economic health, access to resources, and even State stability in a geopolitical context. Together, these two factors—extreme interconnectedness and gaps in socio-economic and political equity—create an overall environment favorable to the formation and continued growth of TCOs. Current and future TCOs will be geographically and culturally dispersed. They will exhibit different socio-political tendencies and values and, importantly, evolve different socio-technical infrastructures to support and protect their activities.

This consequently presents an environment for future U.S. military operations considerably different from traditional force-on-force warfare. Whether engaged in IW or Security, Stability, Transition, and Reconstruction Operations (SSTRO), U.S. military and civilian personnel will face multiple threats from adversaries associated with various groups well embedded in, and across, local populations and infrastructures. In IW and SSTRO engagements, threats from disparate adversaries are compounded by technological underpinnings of societal structures (power, water distribution, cellular communication availability, etc.) and by rapidly evolving technologies on both sides of the conflict that may further disrupt the operational environment. Similarly, a technological action such as preventing local cellular communication may elicit a social, though still very real, reaction. TCOs, with their strong influence if not outright control over various segments of the population, resources, and potential collaboration with Violent Extremist Organizations (VEOs), are emerging as a significant threat in this dynamic.

This chapter will focus on the convergence of technology with social processes and, notably, the influence technology may have on the future evolution of TCOs and their operations. Similarly to large transnational corporations, TCOs already pursue global markets using advanced information, communication, and transportation technologies. Much as the emergence of a seamless electronic environment is giving rise to new societal structures and processes, TCOs are also evolving structurally and operationally. This creates new threats not only to our military personnel's success and security in future engagements, but also to our ability to effectively analyze TCOs. This chapter is thusly divided into three primary sections: a description of the socio-technical confluence and how TCOs employ technology, what this may mean for the future structural and dynamic nature of TCOs, and why this poses a great analytical challenge as we move forward.

## Socio-Technical Confluence and How TCOs Exploit Technology

### Socio-technical confluence

A society is, at its core, a set of intertwined rules (culture, processes, etc.) and resources (what is available for sustainment, including technological drivers) that bind it together. In the socio-technical sense, technology includes infrastructure, transportation, and information and communications systems. Increasingly, the latter are becoming an inseparable and vital component of the critical infrastructures of societies alongside more mature systems such as power and water distribution. Cellular communications with wide access to global positioning services (GPS) are now ubiquitous; vast leaps in interoperability across wired and wireless platforms have combined with the explosion of Internet technologies to provide services previously unimaginable. Technology has changed the very foundations of how we communicate and how we are influenced.

Social structures and processes in business, governance, and societal communication have merged with the evolving technological medium. What at first may have been a more symbiotic relationship between society and technology is now a true confluence. Just as the Ohio River cannot be separated back into its converging feeders, the Allegheny and Monongahela, the socio-technical nature of globalization is no longer treatable as separate elements. This blended reality is now a part of our future and is dramatically affecting how we view the world as well as how we operate within it. The impact of socio-technical confluence may be described as a triad of inter-related concepts, listed below.

1. Use and pervasiveness of technology shapes, mediates, and alters social perspectives, behaviors, and dynamics.
2. Groups within society further exploit technology to influence social beliefs, behaviors, and systems in pursuit of their own goals (whether creatively or disruptively).
3. Actions taken that directly impact use, access, or performance of a given technology can dramatically alter societal behaviors, provoking direct response or pursuit of alternative means. Conversely, use and performance of emerging technologies can spur policy or even direct technological interference by State or non-State actors.

For this chapter's discussion, we will focus primarily on how advances in information and communications technologies (ICT) shape and mediate social dynamics.

Firstly, there is a drastically shortened time constant coupled with a sweeping increase in availability across all levels of society compared to old modes of social interaction and information sharing. Quite simply, data is available nearly instantaneously and can be supplied by nearly anyone to the global community—whether it presents accurate information or not. Most people with Internet access can just as easily find instructions for making an improvised explosive device (IED) as they can a movie review. Content that is legal in one country may be illegal in another, yet equally accessible.

There is also an increasing tendency to believe information posted online as vetted truth, especially among the younger generation who also share a great deal of personal data with little qualms (Beldad, de Jong, & Stehouder, 2010; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Influence and trust dynamics are evolving unique to the new modes of interaction, which enable communication and reach characteristics distinct from face-to-face or single-conversation technologies. Social interaction today is readily accomplished across national boundaries, cultures, and social standing; anonymous or

alternate identities can be created with ease. The online world can offer “real” connectivity, or it can be a conduit to a sense of exclusivity and empowerment vastly different from one’s physical world existence.

The pervasiveness of ICT-provided data and services in the daily social dynamic creates new pathways for marketing, persuasion, and literal steering of users toward certain data ecosystems. For example, many businesses including Google, Facebook, and Amazon frequently control what information ICT users find. Internet searches are filtered; automated algorithms collect and mine user tendencies to steer them toward other users, products, services, or online sites with related content deemed of interest ("The dangers of the Internet. Invisible Sieve,," 2011; Rasmussen, 2012). These filtering and recommendation techniques steer users according to the strategic goals of the business and not simply user preference.

People sought to surround themselves with “likes” in the old, physical paradigm, so this phenomena is not entirely new. Yet ICT users today seem oblivious to or unconcerned with the skewered view they frequently receive. The recent vote Facebook put forth to its roughly 1 billion users on changes to data usage, privacy, and even the right to vote itself exemplifies the trend. The vote garnered response by an underwhelming 0.0668 percent of its users (Farber, 2012). This matters because modern communication technologies together with the explosion of electronically available information have hyper-connected markets and societies across the globe. Time, distance, and cross-cultural interaction simply are not constrained the way they were. A “filtered” worldview with these dynamics can have destabilizing and unanticipated effects on the socio-political-economic fabric at local or transnational levels.

Despite this filtering, access to data and communication is immense for increasing numbers of the world population compared to even 40 years ago. The wealth of information and contrary perspective motivated users may find with ease—and communicate en masse—can be similarly destabilizing to government and/or religious structures that strongly desire to control their society’s behavior. Iran and China, for example, have implemented restrictive controls, filtering or blocking data deemed “sensitive”, requiring identification of users, and even constructing internal Internet structures to control user access to information and communication ("Iran readies domestic Internet system, blocks Google," 2012; Osborne, 2012). In cyclic fashion, other advances emerge to circumvent these controls: proxy websites, virtual private networks, anonymous peer-to-peer distributed applications (Darknets), TOR (The Onion Router), and Java Anon Proxy are examples of alternative systems to access or transmit restricted information with varying degrees of anonymity.

The online world is also replete with deception. It can be simple, as when individual users create alternate identities they desire for certain interactions. The aforementioned evolving trust dynamics coupled with the ease of anonymity enable social deception with great ease, whether for amusement, fraud, espionage, or recruitment for some cause. Deception can also be large-scale. There is an entire underground economy of skilled users selling skills and tools for automated data generation and security circumvention. The result can be automated creation of false accounts, personal profiles, Twitter followers/messages, etc. (OnlineTrustAlliance). A recently cited study by Solve Media projected that 10 percent of all online traffic is now due to bots (software applications that run automated tasks) (Peterson, 2012), while a recent SEC filing by Facebook estimated that 8.7 percent of its 955 million registered accounts are fake, duplicate, nonhuman, or spam accounts (Protalinski, 2012).

## Use of modern ICT by TCOs and other fringe groups

The socio-technical ecosystem offers as much opportunity and convenience to criminal and ideological elements as it does the general population and legitimate economy. TCO's are becoming increasingly savvy with respect to exploiting ICT elements for their own goals and are able to pay top dollar to highly skilled experts and hackers amenable to facilitating their operations for fee. Broadly speaking, TCOs form and flourish for either provision of illicit goods and/or services or infiltration of legitimate businesses (fraud, intellectual property piracy, extortion, etc.). Inclusive of both categories, the ICT realm is rapidly blossoming into a lucrative market for counterfeit products (e.g., digital media, software) and cyber disruption or data corruption (whereupon a victim must pay to unlock and retrieve it) (Choo, 2008).

*TCOs use ICT either to facilitate their business operations or to expand into a cyber-criminal business space – the distinction being ICT as a tool versus ICT as a target of opportunity.* Both take advantage of the relative lack of international boundaries together with the speed and convenience of modern communications and information exchange. As tools to expand or more expediently coordinate operations, TCOs use ICT to communicate much like the everyday populace. Financial and transportation global architectures as well as ICT enable TCOs (and, incidentally, ideologically driven groups such as VEOs) to operate transnationally while maintaining a primary physical presence in a location or locations favorable to their operations and existence (Picarelli, 2012). TCOs use technologies ranging from disposable cellular phones to messaging services and coded exchanges in online forums to facilitate both local and transnational communication. In other manifestations, TCOs may construct and operate physically realized private networks. The Zeta Cartel in Mexico built a network comprised of easily movable and replaceable antennas, signal relays, and simple hand-held radios to conduct territory reconnaissance and circumvent authorities (Weissenstein, 2011). *The lesson is that modern communication technologies are widely available for public purchase, and the expertise to required to set-up and maintain such networks is either already a part of or readily available to TCOs and other threat organizations.*

Organized criminal groups also widely disseminate targeted messages via blogs and other media to influence or even intimidate targeted sectors of their environment. Their motivation is similar to businesses and activists (ideological and political) that have long sought to strategically influence localized or broad segments of society through online channels. Targets include local populations, government regulatory or police groups, or even rival criminal organizations (Choo, 2008). Through these approaches, TCOs aim to help shape an environment favourable for their operations and continued success. Online dissemination of propaganda, extortion, and psychological intimidation by posting video of kidnapped victims or torture of rivals is increasingly common. Social media sites have even served as a tool to identify and target potential kidnapping victims (Longmire, 2011).

Because of the pervasiveness of ICT across all sectors of society and business, online tools and platforms are excellent pathways for TCOs to commit fraud as well. Fraudulent activities encompass identity or other credentialing theft in order to access financial accounts, create fake credit cards, passports, or other documentation. Fraud is therefore both a direct means of profit as well as a tool to facilitate other TCO operations such as transport and sale of illicit goods. Alternatively, TCOs may exploit ICT to launch attacks on various societal infrastructures, whether communication, financial, or civil support systems. These attacks are often for extortion, or they may create confusion that creates a window of

opportunity for safe transport of illicit products. Though still using ICT as a tool, these activities require more advanced technological expertise. Again, these techniques are also available to and exploited by VEO or other ideological groups (Choo, 2008; Eccarius-Kelly, 2012; Holt, 2012).

Exploiting ICT as a target of opportunity carries its own nuances. Traditionally styled TCOs that sell illicit commodities in the physical world may expand their criminal activities to cyber markets with relatively little need for additional resources and physical expansion. All that is really needed is to identify a target of opportunity and then find individuals or small groups with the required expertise for hire or incorporation into the enterprise. A TCO that exists to profit solely due to the cyber realm may present a different structural and operational paradigm altogether. A cyber-TCO enterprise may be drastically smaller than more physically established counterparts because it may accomplish its goals with fewer members and less extensive facilitating networks. Its reach, however, may be nearly unlimited given the socio-technical nature of modern globalization. In either case, cyber criminal activities may occur on a temporary basis according to opportunity. There is no need for expansive, permanent enterprise networks.

The avenues for profit are twofold. First, hackers and other individuals and/or small groups with strong expertise sell their skills or tools to TCOs or any other group willing to pay for their malware creations and services (a fee-for-service approach) (Holt, 2012). This may include development of specialized bots for Denial of Service attacks, malware for identity, password or other credentialing theft (which can then be used to defraud bank accounts, clone credit cards and passports, etc.), and malware for other disruptive attacks. Second, cyber TCOs form specifically with strategic members possessing the aforementioned expertise. These TCOs leverage their particular combination of skills, which they may choose to grow, to focus on any portfolio of markets existing within or directly due to the cyber realm. In addition to fraud and extortion, this includes digital media and software counterfeit and piracy. These two areas are often linked; a great deal of counterfeit or pirated digital media and/or software is infected with malware (e.g., a recent Microsoft study cited by ZDNet (Qing, 2012) discovered that 63 percent of pirated software in Southeast Asia is infected with high-risk malware).

Many recent examples of cyber attacks are described in reports from ZDnet and SecurityOnline (the Kaspersky Security Bulletin), often in great technical detail (Assolini, 2012; Clark, 2012; Dignan, 2012; Gostev, 2012; GREAT, 2012; Phneah, 2013; Semantec, 2012; Tarakanov, 2012). These case studies exemplify how multiple tools and techniques may hide the attack from immediate discovery as well as obfuscate the origins of the attack and identity of those responsible. Importantly, cyber crime can be exceedingly difficult to distinguish from cyber attacks as terror or from entities with any range of political or ideological motivation. This is partly due to similar targets and techniques, and partly because there is a lack of global consistency in what constitutes cybercrime (Holt, 2012).

### **Complexity and the Structural and Dynamic Evolution of TCOs**

### **Complexity and the Importance of Local or Transnational Context**

The degree of societal “differentiation” is increasing as technologies permeate and empower individuals and small groups in new ways. Though seemingly counterintuitive, a well-established understanding in biology is that complexity arises from such specialization. As system entities lose capabilities and become more specialized, an increasing number of outcomes are (and can only be) achieved through interaction with entities having different capabilities or properties (Finnigan, Hanson-Smith, Stevens, &

Thornton, 2012). This holds true across biology, society, technical systems, and their intersections. Individual interactions generate macro-level characteristics and dynamic patterns not found at the micro-level.

The link between macro- and micro-level behaviours relates directly to concepts of emergence, or system evolution. Whichever term is used, it describes a process whereby a macro-scale system property is created as a consequence of repeated interactions among system entities at the micro-level. Because there is often no discernible connection between the micro-level rules and the higher dimensional characteristics, John Holland coined this “hidden order” (Holland, 1995). It is conceptually analogous to the chicken-and-egg dilemma: influence between the macro-level (the environment and other systems) and the micro-level (individual groups or entities within a defined system like a TCO) is bi-directional.

We can translate this to understand TCO behaviour and evolution as transnational enterprises. Similar to biological systems, specialization and interconnectedness of many functional units and networks drive TCO behaviour. Networked layers of local production and supply mesh with higher-level financial and logistical networks that extract and sell illicit commodities. Additional facilitating layers assist with money laundering, obtaining fraudulent documentation, and other services. Many entities in these expanded criminal enterprises are legitimate businesses, existing either as a facilitating front or collaborating for financial gain, while cross-border activities are further supported by diaspora groups through legal or illegal immigration (Farah, 2012).

Individuals or specialized networks comprising a TCO alter their behaviours in response to environmental characteristics while striving to preserve certain goals (financial reward, avoiding prosecution, maintaining market dominance, etc.). These behaviours become patterns that are converted to changes within the TCO's own internal structure and/or processes. The resulting mutations in TCO internal structure and/or outwardly directed actions impact the myriad of facilitating networks, other criminal or ideological groups (whether collaborative or competitive), local societal structures and processes, government responses, etc. that together form the TCO's environment. The “environmental” variation affects the TCO's behaviours, and so on in recursive fashion. Because all of these systems interconnect, small changes in one sector can have unpredictable and disproportionate consequences to another.

Often, the local context of these TCOs and what they must control or influence to successfully achieve their goals in the regional sense is quite distinct from the transnational context of their business. In the latter, distinct support networks are subject to their own local environmental pressures and possess different levels of autonomy depending on their function within the enterprise. The resulting TCO structure is often flatter in a hierarchical sense, with increased connectivity to other criminal groups, than the regional criminal organization(s) from which they originated. This suggests that the structure of a TCO enterprise may look quite different depending on whether a model or analysis targets the local or transnational context.

### **Structural Variation and Dynamic Evolution of TCOs**

Structurally speaking, TCOs evolve both structurally and dynamically (organizational processes). Traditionally styled TCOs are not designed from inception with a complex, highly networked, and layered transnational structure in mind. Instead, like biological organisms, they mutate in response to

environmental pressures ranging from market opportunities to government stability and even emergence of other criminal or VEO groups. Adding to this complexity, TCOs not only react to their environment, they actively seek to redefine it in ways favorable to their activities. TCOs continually undermine social or governmental organization systems to ensure the “right” level of instability or control. And in pursuit of new opportunities, they seek new pathways and facilitative support, affecting yet more social and governmental systems in the process as well as their own structure (Andersen, 2011).

The natural mutation of TCOs over time is further complicated by expansion into emerging markets made possible by current (and future) ICT advances. Consider the PKK in Turkey, which is known to have a strong centralized control of criminal and guerrilla activities. As the PKK expanded into new relationships to pursue new opportunities, ICT advances allowed them to develop multiple, distributed points of operational control. Yet over time, these physically separated extensions began to take their own initiative in the political realm and operate with a more pluralistic agenda (Eccarius-Kelly, 2012).

Many complex combinations of fluid and adaptive networks may support the criminal operations. The triads in China, for example, exhibit a flexible and decentralized structure with no single unifying body over all triads. Organized crime in the “Golden Triangle” (where Myanmar meets northern Thailand, northern Laos, and southwest China) has opportunistically linked with local insurgencies, elements of local and national governance, and international crime syndicates in an ebb and flow with ethno-political dynamics and market forces (Broadhurst, 2012). The presence of formal or permanent structures and relationships is not always a necessary condition defining TCO capabilities.

Cyber TCOs are a further example of this point. TCOs that exist solely to exploit the cyber realm do not tend to exhibit the same degree of structure and operational support as their more traditionally established counterparts and may completely lack a localized (even if distributed in multiple locations) cultural presence. Criminality in the cyber domain requires minimal organizational capacity and physically traceable presence compared to production and supply of illicit goods such as drugs or weapons. TCOs that exist to take advantage of these opportunities can form and disband relatively quickly. They can also organize and sustain their operations in a highly distributed fashion. In fact, cyber TCOs may not have a primary physical presence or personal connection among members at all (Choo, 2008; Holt, 2012).

### **Challenges in Defining Relationships or Hybridization with Ideological Groups**

A second significant challenge to effective characterization of TCOs is the hybridization of TCO and VEO characteristics, techniques, and networks of expertise. A prevailing view has been that TCOs and VEOs are driven by such different motivations (money versus ideology) that collaboration will always be sporadic and based on personal connection more so than longer-term operational drivers. There is, however, a universal truth: both TCOs and VEOs need resources to operate and assert their power. Additionally, environments most conducive to the formation and support of TCOs possess the same characteristics as those where VEOs spring up and flourish (Eccarius-Kelly, 2012; Picarelli, 2012; Sharma, 2013).

The Columbian FARC, Abu Sayyaf Group in the Philippines, and Turkish PKK are all examples of insurgencies demonstrating increasing tendencies toward criminalization. It remains challenging, however, to discern whether this signals a true shift or if they remain ideologically motivated and are

just pragmatically expanding to secure resources (Eccarius-Kelly, 2012). Dawood Ibrahim's D-Company in India offers another example of overlapping criminal-terror activity and organizational collaboration. D-company began as a smuggling operation, grew to a significant TCO, and then began to augment its operations with Islamic ideology, collaborating with and supporting various VEOs along the way as well as undertaken terror activities of its own (Picarelli, 2012; Sharma, 2013).

Collaboration between or outright hybridization of TCOs and VEOs may currently be largely circumstantial, though favourable circumstances for both exist. Growing and persistent socio-political inequalities raise insurgent potential; globalization via ICT transformation and increasingly hyper-connected markets and economies blurs boundaries and even authority across socio-political processes and State control. Opportunities for TCOs and VEOs to work side-by-side, overlap, and even merge aspects of their organizations or goals are proliferating. In turn, this expands the likelihood of TCO and VEO entanglement in the future. Striving to grasp crime-terror convergence dynamics aside, the potential for hybridization presents a major analytical problem. TCOs, VEOs, and their collaborations may fluctuate back and forth in time and on the criminal-ideological spectrum according to environment and opportunity. Many of these organizations may no longer fit neatly into either category as a structural organization or an evolving entity interacting with its environment.

## Challenges Facing Operationally Relevant Analytics

### What Are We Trying To Do?

Given the complexities discussed thus far, the operational and scientific communities must articulate our goals regarding TCOs to construct effective analyses. In an era of limited resources for analysis, yet an exploding electronic data universe and commensurate proliferation of supranational structures and dynamics, what do we really care about? As humanistically abhorrent as they may be, are the criminal pipelines and products (drugs, weapons, or human trafficking) our target? Or, do we seek a longer-term, more transcendent approach to define future transnational capacity to disrupt and prosecute TCOs? The list below offers a range of potential goals for analyzing TCOs and their impacts, and many are highly inter-related. The following nuances may also be helpful: "dangerous" depends on perspective (perhaps national), and "regions" may refer to abstract features or intersections (markets and financial systems) instead of simply geophysical spaces.

1. Monitor hot spots, or regions of risk, where TCO activity may, firstly, form or significantly expand, or, secondly, create a dangerously destabilizing effect. This encompasses the need to identify which geo-political spill over aspects could adversely impact our national security, whether economically or militarily.
2. Improve understanding of TCO structural and dynamic mutation for growth, shift in focus, and self-sustainment, inclusive of TCO relationships with other complex systems (e.g. VEOs, socio-political systems, and financial systems).
3. Use greater understanding of TCOs to better forecast expected or possible TCO behaviours.
4. Improve understanding in order to better predict unanticipated consequences of proposed actions (policy, military operations, economic, technological) to TCOs and the systems with which they are enmeshed.
5. Define how TCO establishment of political and financial influence, especially in concert with VEO expansion, can directly impact American economic stability, border security, and success/

security of military operations. In tandem, define what resources and actions are necessary to monitor and disrupt TOC operations prior to adverse impacts reaching our interests.

6. Identify principles and intersections key to helping better define necessary international collaboration and capacity to combat TCO activities.

Ideally, one may say “all of the above plus ten more.” Realistically, however, one may find that a lack of resources, international cooperation and consensus, and data to inform analyses may hinder such ambitions. The following sections briefly discuss the challenges of defining our analyses and collecting and characterizing data on which to base them.

### Can We Define the Problem?

There are a myriad of ways in which analyses of TCOs and their impacts to legitimate socio-political and economic systems can be approached. Typically, many research efforts categorize according to (Broadhurst, 2012; Farah, 2012; Picarelli, 2012):

- Nature and type of organized crime by market or geopolitical jurisdiction;
- Classification of organized crime by methods and operational principles;
- Identification linkages to facilitating or collaborating networks via social-network or transactional approaches; and
- Identification of markets or geopolitical jurisdictions at high-risk for TCO penetration.

Regardless of the analytical perspective, defining what constitutes “criminal” is not always unambiguous or even compatible in a transnational sense. Similarly, the previous discussion highlights the issues concerning increasingly blurred delineation between TCO and VEO groups. In a recent review, John Picarelli at the DOJ points out (Picarelli, 2012) *“the terms ‘organized crime’ and ‘terrorism’ are applicable to describe not just activities but also the organizations that perpetrate these activities.”* He excellently articulates how crime-terror interaction is not limited to organizational linkages but also includes activity appropriation. Definitions set the scope of what is considered in any analysis, and those definitions that are too broad or too narrow can dramatically change the findings.

This aspect is critical as various analyses are combined in an effort to more thoroughly encompass the scope of complexities contributing to the problem(s). Different analyses may use such different bounds of definition or foundational assumptions that they *should not* be combined. Being cognizant that analyses help lay the foundations for policy or action, and that international collaboration is necessary to disrupt TCOs, definitions matter.

### Data is a Challenge

What is data today? In the ICT sense, “big data” is the current catchall phrase describing the wealth of data generated from billions of Internet searchers, Social Media sites and services, ATMs, smart phones, traffic cameras, online financial transactions, and any other ICT “connected” device or system. The worth of this data and how to turn it into information lies in individuals’ abilities to categorize, process, and shape it into something meaningful and useful. Billions of objects are already operating and interacting with each other, and more and more devices and systems are being created with automated (or “self-aware”) functionality. Just a short time ago, people were primary “sensors” inputting data to the electronic world, while still important now technological advances are steering people toward certain information according to various algorithms and motives, and automated tools generate a

multitude of other—some false—accounts and connections, the nature of the data is harder to ascertain.

Quite a bit of data that might support TCO analysis is simply very hard to find. This is partly due to the generally hidden nature of criminality and partly due to a lack of resources or will by many governments to collect it. Some data is still qualitative or rhetorically based and may not be captured electronically. Geo-coded data sets are useful, especially for geo-political referencing and visualization, yet a lot of data still lacks this attribute. Other data (e.g., financial transactions) may be quite structured, coded, and quantifiable, assuming it can be found and attributed to criminal activity.

### **Parting Thoughts: Future Operational Challenges and Needs**

Technological advances for information sharing and communications have already changed the socio-political, financial, and military operational dynamics in ways that were not anticipated just a few decades ago. As new developments emerge, whether through singular effect or in complex synergy, they will present unique potential opportunities and threats. The following perspectives extrapolate on what approaches may help support effective analyses of TCOs and how new developments could threaten our interests and capabilities in the future.

### **Analytical Frameworks**

The analytical challenges presented previously are all interrelated. To conduct empirically grounded analyses, the available data needs to be characterized, its reliability, and whether its foundation (how it was classified for collection) may conflate definitional boundaries. Analyses may present dramatically distinct perspectives due to scale (local or trans-regional), underlying assumptions, hierarchical layering of structures or processes, or problem dimensions represented. No one model or analysis will capture *all* of them. Based on what dimensions of a problem we seek to analyze, it is necessary to understand what data can or should not be combined before striving to characterize which analyses can or should not be combined.

Though everything cannot be addressed simultaneously, there continues to be a focus on socio-cultural, -political, or -economic viewpoints but a comparative dearth of socio-technical perspective. The community should develop new approaches to blend the social components with consideration of technical systems that frequently enable, shape, and mediate those behaviors. This will help create realistically grounded and actionable outputs. Two primary questions may serve as a starting point to help develop a framework for analytical synthesis and address these issues, listed below.

- Which dimensional combinations are required to address which operational problems or classes thereof?
- What architectures and methods will enable meaningful and effective combination of different analyses with distinct dimensions and outputs into an informative and relevant whole?

### **Rapidly Evolving ICT: Software Defined Radio**

Software-defined radio (SWDR) is a fairly recent ICT development in terms of its availability to the wider public. Once limited to research labs and already developed for military use, SWDR technology is now available on the open market with a wealth of guidance and free software in the open source community. Significantly, prices are dropping as capabilities increase. A new SWDR board covering 100

megahertz to 6 gigahertz will retail for US\$300 (Greenberg, 2012), while another start-up will offer an integrated SWDR package for the masses for around US\$750 (Lee, 2012). The power of SWDR lies in its versatility. Whereas traditional radio chips are limited to a specific communication protocol (e.g., cellular, WiFi), SWDR is tunable across the electromagnetic (EM) spectrum for nearly any protocol. This includes GPS signals, RFID chips, cellular communications, FM radio, digital television, and others. SWDR can transmit and receive, shifting across frequencies or even using them simultaneously as controlled simply by software (typically from a laptop computer).

It means that anyone with SWDR hardware and the right software and skills can create their own communication protocols, or intercept (and reproduce) communications from those already established. This fundamentally impacts the security risks to existing communications systems face: cellular communications, radio frequency-based entry systems, police radio, and air traffic control systems are all at risk. Societally, SWDR may potentially undermine Federal Communications Commission (FCC) control here in the U.S. Militarily, U.S. forces may face altogether new threats because of SWDR advances during future engagements, including obsolescence of current technology platforms. For example, current electronic attack jamming systems are designed to interfere with a range of cellular and other communications signals to prevent communication among combatants, EM-signal triggered IED detonation, or other electronically based threat activity. SWDR can redefine these threats. TCOs and VEOs are expected exploit this technology in the future, both as a means of offensive and defensive action.

#### **Data Obfuscation: Identifying the Threat**

As the data universe becomes increasingly autonomous and machine-generated, devices are evolving into the true sensors with people taking a more facilitating or receiving role. Information these devices or other ICT media present to individuals forms an increasingly significant basis of how they feel or behave. This creates two distinct risks. Firstly, machines and artificial intelligence may largely shape the data ecosystems in the future, molding perspectives of individuals and groups and therefore their actions. Given the complexities of the data universe coupled with data collection and steering algorithms modified via artificial intelligence, society, governments, and researchers may not realize the full impact or extent of this dynamic on socio-political evolution may not be realized. Secondly, because of this dynamic, automated data generation may offer an immense potential for deception. TCOs, VEOs, and other ideological or activist groups may use bots or malware to create surges in auto-generated data including text feeds, online posts, accounts, and account linkages, etc. This practice could create the perception of panic or instability where no physical manifestation of that reality exists. Such large-scale deception via cyber media and means may sway socio-political opinion to spawn instability across government or even financial systems. Alternatively, these techniques may intentionally obfuscate attempts by authorities to detect and track the online presence and activities of these groups. In the words of Marvin Gaye: "Believe half of what you see, son, and none of what you hear."

#### **Transience and the Power of the Masses**

Modern ICT capabilities allow TCOs to rapidly recruit expertise and employ various skills on a temporary or transient basis without the need to formally augment their enterprise. Similarly, VEOs may recruit and sway sympathetic individuals without relying on old methods of radicalization or complete indoctrination to the cause (Holt, 2012). Since online behaviours are often more brazen or disconnected

from physical reality, people frequently perceive less personal risk when connecting and acting electronically. The modern phenomenon of “flash mobs”, where a group of people organized via ICT channels appear suddenly in a public space to do something unpredicted, offers an example from which we may extrapolate how this TCOs and VEOs could exploit this dynamic. These flash mobs have so far been mostly amusing. In another manifestation, a TCO or VEO could recruit an online-only “flash mob” to help launch a substantial attack on government, economic, or critical infrastructure systems using Internet connections distributed across individual members of the “mob”. TCOs may discover this approach helps obscure other activities and distract authorities; VEOs may be attracted to the sheer power of the masses to further their own vision. These aiding users do not face the same physical risks they would in an assault, and the action’s online nature may allow them to emotionally distance themselves from its real impact. The bar for radicalization may be substantially lower; financial compensation may not be necessary. The potential threat, whether criminal or ideological in origin, is the same.

### Defining a Cyber Plan Synergistic with Military Operations

Unstable governance structures and extreme socio-economic inequities open some geopolitical regions to a much greater risk of criminal or ideological manipulation and growth than others. Security experts anticipate that some of these areas, particularly Africa and parts of Asia, may produce an explosion of cyber-related crime (Roberts, 2012). Adding to the confusion and risk, a cyber attack could originate or appear to emanate from the area, the latter possibility based on the true source’s technological savvy. Concrete attribution of responsibility may not be possible. Together, these factors and the very presence of State funding or outright participation in cyber attacks result in a great deal of mistrust across the global community. The recent arguments and contentious environment at the World Conference on International Telecommunications (WCIT-12) summit regarding Internet governance and the role of the International Telecommunications Union (ITU) exemplify the perspective chasm. Given pluralistic motivations and suspicion inherent across public and private sectors, the global community lacks sufficient agreement—much less collaboration—to define preventative measures, legislation, or unilateral actions that could or should be taken against identified cyber-criminals or cyber-terrorists.

Unique military operational challenges are emerging from modern communication and information exchange dynamics as well. In the ICT sense, where do the threats stop and the civilian infrastructure begin? If interfering with cellular communications or Internet access is operationally necessary, for example, it will impact combatants and non-combatants alike. With ICT systems now integral components of States’ critical infrastructures and interwoven with the social fabric, what response(s) will actions like these elicit in different geopolitical regions? As a community, we must develop a better fundamental characterization of the cyber-socio-technical nexus to help form cogent defense-related policies and guidance for operational context. Similarly, the context of delineations that do or should exist with DOS responsibilities should be considered to successfully appraise and defend against risks to our national interests outside of and in concert with military engagements.

## Chapter 10: The Geopolitics of Clandestine Innovation in the Drug Business: A Framework of Analysis to Understand Adaptation Capacities of TCOs

Rodrigo Nieto-Gomez, PhD

[rodrigonietogomez@gmail.com](mailto:rodrigonietogomez@gmail.com), [rnietogo@nps.edu](mailto:rnietogo@nps.edu)

Naval Postgraduate School

TCOs operate as fully developed platforms for innovation that compete violently with each other to provide to deviant entrepreneurs some of the key advantages of what Michael Porter labels “business clusters.” A porterian cluster is defined as a “geographic concentration of interconnected businesses, suppliers, and associated institutions in a particular field that are present in a nation or region. Clusters arise because they increase the productivity with which companies can compete” (1998). Silicon Valley is probably the gold standard of porterian clusters, and many governments around the planet have been trying to artificially create clusters as a central objective for urban planning and economic development.

In reality, the track record of artificially managed urban planning policies to encourage innovation through clusters is controversial. For example, a recent study of innovation dynamics in Norway found that “firms that develop international partnerships are likely to innovate, firms that rely on national and local interaction are not, meaning that the transfer mechanisms of knowledge and innovation within close geographical proximity are either broken or less prominent than previously thought.” (Fijtar & Rodriguez-Pose, 2011, p. 32). The study did find an important nexus between “global pipelines” and radical innovation, that is “purpose-built connections between a given local firm and partners in the outside world. Partners can range from other firms, suppliers or clients, to universities or research centres.” ( Fijtar & Rodriguez-Pose, 2011, p. 8) From the results of this study, Vivek Wadhwa, one of the biggest innovation “gurus” of Silicon Valley goes as far as labeling regional cluster policies as “modern day snake oil,” because in his view, they obsess over the wrong thing. Wadhwa (2011) provides what he calls a “formula for nurturing growth”:

We need to remove the obstacles to entrepreneurship — such as knowledge of how to start companies, fear of failure, lack of mentors and networks, government regulations and financing. And we need to repair our university research commercialization system so that research breakthroughs translate into invention. That’s the correct formula for nurturing regional growth.

At the center of this controversy is a geopolitical question: What is the relation between territory, global pipelines (or networks) formed by human capital and radical innovation? The question is relevant for the innovation dynamics of TCOs, as they are surrounded by a singular innovation environment that combines the organic and unpredictable emergence of deviant porterian clusters, with the innovation nurturing formula that Vivek Wadhawa considers central to effective entrepreneurship, and a dark pipeline that promotes knowledge-transfer to propagate successful deviant innovations throughout the network.

## The Emergence of Deviant Innovation Clusters in the Mexican Geography

The geopolitics of the criminal drug business in Mexico are defined by an evident hegemonic dominance of Sinaloans. The state of Sinaloa provided to drug smugglers with “the needed geographic and climatic conditions, good infrastructure, the required know-how from certain Chinese immigrants who knew how to cultivate and prepare opium, an entrepreneurial ethos, and probably better protection by the police...” (Astorga, 2004). That is, Sinaloa, particularly the region surrounding the municipality of Badiraguato, provided the cluster of interconnected organizations, suppliers and institutions to innovate and produce the sustainable smuggling market that TCOs run today. While the first recognizable cartel in Mexico received the name of the cartel of Guadalajara because its headquarters were located in the capital of the state of Jalisco as a consequence of law enforcement operations, it was founded by the Sinaloan Miguel Angel Felix Gallardo and run by Sinaloans who never lost their geopolitical relation with the Sinaloan territory.

When Felix Gallardo decided to split the cartel of Guadalajara, the division of this “parent cartel” triggered the formation of four spin-offs: the cartels of Tijuana, Juarez, Golfo and Sinaloa. These new organizations were meant to create a collaborative business environment by distributing peacefully key smuggling routes among important criminal stakeholders. As we know today, the peace would not last.



Figure 13: Geopolitics of the original deviant innovation territories in Mexico

This original group of deviant entrepreneurs migrated to other territories, taking with them key components of the cluster. One way to think about this is to imagine what would happen if an external eventuality (probably a big earthquake!) forced the entrepreneurs of Silicon Valley to fragment and move out of the Bay Area, bringing with them the intellectual property, the companies, the business connections and financial capacities to new territories (Figure 13).

Sinaloa provided the conditions of a successful business cluster from where the Mexican drug cartels evolved into the highly complex criminal business operations they are today. The decision to split the original monopoly that had emerged from that cluster into four different geographic regions distributed not only the routes for drug smuggling, but also the innovation capacities of deviant entrepreneurs and encouraged a fierce competition among the four new organizations, producing the exact opposite effect of the “peaceful” objectives of the division. This expansion and fragmentation has continued beyond those original territories, and as a consequence the Mexican territory is today covered with many competitive deviant clusters (with different levels of success), where some or all the required conditions to become a clandestine innovator are collocated, or at least easily accessible.

Without a central planning authority managing cluster formation, TCOs that operate in the Mexico innovate and compete to survive, remaining profitable in the context of a deadly, non-regulated and highly competitive environment. They create responses to public policies that are simple and cost-effective, and consistently penetrate the centrally planned security deployments of the governments of Mexico and the U.S.

At the same time, pipelines of criminal businesses, service providers, institutions and protection are all available in many territories for the deviant innovator who may want to enter the high risk/high reward world of TCOs, where information flows and innovation is replicated throughout the system.

### **Deviant Pipelines: Learning From Others To Do Right The Wrong Thing**

As previously mentioned, TCOs benefit from both sides of the geopolitical controversy vis-a-vis the relation of territory and innovation. On the one hand, enough clusters have emerged in the Mexican geography to scaffold the innovation process of deviant organizations with a complex network of clandestine institutions that make them sustainable. This indicates that deviant innovators have geographic spaces from where it is possible to start and grow profitable transnational criminal organizations. While there are multiple spaces in the planet that can serve as safe havens for clandestine non-state actors, not many of them have the right elements to serve as an innovation platform to create criminal startups and grow them to become a link in the chain of multibillion-dollar global operations.

On the other hand, the competitive environment in which TCOs operate has already removed the previously mentioned individual obstacles to entrepreneurship that Vivek Wadhwa identified (2011). This encourages the formation of deviant pipelines that distribute knowledge at multiple geopolitical scales (local, regional and international) among the people that form clandestine networks through the ways listed below.

1. **Knowledge about how to start deviant companies and mentoring.** There is enough knowledge in the system to educate potential deviant innovators about how to start a smuggling company. The knowledge is reproduced through an effective mentoring and apprenticeship pipeline where individuals get to learn, "on the job," how a specialized portion of the drug business operates, from other entrepreneurs.
2. **Fear of failure.** The fear of failure takes a different meaning when the life and freedom of deviant entrepreneurs depends on the success of their operation. While a very special kind of risk management is at the center of the decision making process of TCOs, the organizations are naturally formed by people who have a high-risk tolerance.
3. **Government regulations.** The business environment of the TCOs is mostly unconstrained by governmental regulation. Supply and demand of the criminal products or services dictate the price; the product is sold tax free and no authority controls workplace safety, workers rights, product quality, or managerial practices, including financing and subcontracting. The only

exception to this is money-laundering activities, as they are designed precisely to move drug profits from this unregulated space to the legitimate and regulated economy.

Interdictions and tactical deployments do impact the business environment of TCOs, as the definition of the problem that creates a market but rather in their role of a legal regime. Finding creative ways to break legal regimes is a key task of the TCO business model. For example, the interdiction to buy and sell cocaine creates the supply “problem” TCOs then solve. Likewise, a new technology deployed in the borderlands sends an innovation signal to deviant innovators to develop a smuggling countermeasure. Therefore, governmental action does not play the role of a regulatory regime but of a problem for which an innovative solution creates a market.

Finally, there is enough clandestine seed and venture capital in the system to fund deviant entrepreneurs of all sizes, from small research and development (R&D) projects to create prototypes of new smuggling technologies to the expensive private enforcement armies that fight to keep open the supply and distribution chains.

The result is a strategic environment where disruptive ideas rapidly become products or processes that are tested in the real world very fast, and success is easily imitated and iteratively improved. The path from clandestine innovation to deviant entrepreneurship is very short thanks to the removal of these four obstacles freeing the flow of information through this unobstructed pipeline.

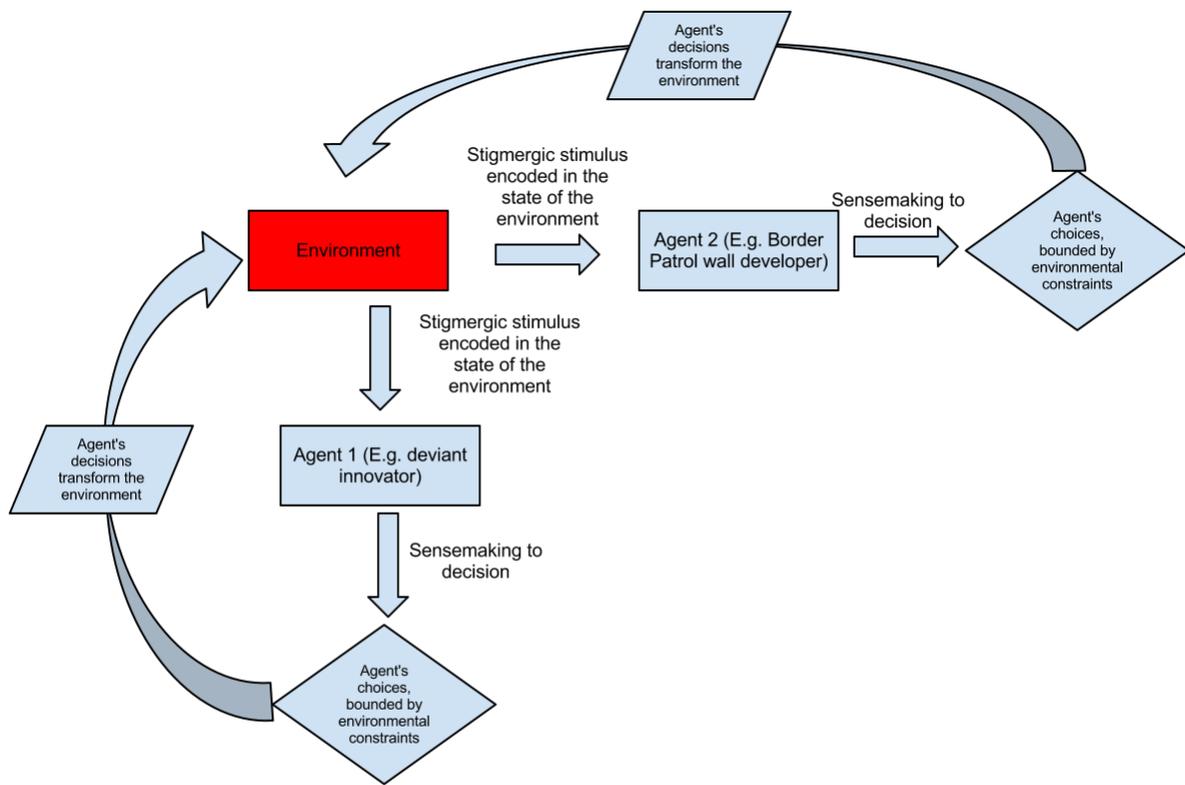
Most of this deviant innovation activities are directed to accomplish one specific task: to illicitly appropriate the technological backbone of globalization and penetrate the tactical technologies deployed by the governments of nation-states (Calvillo & Nieto-Gomez, 2010). This is done in order to perform what Gilman calls the “ultimate arbitrage activity, growing at the intersection of ethical difference and regulatory inefficiency” (2011, p. 3). That is, the product that for-profit TCOs commercialize is the arbitrage of a geopolitical spread between a morality based legislation and human desire, by innovating solutions to the challenges posed by technology based interdictions.

### **Hacking Interdictions: A High Risk, High Reward Innovative Business**

As the constant supply of illegal drugs into the U.S. has demonstrated over the last 20 years, TCOs are innovation patterns in time. These networks manage complexity and environmental change with success through a constant innovation process that iteratively solves the challenge of “hacking” governmental technologies, institutions, and deployments.

Walled fortifications and new surveillance, interdiction, and detection technologies have provoked an innovation/response cycle by the clandestine actors who are fighting to penetrate them. Each technology deployed in the borderlands or the interior of the national territories of the U.S. and Mexico sends a stigmergic signal to deviant entrepreneurs to improve their capacities and innovate a countermeasure to respond to the new shape of the system.

Stigmergy “captures the notion that an agent’s actions leave signs in the environment, signs that other agents sense and that determine their subsequent actions” (Parunak, 2005, p. 2). In situations with a stigmergic architecture, like the geopolitics of clandestine innovation, the agents in a system perceive the state of the environment and from that stimulus, they make their choices that transform that state, leaving in the process new signals for other agents to interpret, in an iterative process (Figure 14).



## Human stigmergy

Author: Rodrigo Nieto-Gomez.

Figure 14: Iterative Human Stigmergy Cycle

This stimulus/response cycle is at the center of the development of innovation of technologies used by TCOs to hack governmental interdictions. As Ted Lewis explains, stigmergy is “the product of individuals who work independently but are stimulated by the work they and others do...invention stimulates innovation, which leads to more invention, and so forth, in a never-ending cycle” (2011).

In Figure 14 a border technology developer and the deviant innovator that hacks that technology never interact directly with each other. Nevertheless, through the signals that each of them encode in geopolitical environments as part of their decision making process, they stigmergically influence each other’s actions.

Through stigmergy, a social dynamic that we do not fully understand emerges around the clandestine pipelines to solve in an iterative process one well defined problem: identify and exploit the vulnerabilities of a complicated but predictable enforcement architecture, building resilience to the clandestine supply chains as a consequence of these patterns. These social behaviors emerge because of the systemic forces that shape the environment in many counterintuitive ways, following a set of geopolitical rules that condition the risks and rewards for all the involved agents.

As the narcotics ethnographer Howard Campbell (2009) puts it, for deviant innovators

...the issue is avoidance trickery, evasion and “slantwise behavior,” that is actions that are undertaken by actors in order to achieve their own ends and that ... frustrate state interests... Simultaneously, for the narcotics agents it is an endless intelligence game: decoding the signs, symbols, and movements of ... nameless traffickers. (p. 12)

The behavior Campbell describes is exactly the same kind of behavior of most computing hackers that learn how to impose their will to a system designed to perform a different task (Norton, N.A.). On the other hand, those signs and symbols Campbell talks about are precisely the stigmergic stimuli that trigger the iterative responses of all the actors involved in this web of maneuvers and counter-maneuvers.

Many of the failures in the current strategies to confront the threat of TCOs can be attributed to an important lack of systemic understanding of the innovation dynamics these policies affect but do not comprehend. Stigmergy has produced a social environment in which criminal clusters in these deviant networks respond iteratively to very aggressive but fairly predictable sustaining innovations pushed into the system by state actors. As a consequence of this process, the global pipelines operating in the intersection between legal interdiction and human desire have continued to improve their innovation capacities.

Innovators see in the problems of today the big markets of tomorrow. For deviant innovators, solving the scarcity “problems” that interdictions provoke as certain products or services become illegal is akin to an innovation grand challenge that stimulates TCOs’ creative behaviors in such a way that they base a big part of their business model in solving those geopolitical challenges.

For example, the drug smuggling innovation challenge has very clear rules.

- The participating “teams” must optimize the transport of a series of interdicted chemical products to minimize risk, from a territory where they are cultivated and/or manufactured but have little market value, to another one where they are highly appreciated by a consumer market, avoiding the deadly predatory opposition of law enforcement agents, military and other adversarial forces (I.e. multiple competing TCOs).
- The “purse” for those who succeed is high. According to DEA estimates cited by the UNODC, the average street value of a gram of pure cocaine in 2009 in the US was \$176 dollars (UNODC, 2009, p.87) that is \$17,600 per kilo. One suitcase with 25 kilos (a normal allowance for international flights) of pure cocaine is worth \$440,000.
- The profitability of smuggling activities is dependent on the solidity of the interdiction to maintain that business model. An effective border fortification increases the incentives to penetrate it because the interdiction sustains the artificial scarcity of the smuggled product. The more the governmental response is effective, the more TCOs receive stigmergic stimuli to break it.

Punishment mechanisms are also well integrated into the geopolitical environment of TCOs. A deviant innovator using ineffective smuggling technologies or processes will rapidly be captured or killed. The effectiveness of deviant innovations is thus easy to evaluate. Continuing with the cocaine example, deviant entrepreneurs who do not manage risk in an effective way to transport those chemical products

from where they are abundant to where they are desired, provoke the arrest or death of the smuggling agent, removing the technique (and sometimes also the innovator) from the clandestine pipeline. That is, failed programs do not survive for too long in the way they do it in governmental environments where rewards and punishments follow a set of different rules.

Deviant innovators have one essential business requirement: to be one step ahead of the governmental deployment of interdiction technologies to remain a profitable operation that satisfies an artificially scarce human desire, while being ready to hack new inventions as soon as they are deployed. This hacking behavior can be observed in multiple contexts where deviant technologies are developed. For example, a deviant innovator who finds a method to counter the Digital Management Rights of the Xbox 360 can sell pirated video games, while another one who finds a way of manufacturing the newest leather pattern in vogue with enough fidelity to satisfy the consumer, can make and sell counterfeit Louis Vuitton handbags.

Of course, the most profitable and more critical of all the hacking behaviors of TCOs is to hack the tactical infrastructures and systems deployed at and around international points of entry to create and sustain profitable international smuggling routes. Hacking borders can be accomplished through multiple kinds of innovations, but the most common ones are: concealment technologies (e.g. modified cars or drugs in breast implants), smuggling in between points of entries (e.g. narco tunnels, ultra light aircrafts or catapults and pneumatic guns) or corruption schemes and other forms of social engineering (e.g. corrupt Border Patrol agents or American mayors or Mexican politicians, military or law enforcement).

Once a deviant technology is proven by a deviant innovator, others deviant entrepreneurs will adopt what innovation literature calls an "early followers" approach. Because there are no patents or property rights limiting the use of clandestine technologies, successful hacks rapidly propagate throughout the system until, at one point, governmental technologies close the gap, "patching" the vulnerability and outdating the deviant technology. However, normally by the time that governmental technologies have closed a particular exploit, deviant innovators have already been thinking about potential alternatives, and testing new methods for when the previous ones become legacy technology.

They do that not through a centrally planned strategy, but thanks to human stigmergy. Because of this, no agent has to be responsible of the whole "project" to keep the TCOs routes innovative, or know exactly about each governmental decision. Instead, the mechanisms of self-organization partially depend on the changes and signals encoded in the security landscapes and environments (geopolitical and social) of the borderlands. From indirect stimulus, clandestine agents innovate to survive.

Clandestine innovators who can make sense of this complex environment are constantly rewarded by the big profit margins of the drug business, while those who do not know how to exploit stigmergic information and innovate in a sustainable way, fail. Therefore, innovation is the key behavior that provides geopolitical resilience to TCOs, because the raw materials and resources TCOs use are easily replaceable before crossing the border. As the majority of the added value of drugs comes from their geographic location, innovation capacities are more important than other costs.

The borders of North America are the gateways that interconnect the American economy with the rest of the planet and represent big business opportunities that transnational corporations have exploited for the benefit of the U.S. economy. Because of globalization, the U.S.-Mexico border is the busiest

border in the world, and production and supply chains have developed multiple interdependencies between the two countries. But, the same innovation tools that have increased global commerce are available to deviant entrepreneurs as well. Current conditions in the international environment encourage the illicit appropriation of those same technologies by clandestine actors who innovate using those tools to research and develop immigration technologies to hack interdictions, and this includes the emergence of deviant porterian clusters and global knowledge pipelines, as previously described.

For example, thanks to that environment, a Mexican citizen can “pitch” an idea (an invention) to the right deviant Venture Capitalists (VCs) to improve the nature of submersibles to smuggle drugs from South America to Mexico. These VCs will be represented by a third party, so the entrepreneur is never in close contact with the person funding his research, and actually knows very little about the leadership structure of the TCO that is providing this first round of funding. With some “luck,” he will obtain the necessary money to do tests and build prototypes (the process can even receive a project name, “Project Neptune”) creating something akin to a deviant startup company. A FARC controlled territory in Colombia can then provide the porterian cluster where the deviant innovator finds subcontractors with the required mechanical and engineering skills to build the prototype, labor is cheap, offices as well as test labs are available and therefore the deviant startup can be incubated to produce an innovation that ultimately will be successfully adopted by contractors smuggling drugs for TCOs.

This is the story of Miguel Angel Montoya, one of the few documented cases in which a deviant entrepreneur has provided a detailed recount of how he mounted a deviant startup to build a new kind of fully submersibles for a TCO (Montoya, 2007). His experience is very similar to that of thousands of innovators that are attracted to clusters like Silicon Valley to take advantage of the geographic concentration of the necessary building blocks to build a new technology company. The only difference is that the problem he wanted to solve was not how to upload photos to Facebook more easily or how to build tablet computers, but instead how to make narco-submersibles undetectable from the vantage point of a Coast Guard or Navy helicopter.

While there is little information about the management of other innovation projects, it is known that this subcontracting model based on human stigmergy has played an important role in the emergence of many other smuggling and concealment technologies. For example, deviant innovations like ramps to climb security walls, catapults or pneumatic guns to shoot drugs across the border or the development of construction techniques to dig narco-tunnels, are all projects that emerged as a stigmergic response to environmental stimuli, conducted by deviant subcontractors who thought that they could solve the problem. What is not known is how that model operates, how much VC money is spent to develop innovations, the key actors in the innovation clusters, or how the networks of the global pipelines are really structured.

Understanding the forces behind the geopolitics of deviant innovation is essential to produce more effective strategies to counter the innovative capacities of TCOs. It is clear, for example, that the dominant idea of a centrally planned mafia coordinating every response to the deployment of governmental technologies is the wrong sensemaking model to understand the adaptation capacities of these clandestine organizations.

Instead, the complex system in which TCOs operate is more similar to the clusters and pipelines that fuel innovation of legitimate globalization, because deviant globalization uses the same tools. A lack of understanding of this funding and contracting and subcontracting model, for example,

The geopolitics of clandestine innovation are defined by the way in which deviant innovators monetize territorial conflict through invention, creativity and the illicit appropriation of the same engines that propel legal globalization. The clandestine supply chains are constantly challenged by governmental

interdiction, and changes in the security landscapes of North America produce the stimuli that fuel the stigmergic architecture of this deviant sociotechnical system. The main objective of security and defense policies to deal with the threat of TCOs should be to learn how to dismantle not a particular innovation or a particular subcontracting unit. Prioritized should be how to manage the wicked problem presented by the innovation capacities of TCOs. In order to do that, TCOs innovation and business models should be back engineered.

### Conclusion: Prepare for Obsolescence

At the seventh floor of the headquarters of the SEDENA (the Mexican Department of Defense) lays the “Museo del Enervante” or Museum of Drugs. Its access is restricted to members of the Armed Forces or special guests of the SEDENA and it serves as a didactical space to train the military personnel who will be involved in the so-called “war on drugs.”

The collection of this museum is formed by two different kinds of objects. One the one hand, the museum displays an important number of what could be described as the artifacts of the “narco-kitsch” culture that scaffolds the identity of drug dealers: Golden revolvers and AK-47s with engraved Mexican revolutionaries, belt buckles with marijuana leaves and diamonds incrustations, customized cowboy boots, and many other products like that. This shared culture plays an important role, reinforcing the identity of the members of the narco-global pipelines and clusters (Fugate, 2012), not unlike the innovation culture that with its own artifacts and fashions permeates Silicon Valley. On the other hand, the museum has an abundant collection of smuggling artifacts that have been confiscated during the multiple operations that the Mexican armed forces carry against TCOs, to be used to teach about smuggling techniques. A visitor of the museum may be tempted to observe the collection as a set of oddities: the artifacts of a never ending struggle against TCOs, collected by the SEDENA as the spoils of the war on drugs. Like in a zoo, the objects in museums invite us to observe them decontextualized from their environment. Observing this collection like that would be a mistake.

In reality, those objects expose some of the innovation capacities of TCOs, as well as some of the most powerful memes in deviant innovation sociotechnical systems. The objects in the museum of drugs form sets of evolving technologies and trace the stigmergic adaptation capacities of deviant innovators that respond to governmental stimulus by developing new tools to hack the interdictions in the geopolitical territories of the drug market.

Many of those technologies are now legacy technologies. For example, smuggling systems that cannot be used anymore as governments have adopted effective countermeasures. Nevertheless, the flow of drugs has not been interrupted by the obsolescence of those particular innovations, as many other technologies have taken their place.

Certain high tech companies are famous for outdating their own products before the competition does it. Some others resist change that challenges the status quo of past successes, creating the famous innovator’s dilemma where the same managerial decisions that produced success in the past, produce failure when environmental conditions change (Christensen, 1997).

Members of TCOs who fall victim of the innovator’s dilemma do not linger for too long in the sociotechnical system. This means that whenever a stigmergic signal is perceived by TCOs, they have to respond fast or they will be removed from the network. This encourages a very agile approach to

innovation, where multiple deviant “subcontractors” test ideas at the same time to solve new configurations of problems. Some work, some fail, but in general this approach builds resilience to the clandestine chains as the good ideas are propagated by the innovation pipelines and clusters, and the unsuccessful subcontractors are captured or killed when their approach fails.

On the other hand, governmental actors are constrained to follow a very regulated innovation path where previous policies and technologies are rewarded by the political environment in the form of continuing funding, renewal of contracts or promotion of successful individuals, independently of the real performance of those approaches, and high-risk ideas offer little reward to governmental entrepreneurs (Nieto-Gomez, 2011).

To counteract this harmful effect of the governmental architecture for innovation, a “contrarian technology perspective” (Vogel, 2013, p.48) should be encouraged in threat assessment processes when developing technologies to affect the geopolitical environment of deviant innovation. White hat hacking or red teaming are good examples of this contrarian perspective. Governmental developers must be allowed to constantly play the role of TCOs, penetrating governmental technologies.

Also, governmental technologies would benefit from following the obsolescence path, understanding that any particular technology is not an end in itself that will “solve” the TCO problem, but just one more link in the innovation chain that will probably be penetrated at one point.

Furthermore, technology developers and stakeholders should have a good understanding of the systemic forces interacting in the environment, as quite often the counterintuitive effect of some of the governmental technologies is to improve TCOs capabilities by unleashing disruptive innovation forces.

For governmental interventions in the geopolitical environments of TCOs to be successful, they should be “pivot friendly.” That is, policies should be designed in a way that whenever the environment changes, the shape of the governmental response can change with it. This means that instead of thinking about one particular innovation that must be neutralized, it is important to think at the scale of big technology trends, devaluing the importance of any individual adaptation in any threat assessment.

Finally, designing for obsolescence means designing for innovation and penetration. Governmental strategies should not ask the question “will this particular response be hacked?” but instead, “what to do when this particular response is hacked?” In this way, decision makers can avoid the trap of concentrating too much in one particular strategy or technology program, and instead encourage a contrarian technology perspective that looks for the right points of intervention to limit the geopolitical availability of deviant innovation clusters, and also fragments the systemic effectiveness of the pipelines that provide the creative resilience to TCOs.

# Chapter 11: Game-Changing Developments in the Proliferation of Small Arms and Light Weapons: Anonymizing Technologies and Additive Manufacturing

Dr. Regan Damron

[regan.w.damron.ctr@mail.mil](mailto:regan.w.damron.ctr@mail.mil)

USEUCOM, J2 Strategy Division – Deep Futures

This paper analyzes the contemporary tactics, techniques, and procedures (TT&Ps) associated with the manufacture and illicit distribution of SALW and how technological trends are likely to converge to augment and/or alter those practices.<sup>40</sup>

SALW are particularly nefarious in their potential to ignite, worsen, and prolong conflicts (SEESAC 2010, pp. 7-8). Additionally, SALW proliferate more easily and more often than larger, more complex conventional weapons systems because:

- Access to SALW is less strictly controlled;
- They are physically smaller and thus easier to transport/smuggle;
- Ammunition/ordnance for SALW is easier to come by; and
- They are within reach of many more end users because far fewer resources are required for their purchase, maintenance, and use (particularly if small quantities are desired).

Small Arms and Light Weapons (SALW) refers to weapons and ammunition of 100mm caliber and below. It thus includes such items as pistols, assault rifles, machine guns, mortars, man-portable surface-to-air missiles (MANPADS), shoulder-launched anti-tank rockets, conventional explosives, and detonators (SEESAC 2010, p. 7). Hereafter, the term “arms” refers to SALW.



Currently, relatively few, large-scale traffickers dominate the illicit distribution of SALW (Interview Damron and Henke, 2012). This is unlikely to change immediately, but two things may happen as existing trafficking networks are confronted with developments in anonymizing technologies. First, existing large-scale traffickers may capitalize on these technologies to minimize their risk by neutralizing existing vulnerabilities. They will use online anonymity in combination with anonymizable currencies to make it much more difficult for law enforcement to monitor and/or trace their communications and financial flows. Second, a “deep web” trafficking model may develop in parallel with this one as a result of these new anonymizing technologies (Wright, 2009).<sup>41</sup> This model capitalizes on the anonymized “deep web” environment to obfuscate arms sales and focuses on expanding the availability of SALW to individuals who may not have had the resources or the connections to procure such weapons before. These new consumers demand smaller quantities of arms that are typically delivered by shipping component parts separately to a variety of physical addresses, to be assembled by the end user(s).

<sup>40</sup> Herein I use the terms “illicit distribution” and “trafficking” interchangeably to refer inclusively to all processes associated with the proliferation of SALW once they are manufactured (e.g., brokering, diverting, smuggling, the forging of documents, etc.). The terms thus include both “gray market” (possibly legal, but either secret or unauthorized) and “black market” (wholly illicit) proliferation. For more information, see Krause, Keith. “Small Arms and Light Weapons: Proliferation Processes and Policy Options.” Canada Department of Foreign Affairs and International Trade, 2000.

<sup>41</sup> In fact, this has already occurred at an underground website called the *Armory*. The term “deep web” refers to World Wide Web content that is not indexed by standard search engines.

Looking deeper into the horizon, the maturation of desktop 3D printing (or “additive manufacturing”) technology is likely to completely revolutionize both the manufacture and the trafficking of SALW by eroding the economic foundations on which the business model of arms trafficking is currently built.

In order to examine these phenomena, this paper first examines mature anonymizing technologies (online anonymity and anonymizable currencies). The implications of these for SALW trafficking are discussed and recent developments in each are recounted. The paper then examines additive manufacturing (or “3D printing”) as a nascent technology that has the potential to change the contours of the landscape entirely. Potential signposts for which to watch as developments continue to unfold are then enumerated, and the paper concludes with a discussion of risks and opportunities from a U.S. DOD perspective.

### Online Anonymity: The Black Leather Gloves of the Internet Age

Online anonymity is the state of being untraceable in one’s online activities (Henke and Damron, 2012).<sup>42</sup> While there are several technologies that may be used in different combinations to achieve various levels of anonymity, this discussion focuses on a single, broadly available one in order to illustrate the concept: The Tor Project.<sup>43</sup>

Tor is a software implementation of “onion routing,” a technology that obscures the connection between the originating IP address (e.g., a user’s computer) and the destination of the network traffic (e.g., a website). Combined with widely available end-to-end network communications encryption,<sup>44</sup> Tor effectively allows a user to browse the Web without others being able to divine their identity (Syverson, 2013).<sup>45</sup>

Equally relevant, however, is the ability for websites to reside within the Tor network. Sites can have a “.onion” address that anonymizes the location (both virtual and physical) of the site itself. Such sites are viewable only from within a Tor-enabled browser (see Figure 15), which provides an additional layer of security.<sup>46</sup> These .onion sites constitute a very deep part of the so-called “deep web.” Interestingly, the “Use a New Identity” button changes one’s virtual IP address by changing proxies.

---

<sup>42</sup> This is the definition used in previous Deep Futures work; it is goal-oriented and thus includes technologies that function passively by creating a system with generic attributes as well as those that actively mask IP addresses, encrypt e-mail communications, and the like.

<sup>43</sup> This is an important point that should not escape the reader’s notice. No single technology is unassailable. What is most disturbing about Tor is its *accessibility* and its ability to be used in conjunction with other technologies to achieve higher levels of anonymity. TT&Ps exist for this sort of integration and are promulgated online. For these reasons, Tor has been chosen to serve as the archetype of an anonymizing technology in this study.

<sup>44</sup> The encryption protocols currently most commonly used for this are Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

<sup>45</sup> As with anonymizable currencies (discussed below), the anonymity for any single user increases as the number of users expands. Tor does indeed have various vulnerabilities, but they generally require a suspect to be targeted for analysis in advance and thus cannot be used to aid in the initial identification of target sets. The most practical approaches to exploit these vulnerabilities are “end-to-end correlation analysis” and “website fingerprinting.”

<sup>46</sup> These site addresses can also be changed by the owner at will. Because of this, the site operator can control access to the site by offering the address only to those who have certain characteristics (e.g., those who have exchanged Pretty Good Privacy (PGP) encryption certificates of a certain security level with the site operator—a virtual “secret handshake,” if you will).

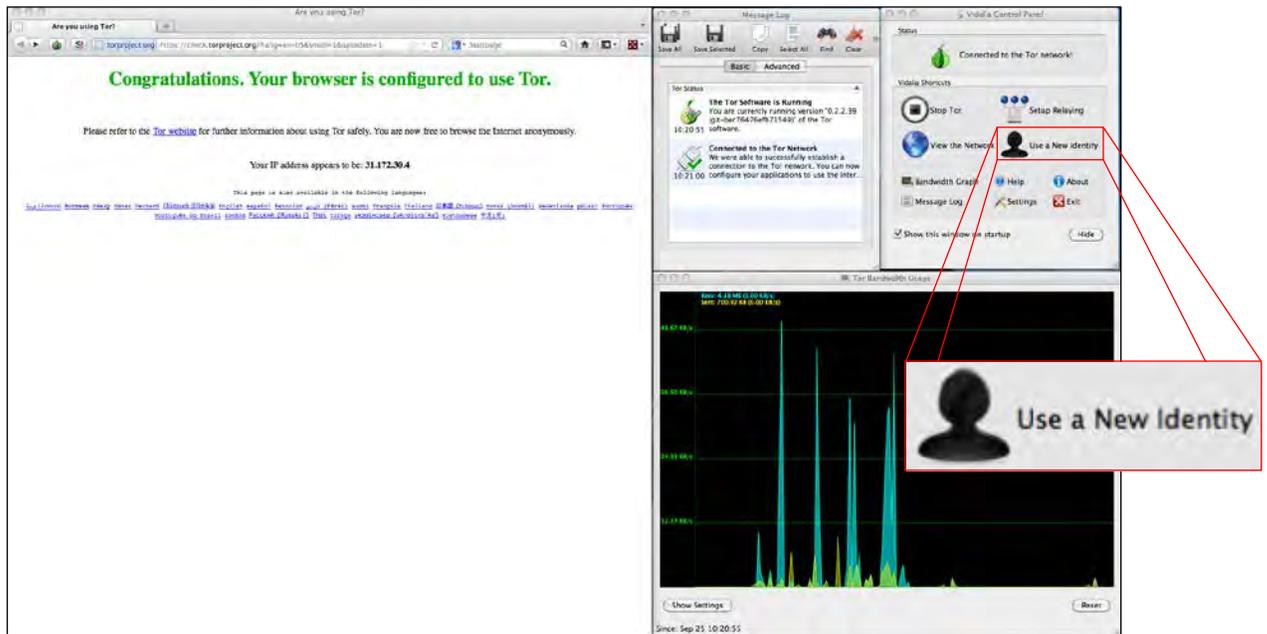


Figure 15: Tor Initial Configuration Screen, Control Panels, and Network Status Monitor<sup>47</sup>

The ability for websites to “live in” Tor is what makes the technology so game-changing with regard to SALW proliferation. This means not only that end-user solicitations for weapons (or drugs, hacking services, etc.) can be completely anonymous, but that the suppliers can be anonymous as well (and furthermore, each is anonymous with respect to—and thus protected from—the other). Add anonymizable currencies, discussed below, and even financial transactions between the two can be protected.

### Anonymizable Currencies: Out of Sight, Out of Mind

Anonymizable currencies are media of exchange that require no personal identification for use and whose networks can operate in near-complete isolation from the mainstream financial system.<sup>48</sup> They are “anonymizable” rather than “anonymous” because although their use alone does not guarantee anonymity, they are amenable to full anonymization if certain procedures are followed.<sup>49</sup> Bitcoin is a prominent example of such a currency and eCache is a lesser-known, gold-backed, and Tor-enabled variant (Keiser, 2011).

What makes these currencies disconcerting is the anonymity they afford to their users and they are potentially dangerous due to their broadening availability and acceptance. The larger the pool of users, the more difficult it is to discern illicit from licit transactions and to monitor and/or trace the former.

<sup>47</sup> This graphic was generated from a screen capture taken by the author from an Apple MacBook computer.

<sup>48</sup> This is the author’s definition. Full network isolation is not possible if one wishes to convert funds to and from a national currency for use; however, such intersections can be minimized. It should also be noted that cash could satisfy the first condition of this definition under certain conditions. It cannot satisfy the second, however, because its use and even its physical movement are regulated by the central authority that issues it (e.g., U.S. Customs and Border Protection reporting requirements governing the transport of cash across the U.S. border).

<sup>49</sup> One might expect that the conversion of funds into the currency (“placement,” in threat finance terminology) and the conversion of funds back into a national fiat currency (“extraction”) to be the points of greatest vulnerability, but even these steps can be anonymized. “How-to” tutorials for such procedures may be found on the Web; one need only troll the appropriate discussion threads. See <https://bitcointalk.org/index.php?topic=79288.0> for an example.

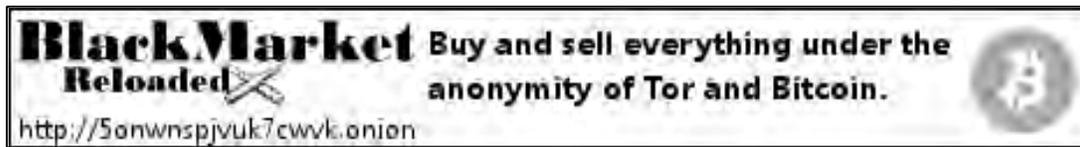


Figure 16: Black Market Reloaded Advertising Banner from the TorDir (Tor Directory) Homepage. Note the .onion address at the lower left and the Bitcoin logo at right

### Implications of Anonymizing Technologies for SALW Trafficking

Currently, the illicit distribution of SALW is dominated by relatively few, large-scale traffickers. This is unlikely to change in the near term (Interview by Damron and Henke, 2012). However, traffickers of SALW can benefit from online anonymity and anonymizable currencies by using them to reduce their vulnerability. Anonymity in the digital realm exerts its influence by effectively isolating the digital world from the physical one (or perhaps more precisely, one’s digital identity(ies) from one’s physical self).

The greatest points of vulnerability in any such system are the points at which the digital world intersects with the physical one because it is there that anonymity is jeopardized. In arms trafficking terms, these would be the points at which a person’s physical presence is required (where physical currency is exchanged for physical goods, for example) or where non-encrypted and/or traceable communications occur.<sup>50</sup> In threat finance terms, these would be the points at which the money is placed into or extracted from a laundering system (in this case, an anonymizable currency).

To the extent that communications, transactions, and delivery of goods and/or services can be fully executed within an anonymized system, then, vulnerabilities are limited. Using these technologies, only the delivery of physical goods (e.g., weapons) must be done outside the anonymized system. The current strategy employed by .onion sites like the Armory and Black Market Reloaded (see Figure 16) for minimizing the risks inherent in delivery is to ship the weapons’ component parts separately to a variety of physical addresses (P.O. boxes, generally) and have the end user(s) assemble the final product.<sup>51</sup>

Table 5: Effects of Anonymizing Technologies on SALW Trafficking

What Anonymizing Technologies Do	First-order Effect	Second-order Effect	Third-order Effect
Anonymize both acquisition and sale of SALW	Risk of engaging in illicit activity is reduced (makes trafficking safer)	SALW become more accessible	Potential market for SALW expands
Reduce time required for social network development/ penetration	Lead time required for weapons procurement is reduced (makes trafficking faster)		

<sup>50</sup> Additional points of intersection (and thus vulnerability) exist as well (e.g., a record of passwords to anonymous accounts may link a person’s physical identity with their anonymized online one, thus compromising anonymity), but these are beyond scope for present purposes.

<sup>51</sup> “...buyers get each gun component shipped in shielded packages—disguised to look like other products—that then require self-assembly. You get your gun, the dealer gets his money, The Armory retains its secrecy, and the mail carrier doesn’t realize it’s part of an international weapons smuggling operation” (Biddle, 2012).

As illustrated in Table 5, there are two higher-order effects of these anonymizing technologies. First, as a second order effect, they make weapons more accessible in Web-enabled societies through:

1. Reducing risks of exposure by anonymizing the processes of both acquisition (demand) and sales (supply); and
2. Making it easier for buyers and sellers to find one-another by lowering barriers to entry to the trust networks that regulate access.<sup>52</sup> Effectively, these technologies make it both quicker (because less time is required to cultivate contacts) and safer (due to anonymity) to sell and/or purchase weapons.

The third-order effect follows from the second, as increased access to weapons enlarges the potential market for them. As risk is reduced and the necessity to make “underworld” connections in the physical world declines, people who might not otherwise dedicate the time and resources to pursue weapons procurement are freed to do so.

This is not to suggest that people will suddenly begin to procure weapons simply because they become available to them; rather, it points out changes in the environment that can be permissive to those who wish to exploit them. This is the demand side of the equation.

Suppliers will see that there are potential revenues to be made in supplementing large-scale transfers by selling smaller quantities of arms. Economies of scale have historically been a key to profitability for traffickers due to the high risks involved in their work, and this fact drives them to deal in larger quantities. Dealing in smaller quantities becomes more viable as risk is reduced and the market expands.

It costs very little for traffickers to create and maintain an anonymous online presence (one’s own .onion site, listings on .onion sites such as the Armory or Black Market Reloaded, PGP-encrypted anonymous e-mail through Tormail, etc.), and this is all that is needed to make their wares available to those who would seek them out in that forum. Suppliers will recognize this fact and will appreciate the potential to reach new markets with very little additional cost or risk to themselves.

## Tradeoffs

The use of anonymizing technologies is not purely beneficial for traffickers. Online anonymity can make it more difficult to discern genuine traffickers (or buyers) from impostors even as it reduces the risk of engaging in illicit activities. Anonymizable currencies present similar verification hurdles to making transactions, since the money must change hands before the arms are shipped (or vice-versa). That is, it is difficult for the buyer to verify the quality of the arms and whether or not they have shipped prior to payment being made if anonymizable currencies are used, since payment is generally processed online at this time.<sup>53</sup> Finally, the values of anonymizable currencies can be unstable.

---

<sup>52</sup> While the first point about reduced risk is fairly intuitive, the second about trust networks may be less so. A high degree of person-to-person trust has historically been required to gain access to illicit networks, and this trust takes time to accrue. This is due mainly to the high risk of exposure that goes along with participation in illicit activity (even just knowing enough to buy from an illicit network (contact information, TT&Ps used to execute exchanges, etc.) means that the buyer has the potential to compromise at least part of that network). Any additions to the network thus have to be vetted. Anonymity affords protection to both parties of an illicit exchange while still allowing the exchange to take place because individuals can be uniquely identified in the virtual world while nothing of substance is known about their identities in the physical world. This reduction in risk means that a user can be “vetted” simply by demonstrating his/her use and knowledge of anonymizing technology. That is, the mere fact of being anonymized is enough to allow one to access a .onion site and participate in an economic exchange; to gain knowledge of a sort that could compromise either party, further trust would have to be developed. This likely affects law enforcement TT&Ps; exactly how it does so is an area for further research.

<sup>53</sup> See also Mack, Eric. “Are physical Bitcoins legal?” [http://news.cnet.com/8301-17938\\_105-20125470-1/are-physical-bitcoins-legal/](http://news.cnet.com/8301-17938_105-20125470-1/are-physical-bitcoins-legal/); and Caldwell, Mike. “Physical Bitcoins by Casascius” <https://www.casascius.com/>.

Strategies do exist to mitigate these concerns, however, and the marketplace continues to evolve. The infamous .onion drug trafficking site, Silk Road, and its sister arms trafficking site, the Armory, have dealt with these problems by allowing buyers and sellers to rate one-another to promote accountability through reputation, a strategy co-opted from such sites as Ebay.com and Amazon.com (Biddle, 2012). And those who deal in anonymizable currencies can minimize their exposure to value volatility by converting their capital into and out of the currency quickly (BitInstant, 2013).

### Recent Signposts for Anonymizing Technologies: Tor and Bitcoin

The anonymization space continues to evolve rapidly; the following are some significant developments that have occurred recently, including the following (Henke and Damron, 2012).

- Tor usage continues to grow (see Figure 17), and it has been ported to popular operating systems, including smartphones (The Tor Project, 2013).<sup>54</sup>
- “How-to” articles showing how to properly configure and use Tor in conjunction with other tools to achieve fuller online anonymity continue to proliferate on the Web (sudo-su, 2012).
- An analysis of *Silk Road*, a Tor-enabled anonymous marketplace specializing in the sale of controlled substances and narcotics, found that the site generated 1.9 million dollars per month in essentially untraceable revenue (Christian, 2012). A sister site for the trafficking of arms, the *Armory*, also existed at one time and may still (Koebler, 2012). Multi-purpose marketplaces such as *Black Market Reloaded* exist, as well, and deal in all manner of contraband.



Figure 17: Estimated Tor Average Daily Users Worldwide (The Tor Project, Metrics Portal, 2013)

Implications from anonymizable currencies, as represented by Bitcoin are listed below.

- The European Central Bank published a report examining the possible threats posed by digital currencies; roughly a quarter of the 55-page report is dedicated to Bitcoin (European Central Bank, 2012).
- Individual Iranians have discovered Bitcoin as a method for skirting sanctions; TT&Ps include using Bitcoin to purchase foreign currencies (e.g., U.S. dollar) for holding/investing outside the Iranian banking system (Raskin, 2012).
- A Bitcoin exchange has been allowed to operate legally within the European regulatory framework (Bitcoin-Central.Net, 2012).

<sup>54</sup> See also “Stronger Anonymity Comes to iPhone With Tor-Enabled App.”

<http://www.forbes.com/sites/andygreenberg/2011/11/18/stronger-anonymity-comes-to-the-iphone-with-tor-enabled-app/>.

- Bitcoin market capitalization (the number of Bitcoins in circulation multiplied by their exchange rate—against the U.S. dollar, in this case) has risen continuously over the past year (see Figure 18), reaching nearly \$180 million in circulation as of this writing.<sup>55</sup>

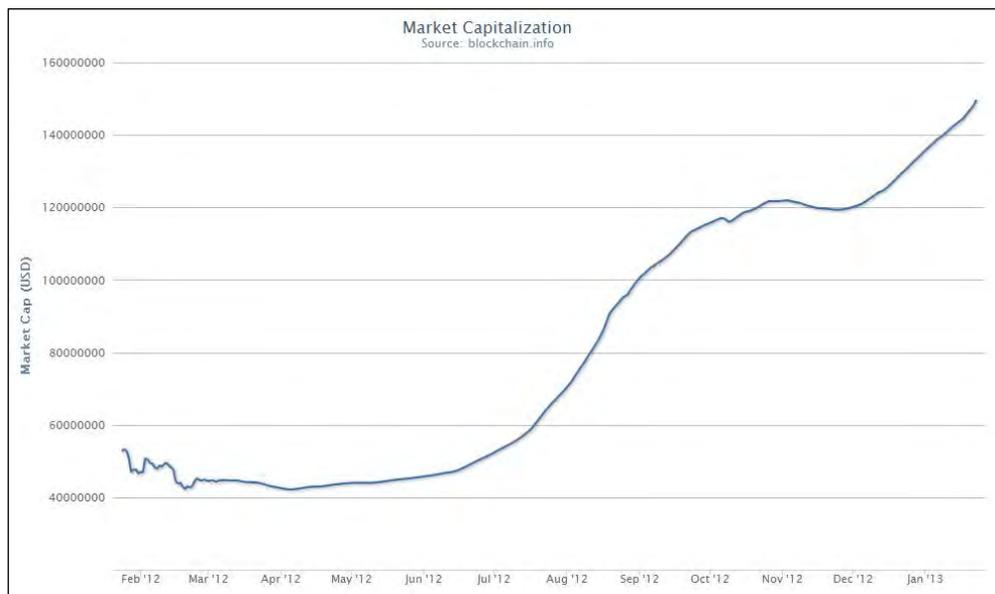


Figure 18: Bitcoin Market Capitalization: 50-day Moving Average (Blockchain.info, 2013)

Anonymizing technologies provide a cloak under which to engage in illicit activities by isolating the physical from the digital. As explained earlier, the physical movement of trafficked goods is the only link in the trafficking chain that must currently be executed outside of the anonymized system. As additive manufacturing technology matures, the distribution of physical goods is pulled into the digital realm, minimizing (if not eliminating) the vulnerabilities associated with the delivery of illicit goods.

### Additive Manufacturing: The Game-changer on the Horizon

Additive manufacturing, or “3D printing,” is a process by which a physical object is generated from a three-dimensional computer model (Oxford, 2012). Typically, the object is constructed by laying down many successive thin layers of material. Depending on the equipment used, materials can range from flexible plastic to high-tensile-strength metals such as titanium (Material, 2013).

This technology is still nascent, but it is rapidly developing and will have broad impacts as it matures and spreads.<sup>56</sup> Most significantly, it has the potential to not only supplement, but actually replace arms trafficking networks as a distribution system.

Currently, the weapons manufacturing potential of 3D printing is limited by the fact that desktop printers are unable to produce parts with sufficiently small manufacturing tolerances, high tensile strengths, and high ductility (low brittleness) to produce reliable firearms.<sup>57</sup> That said, it is important to

<sup>55</sup> The precise number as of January 22, 2013 is 177,435,740 USD according to <http://www.bitcoinwatch.com>. Note that this amount differs from the highest point in Figure 18, as the latter reports a 50-day moving average.

<sup>56</sup> See also National Intelligence Council’s Global Trends 2030 report: <http://www.dni.gov/nc/globaltrends>.

<sup>57</sup> The general consensus seems to be that common firearms manufacturing tolerances are at around 0.1 mm, which is approximately 20% more precise than the single-plastic 3D printers in Table 6. Brown (2012) quotes “Haveblue” (the pseudonym of the person who first printed and tested an AR-15 lower receiver) on the insufficiency of material tensile strengths. SAAMI (2012) lists actual ammunition pressures that support such

point out that home-use technology is already capable of printing of plastic “zip guns” that are undetectable by airport security (Dearon and Oliver, 2012). Only the proper designs are lacking, and plans are actively being tested and researched with private funding.<sup>58</sup>

Moreover, two of these three engineering challenges have already been overcome in industrial applications of 3D printing.<sup>59</sup> High-stress weapons parts such as barrels and bolts require materials that are hard, but not so brittle that the parts will fracture with repeated use. This brittleness (low ductility) remains an issue with current additive manufacturing processes and materials (Carlson, 2013).

That said, the reliability of fully-printable firearms will increase dramatically once current industrial-grade metal printing technology becomes economically viable for the desktop user.<sup>60</sup> In order to estimate when this might occur, Table 6 compares the lowest-priced current home-use 3D printer with an industrial model from just over a decade ago.

Table 7 then extrapolates based on this comparison and projects the cost decline of multi-material and metal 3D printing technology.

Table 6: Cost Decline of Additive Manufacturing Technology Since 2000 (Planes, 2012)

<b>Make and Model</b>	Stratasys Maxum	3D Systems Cube
<b>Introduced</b>	November 2000	January 2012
<b>Capability (Technology)</b>	Single-plastic (Fused Deposition Modeling)	Single-plastic (Fused Deposition Modeling)
<b>Cost</b>	\$312,600*	\$1,299
<b>Accuracy</b>	0.127 mm	0.125 mm
<b>Max Print Size</b>	600 x 500 x 600 mm	140 x 140 x 140 mm
<b>Machine Size</b>	6.5 feet tall, 2500 lbs	Desktop size, 9 lbs

\*Cost adjusted for inflation

---

claims. Gunsmith discussion threads such as kunkmeister (2013) and Unicorn (2013) give information on common manufacturing tolerances required for weapons manufacture.

<sup>58</sup> Defense Distributed is a group that is researching 3D-printable weapons with the stated goal of making the plans publicly available. See DefenseDistributed.com. “Our Plan.” Accessed January 18, 2013. <http://defensedistributed.com/proofgun-2/>. The group’s funding has been crowdsourced, predominantly in Bitcoin.

<sup>59</sup> Direct Metal Laser Sintering (DMLS—also known as Selective Laser Melting (SLM) or Laser Cusing), for example, is an industrial-grade 3D printing process that produces full-density metal parts that have properties very similar to those that are cast or machined. See GPI Prototype (2010) for a brief video primer. Also, NASA plans to use this technology to manufacture parts for rocket engines (Greenemeier, 2012). For more information, see International Powder Metallurgy Directory (2011).

<sup>60</sup> This enhanced reliability could extend the life of a fully-printed weapon from merely a few rounds (using a plastic weapon) to a few hundred rounds (using a metal one); the precise extent of the improvement achieved depends on how materials, methods of fabrication, and weapons designs co-evolve and cannot be known in advance.

Table 7: Projected Ten-year Cost Decline of Additive Manufacturing Technologies<sup>61</sup>

Capability (Technology)	Single-plastic (Fused Deposition Modeling)	Multi-material (PolyJet)	Metal Sintering (Direct Metal Laser Sintering)
Approximate Current Cost	\$2,000	\$45,000	\$600,000
Projected Cost in 10 Yrs	\$100 or less	\$500 or less	\$3,000 or less

As costs decline, 3D printing technology is likely to spread in much the same way as inkjet printers did throughout the late 1980s and the 1990s (Hopkinson, 2010). Once this happens, the technology will have much broader impact.<sup>62</sup>

Table 8 presents a proposed timeline for this and other milestones in the development and dissemination of 3D printing technology, as well as the consequences of these events for SALW proliferation. It focuses on the availability of 3D printing to the desktop end-user because this will be the most widespread application of the technology. The time frames and events in the table have been derived by cross-referencing information from a review of industry conference proceedings, investment reports, and news articles with the cost analysis underlying Table 5. The effects have been estimated by the author.

Additive manufacturing exerts its most significant effects via three major mechanisms:

- *Cost reduction:* The broader adoption of 3D printing technology into the home and office is made possible by reductions in its cost. This is true for both current single-plastic systems (see Table 8, Phase I) and industrial-grade metal printing (Phase II). Cost reduction also factors in on a per-unit basis to enable economies of scale later on (Phase IV).
- *Enablement of nonphysical distribution networks:* Distribution of physical goods will shift from physical (shipping/smuggling) to nonphysical (computer) networks, leading directly to a number of significant ramifications (Phases II and III). This will occur as 3D printing technology becomes more widely adopted (see previous bullet), software becomes more user-friendly, and open-source plans become freely available (not only for weapons, but for other items—imagine printing a single screw that is perfectly tailored to your application instead of driving to the hardware store to search for and buy a box of fifty; such convenience and efficiency gains will drive demand for the technology).
- *Extension to other materials:* As 3D printing is applied to other materials, more types of goods become digitally distributable. Printers are already being developed that can use chemical building blocks to generate pharmaceutical compounds (BBC, 2012) and cells to generate tissues and organs (Osborne, 2013; Thompson, 2012), for example. Explosive chemical compounds may be fully printable in the future, along with embedded electronics and optics (Phase V).

<sup>61</sup> Figures are based on a cost curve derived from the comparison presented in Table 7. For an overview of various 3D printing technologies, see Solid Concepts (2012).

<sup>62</sup> Few industry analysts doubt that 3D printers will become more common in the home as costs come down, but it remains to be seen whether there will be a move towards multi-material and metal 3D printing in the home or whether people will more commonly outsource their high-quality printing needs to on-demand service providers. Staples is now rolling out color 3D printing services in all its European stores in an effort to drive toward the latter, in fact (Bilton, 2012).

Table 8: Prospective Timeline for Developments in Additive Manufacturing Technology and Implications for SALW<sup>63</sup>

Time Frame	Prospective Event	First-order Effect	Second-order Effect
Phase I: 1-10 Yrs	Costs of single-plastic 3D printers fall; units are widely adopted into the home and workplace	Plastic “zip guns,” lethal at close range and undetectable by airport security systems, become easily and broadly accessible; ammunition remains detectable and must be smuggled	TTPs for use include killing armed personnel and taking their weapons, assassinations, etc.—functionality is akin to that of the WWII “Liberator” pistol <sup>64</sup>
	Defense Distributed (and/or similar groups) succeed in producing plans for a 3D-printable plastic “WikiWeapon”		
Phase II: 10-20 Yrs	Current industrial-grade 3D printing technologies become economically viable for home/office use and are widely adopted <sup>65</sup>	Tolerance and tensile strength issues are overcome for home/office users; material brittleness (low ductility) may remain an issue	Fully printable weapons become more reliable
		Distribution (trafficking) of low quantities of small arms begins to shift from physical to nonphysical networks	Conventional physical distribution of SALW is supplemented by digital distribution of low quantities of small arms It becomes possible to anonymize the distribution of low quantities of small arms
	Downloadable, printable plans for more reliable small arms become freely available	Trust networks become altogether obsolete as gatekeepers to small arms networks (for those who seek small quantities of these weapons)	Small arms become even more accessible; <sup>66</sup> anonymizing technology becomes unnecessary (assuming weapons plans remain legal), but still affords an extra measure of protection to seekers of arms who choose to use it
		Anonymizable currencies <sup>67</sup> become unnecessary (for those who seek low quantities of small arms) because weapons need not be purchased	
Phase III: 15-25 Yrs	Trends commenced in Phase II continue to mature (costs continue to fall, technology and materials co-evolve, and weapons plans proliferate)	Digital distribution becomes capable of fully replacing physical distribution of low quantities of small arms	Online anonymity <sup>68</sup> can cloak the entire proliferation process for low quantities of small arms (from solicitation to supply of plans to manufacture at or near local point of use)
Phase IV: 20-30 Yrs	3D printing achieves greater production speed/capacity and per-unit cost of production plummets	Even large-scale transfers of small arms can take place digitally because production of many weapons from a single plan becomes more economical	Large-scale trafficking is undermined as a business model; organized crime reacts to this
			Online anonymity can cloak the entire proliferation process for all transfers of small arms, regardless of scale
Phase V: 25-50 Yrs	Explosive chemical compounds, integrated electronics, and optics become printable in the home/office <sup>69</sup>	Ammunition and light ordnance, as well as light weapons such as RPGs, MANPADS, and IEDs become fully printable	SALW become fully accessible

<sup>63</sup> The analysis behind this table assumes that current trends continue unaltered by external factors (such as government regulation).

<sup>64</sup> The FP-45 Liberator was a cheap and crude .45 caliber pistol, intended to be air dropped into occupied German territory to enable resistance fighters to kill German soldiers at close range and take their weapons.

<sup>65</sup> Although the likelihood of home adoption of metal and multi-material 3D printing (the technologies that could be used to create more reliable weapons) is debated; certainly home use would be more troubling, since this would lead to the greatest availability of the technologies, but office use would also provide widespread access.

<sup>66</sup> Those who desire the full reliability of a mass-produced weapon may have to look to traditional traffickers at this point, depending on whether or not the material ductility issues have been overcome. But those who desire an essentially untraceable, yet accurate and serviceable firearm for use in a crime that would require a short weapon life span would be able to download and print one in this time frame regardless.

<sup>67</sup> For more information on anonymizable currencies (such as Bitcoin and eCache), see Damron and Henke (2013).

<sup>68</sup> For more information see Ibid. and Henke and Damron (2012).

<sup>69</sup> This prediction is admittedly rather speculative owing to the temporal distance involved (hence the width of the Phase V time span); still, it extrapolates based on observables, as foundational work is already being done in each of these areas. Examples of groundbreaking research in printable electronics and optics is described earlier in the “Recent Signposts” section, and regarding molecular (chemical) printing that may lead to printable explosives, see BBC (2012).

## Recent Signposts for Additive Manufacturing

3D printing technology can seem more like science fiction than science fact; if the projections in Table 8 seem unreasonable, consider the following:

- A group known as Defense Distributed is actively researching 3D printable weapons with the stated goal of making the plans freely available online.<sup>70</sup> Nearly 85 percent of their funding raised as of 27 September was contributed in the form of the anonymizable currency Bitcoin, and their founder presented at the 2012 Bitcoin conference in London (Hanrahan, 2012).
- Open-source weapons plans already exist and are continually being improved (see Figure 19); a user named “Haveblue” has printed and tested an AR-15 lower receiver (the core part of the weapon that is serialized at the point of manufacture and whose distribution is controlled) using .22 LR rounds (Haveblue.org, 2012) and Defense Distributed replicated that success on 25 December 2012 using .223 ammunition (YouTube.com, 2012).<sup>71</sup> Most recently, a user named “KneecapSniper” posted a video of himself firing a printed AR-15 lower with 5.45mm rounds, and claims that it will work with standard 5.56mm AR-15 ammunition (KneecapSniper, 2013).<sup>72</sup> And in direct response to California Senator Dianne Feinstein’s talk of banning high-capacity magazines in addition to assault weapons (Office of Senator Feinstein, 2013), Defense Distributed developed, tested, and made publicly available plans for a 3D-printed 30-round magazine for an AR-15 (defdist, DefDist Printed, 2013) (recently provocatively renamed the “Cuomo Mag” in honor of New York state Governor Andrew Cuomo and a 40-round magazine for an AK-47 (defdist, No Title) (reportedly to be named for Sen. Feinstein)<sup>73</sup> in just a few weeks.
  - The rapid development of these items illustrates the dark side of crowdsourcing.<sup>74</sup>
- When Thingiverse.com pulled all weapons-related plans from its website in the wake of the Newtown, CT (USA) elementary school shooting (Brown, 2012), the group Defense Distributed began to host them online to keep them freely available.<sup>75</sup>
- The RepRap project is an initiative to create an open-source, self-replicating 3D printer in an effort to democratize access to the technology.<sup>76</sup> Working AR-15 lower receivers have been printed on RepRap devices (KneecapSniper, 2013).
- Two brick-and-mortar 3D printing retail stores have opened, the first in Zurich in August 2012 and another in New York a month later (3D-Model.ch GmbH, 2012).
- The U.S. Army is currently working on a backpack-portable 3D printer for use in generating replacement parts in the field (Meyer, 2012) and already has a 3D printing lab in Southern Afghanistan that operates out of a 20-foot shipping container (Cox, 2012).

<sup>70</sup> See also: <http://defensedistributed.com/>

<sup>71</sup> December 25, 2012 is the date that the video was posted to YouTube. Also of note, the video had been viewed 18,876 times as of 2 January 2013, its notoriety no doubt owing to media coverage of 3D-printable weapons over the past few months.

<sup>72</sup> The user reasons that because the 5.45mm round has greater muzzle energy than the 5.56mm ammunition, the latter should function at least as well as the former in the 3D-printed lower receiver.

<sup>73</sup> This according to an exchange in the commentary on a Defense Distributed video posted on YouTube.com: “formatC2 (comment): I would have call it ‘The Feinsty Mag’... Great work!”; “DXLiberty (reply): Worry not. That honor is reserved for our printable AK mags” (formatC2, 2013).

<sup>74</sup> Rapid development through distributed “tinkering” with plans and materials is possible due to that fact that (1) no single individual must pay the costs associated with generating and testing all of the prototypes required and (2) digital plans for the parts are hosted centrally so that improvements made by one innovator can be vetted and rapidly propagated to others.

<sup>75</sup> The Defense Distributed file repository may now be found at <http://defcad.org/>.

<sup>76</sup> For more information, see the project’s website at <http://reprap.org/>.

- A much “lighter” version of the \$2.8 million Army lab is publicly available for about \$35,000 from a company called re:char.<sup>77</sup>
- There are indications that more sophisticated weapons may be “printable” in the future:
  - A 3D-printed UAV has been designed and flown at the University of Virginia; even the turbofan engine was printed.<sup>78</sup>
  - A 3D-printed UAV wing was produced containing electronics that were printed directly into the structure of the object.<sup>79</sup>
  - A conductive material has been developed that is compatible with single-plastic (desktop) 3D printers, enabling the embedding of sensors and rudimentary electronics for home users.<sup>80</sup>
  - The field of printable optics is in its infancy, but is already capable of producing light-conducting tubes embedded in objects, as well as lenses and sensors (Limer, 2012).



Figure 19: "Printing" and Testing of Assault Rifle Components on YouTube (Kneecap Sniper, 2012)

<sup>77</sup> The re:char website is worth quoting at length on this: “We envision a global network of shop-in-a-box factories operating as an API for hardware: when one new product, Instructable, or other project has been built and documented in a shop-in-a-box, all other shop-in-a-box factories are able to quickly create and improve upon the product. We will deploy hardware like software: a new version of a product is deployed via instantaneous changes to the CAD models, not new products shipped from around the world.” (rechar Inc., 2012)

<sup>78</sup> “To make a plastic turbofan engine to scale five years ago would have taken two years, at a cost of about \$250,000...But with 3-D printing we designed and built it in four months for about \$2,000” (Samarrai, 2012).

<sup>79</sup> The components printed were “a conformal sensor, antenna, and power and signal circuitry” (Optomec, 2013).

<sup>80</sup> It is unknown when the material will be publicly available, but the scholarly paper presenting it was published on November 21, 2012.

## Future Signposts for Additive Manufacturing for Which to Watch

Future developments in additive manufacturing are listed below.

- Legal battles over intellectual property concerns and how these conflict with 3D printing—anyone with a printable good and a micrometer (or better yet, a 3D scanner<sup>81</sup>) can generate the data necessary to create Computer-Aided Design (CAD) files;<sup>82</sup>
- Continuing cost reduction in 3D printing hardware and materials;
- Material properties and tolerances of 3D-printed metal components approaching those of legacy processes;
- Ongoing developments in the Defense Distributed and RepRap projects.
- More weapon designs specifically tailored to overcome 3D printing limitations (such as the reinforcing of the AR-15 lower receiver that was necessary to adapt it to plastics);
- Automated combinations of 3D printing and legacy fabrication methods/tools;
- Extension of the technology to other realms such as chemistry, biology, electronics, and optics;
- Government sponsorship of 3D printing technology via grant funding and/or tax/investment incentives;<sup>83</sup>
- Inclusion of references to printable weapons and open-source weapons plans in TCO/terrorist communications and/or public rhetoric.

## Risks and Opportunities

Members of TCOs now have a greater number of options at their disposal to conceal their identities and obfuscate their communications and financial flows. This certainly presents risks, but also ample opportunities for developing or adapting law enforcement TT&Ps to counter these emergent threats, as well as engaging allies to propagate training based upon them.

Cyber weapons already have all of the advantages that 3D printing affords physical objects including nonphysical distribution and low traceability and inability to attribute. Due to this, these goods (e.g., prepackaged software and “how-to” guidance) and services (e.g., hackers for hire) will increasingly be sold over “deep web” channels in exchange for alternative currencies.

Previous USEUCOM work has noted that online anonymity can be used in conjunction with social media to organize political protests and to generate “flash mobs” for a variety of purposes (Henke and Damron, Trends, 2012). Developments recounted in this paper make it possible for disaffected groups to

---

<sup>81</sup> For an example of one such device that retails for \$2,995 (as of this writing) and is particularly popular among engineers and enthusiasts, see <http://www.nextengine.com/>.

<sup>82</sup> An important caveat to this statement is that the “printable good” must not have complex internal geometry; the author is unaware of any small arms parts that are complex in this way, but some aerospace components may be. To clarify, generating objects with complex internal geometries that cannot be manufactured by other (reductive or casting) means is where 3D printers excel, but the CAD files necessary to generate such items would not be producible with a micrometer or current home-use 3D scanning technology (which uses line-of-sight laser scanning). That said, such capabilities are currently available to industry via non-invasive Computed Tomography (CT) 3D scanning (GKS Services Corp., 2013).

<sup>83</sup> For an example of this, see <http://biginnovationcentre.com/Publications/23/Three-Dimensional-Policy-Why-Britain-needs-a-policy-framework-for-3D>.

both organize *and arm* using the same “deep web” channels, presenting significant risks to social, political, and economic stability.

Overall, in fact, these technologies increase the potential for violent upheaval and instability because they empower greater numbers of individuals to engage in the trafficking of small quantities of SALW as both consumers and suppliers—effectively democratizing access to weapons. In addition, more readily accessible SALW lead to an increased potential for both “lone wolf” and organized extremist attacks. Were they to occur in sufficient numbers and/or magnitude, such attacks could lead to a more widespread desire for arms for defensive purposes.<sup>84</sup> As additive manufacturing technology matures and spreads, these concerns will become more acute.

Due to this trend towards greater opportunity for violence, there is a greater need for socio-cultural analysis (SCA) to understand and possibly address the macro-level factors that motivate individuals to engage in it. There is thus an opportunity for the Department of Defense to invest in expanding and extending SCA capabilities in order to facilitate the development of non-kinetic engagement options.

There are also opportunities to get out ahead of emerging trends. For example, metal additive manufacturing technology could be regulated via a number of different mechanisms due to its technical complexity.<sup>85</sup> Given the security and stability implications that accompany the technology, the DOD could be an early advocate to increase the saliency of these issues.

Early engagement with allies on legal issues, coordination, data access/sharing, and the like surrounding the technologies described herein is critical to enhancing monitoring and enforcement capabilities. These issues know no geographic or cultural boundaries.

Finally, arms trafficking is the third largest illicit trade globally, trailing only drugs and exotic species, and TCOs have benefited by trafficking in SALW (Kotler, 2013). As additive manufacturing technology matures, however, the scarcity of such goods and thus the economic imperative behind their illicit physical distribution will be increasingly undermined: “[TCOs’] near monopolies have allowed them to control the nearly 2 trillion dollar annualized trade in illicit goods. But what happens to their business model when guns, drugs and animals are democratized? How will they respond?” (Kotler, 2013) These are open questions whose answers will pose additional risks (and likely, opportunities).

---

<sup>84</sup> Lone wolf attacks are notoriously difficult to anticipate and prevent. The amount, type, and magnitude of such events that would be required to inspire such fear is unknown and would likely vary by country. For denizens to take up arms, many would have to feel threatened by possible violence and perceive the authorities as being unable to protect them.

<sup>85</sup> I point specifically to metal technology because (1) it is more troubling than plastic from a weapons fabrication standpoint and (2) efforts to regulate plastic technology would likely face more serious barriers (particularly in light of projects like RepRap, whose stated goal is to produce a self-replicating additive manufacturing device—see <http://reprap.org/>). Regulation (to include export control and/or tagging of materials using nanotechnology) of powdered metal 3D printing materials may be effective, as these require high-tech manufacturing of a sort that would be difficult to replicate in a non-industrial setting. This has to do with the level of precision required to manufacture such materials; at least with current techniques, metals must be manipulated to create spheres of a diameter less than or equal to the accuracy of the 3D printer (the printer can generate layers only as thin as the diameter of the metal spheres in the powder that it uses). For examples of such materials and their technical specifications, see 3T RPD Ltd. (2013). Regulation of specialized components (such as high-wattage lasers) that are required to fabricate high-end metal 3D printers could also be viable. Such parts could be listed as “dual-use” components on export control lists (if they are not already), and their manufacture and distribution could be monitored accordingly.

## Suggestions for Future Research

- “Signposts” could be monitored in order to indicate progression along hypothesized trajectories (or diversion from them).
- How might the ability of anonymizing technologies to separate virtual identity from physical identity relate to biometric analysis, which is predicated on physical identity and tracking the physical movement of persons?
- Is there a framework for analyzing alternative currencies from a security perspective? Might one be created if not?
- What motivates people to use (and/or abuse) emerging technologies more broadly? Could an understanding of these motivations aid in identifying non-kinetic engagement options?
- How will TCOs react when one of their major sources of revenue (trafficking in SALW) is undermined/eliminated as 3D printing matures? Will they proactively co-opt the technology somehow before this occurs?

## Chapter 12: Turning Technology's Tables on Trafficking: Building an Anti-Human Trafficking (AHT) Data Ecosystem

Maj David Blair

[Dave.Blair@post.harvard.edu](mailto:Dave.Blair@post.harvard.edu)

USAF, PhD Candidate, Georgetown University

### Project Abstract

Cyberspace is a key part of the business cycle of modern-day slavery. Traffickers use digital data directly, using major web arteries to find buyers and identify victims, and indirectly, like any small business, online banking and digital communications serve as key enablers. Simultaneously, cyberspace is key terrain for trafficking's enemies. Law enforcement and NGOs use the web to share data and collaborate. Traffickers have already targeted anti-trafficking websites, a trend likely to increase as more anti-trafficking work moves online. In order to counter this 'wicked problem,' state and Intergovernmental Organization (IGO) leadership needs to make cyberspace more secure for the anti-trafficking movement and far less secure for traffickers.

As to the former, the anti-human-trafficking (AHT) movement faces an endemic challenge in the inability to collaborate. The AHT movement has been plagued by data problems and unsynchronized (and even counter-productive) efforts. Cyberspace offers a solution—an online collaboration environment provides the movement both an Intranet and a Fusion Center, solving the coordination problem. Such an environment would be a target for hacking, and security is paramount.

Concerning the latter, traffickers find online collaboration far too easy. Their use of cyberspace is almost uncontested. By targeting and prosecuting the cyberspace elements of the trafficking business model, the legally sanctioned elements of the AHT movement make life far more difficult for traffickers. This induces friction, reduces profits, and ultimately protects victims by disrupting trafficking networks.

In short, the traffickers have a market, which serves as a massive data aggregator transmitting both prices and best practices to each other. The anti-trafficking movement has an anti-market, as structural incentives inherent in the struggle for grants and donors causes groups to view each other as competitors and hence hoard resources. It is unrealistic to expect significant impacts so long as the USG's anti-market is fighting the trafficker's market. However, Information technology and a shared data backbone can serve as a 'synthetic market' for the movement, allowing coordination amongst major players, and many more people to take part in the movement in meaningful ways.

### Key Elements

Rather than building one single network, the movement has many players with diverse needs; moreover, the expression of slavery varies from area to area. A network structure fluid enough to let organizations innovate from the bottom up, in response to local conditions needs to be built. This structure includes three elements: local 'Barricade Networks' connected by Dynamic Ontology and Nexus Peering on a Data Ecosystem for the movement.

During the later French Revolutions, people would throw whatever was on hand together into *ad hoc* defenses, where people would gather. These barricades were a physical manifestation of relation

networks; a “barricade network” is a modern version of the same principle. Social relationships, accelerated and amplified by information technology, provide focal points for the struggle against trafficking. A defensive structure made from whatever is on hand that allows normal people to protect whatever is behind it, seems in keeping with the best traditions of the movement. Rather than mandating a structure or a model, whatever is available is utilized. An information backbone should solve organizational problems, build a cyberspace layer atop the 'real space' relationships that already exist, make IT things easier for poorly resourced organizations, etc. These are then synchronized. This model makes it very easy to stand up new networks domestically and internationally. In practice, this looks like a local server under the supervision of coordinating bodies such as the BAATC in the Bay Area or Chab Dai in Cambodia. These Barricade Networks are the body of the secure online space.

Rather than one single network, which is at best inflexible, and in general unworkable given the diversity of the movement, a ‘**data ecosystem**’ is proposed. This is a compact between all major networks in the movement to structure data such that any data point can migrate from any system to any other system in the ecosystem. This allows organizations to share data points with one-click, which is key for time-critical situations and data sharing. This is brought about through IT partnerships amongst the major players in the movement, as well as by the grantors and donors, who place ‘data riders’ in their donations, which encourage data sharing and common standards. This is the backbone of the secure online space.

Developed by Palantir Technologies, **dynamic ontologies** overcome the classic data structure problems inherent in data sharing. Rather than making one central list of categories, by simply linking entities to each other, networks can ingest data and let the data define its own structure. Similarly, **Nexus Peering** allows a whole set of diverse networks to synchronize their data with each other rather than forcing a central network structure. These technologies provide the ligaments of the secure online space.

These three elements allow coordination and collaboration in local spaces, as well as global data sharing. The willingness to actually share data is more of an organizational problem, but if the structures are in place to allow data sharing, the benefits of shared situational awareness will trump this resistance over time, provided organizations observe **Data Reciprocity** (If an organization shares data, any benefit from the data needs to be shared with them.) The key to this structure is collaboration amongst players’ IT staffs, as well as convening authority (C/TIP, J/TIP, INTERPOL and major players in the movement can serve this role.)

## Key Roles

In order to synchronize the movement on this data ecosystem, four key roles must partner.

- **Benchmarking and Best Practices:** A data ecosystem can share best practices and enable collaboration. Both by examining organizational process and by enabling an Application Programming Interface, organizations can help each other by benchmarking what works and what does not, and passing on what works to other members. In this structure, the community would welcome new players to the movement with a ‘starter pack’ of web applications, information and contacts.
- **Time-Critical Data Routing:** As Polaris does admirably, this structure moves data rapidly to whoever needs it the most. In the most direct application, a time-critical tip would move to law enforcement in enough time to rescue a trafficking victim. In a more banal form, offers of

assistance, resources, and information would efficiently move into the ecosystem and to whatever partners could best use them.

- **Social Movement Support:** A study of history points to the critical need for social support for social justice campaigns. In 1849, the British Atlantic Slave Trade suppression campaign faced a crucial challenge. In a close-run parliamentary vote to pull the funding plug and in effect reinstate the slave trade, it seemed no progress was being made despite massive expenditures (Siân, 2011). This network must include access for social movement actors and civil society in order to maintain the long-term health of the campaign.
- **Big-Data Analytics:** With all data in compatible formats, insofar as players are willing to share information, all could then operate in a space of shared situational awareness. There is a tradeoff between resolution and access in this due to security, but law enforcement could maintain the highest-resolution, actionable picture, with vetted organizations using a medium-resolution and refresh version, and academics and advocates with a low-resolution, but accurate picture of known trafficking that poses no risk to sources.

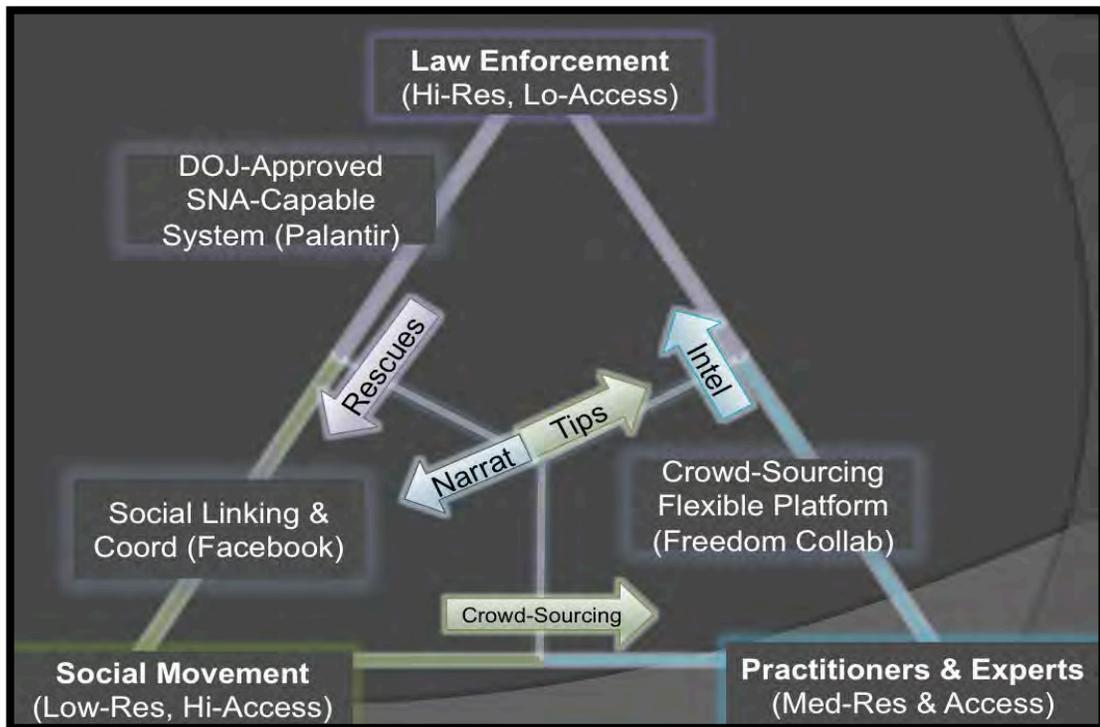


Figure 20: Three-Tiered Data Ecosystem

### Structure: Three Tiers Balancing Security vs. Access

In managing the fundamental tension between access and security, the first question is, “why?” In particular, what are the purposes and intents behind collaboration? Not all communities engaged in the AHT effort require the same degree of access or are capable of the same level of security, and many are simply doing different things with the same overall dataset. For instance, an academic or policy-maker may need only round number estimates by region, whereas a police department requires the specifics on sources and locations. Fortunately, the organizations that require the most specific data are usually the ones with the strongest security procedures. Variable resolution data resolves the security-access

tension— all organizations contribute to the same overall pool of data, and the precision of information they can draw from the shared pool varies according to their data handling standards. Any organization can draw low-fidelity scrubbed data (e.g., low refresh rates, round numbers) but organizations that wish to pull high-fidelity raw data need to undergo security vetting.

### High-Security Tier: The Data Fusion Network

The highest security tier connects law enforcement and national security professionals, cleared for access through a security benchmarking process. This would examine the full cycle of vulnerabilities, including social engineering and physical data processes. This network hosts potentially damaging information with court-admissible handling procedures, and is the only tier in the construct capable of doing so. Individual agencies may retain sources and method information at higher levels of security internally within their organization, but this network should be the primary avenue for state-level data storage and fusion regarding human trafficking.

The primary use of this tier is investigations and data fusion. This tier would also serve as a 'black box' for the lower-security tiers: all data gathered on victims, traffickers or current operations would reside on this tier, and lower resolution aggregated 'digest' versions of the dataset would be provided to the lower-security tiers daily (balanced tier) or monthly (high-access tier.) Players from lower security tiers would always still have access to any data they submitted to the database, and would have the right to submit a query request. Additionally, lower-security tier players can request IT assistance in the case of direct cyber attack or threats.

### Balanced Tier: Practitioner Collaboration Network

The second tier balances access and security in order to enable collaboration amongst practitioners. While the first tier is expected to be fully secure, the second tier recognizes that most field practitioner NGOs do not have the resources to achieve the rigorous prerequisite benchmarks for this. Realizing that most NGOs do not need the highest-fidelity data about trafficker networks, but can effectively collaborate with an accurate general picture of the problem, this tier relaxes the security requirement somewhat in order to include more players. The intention for this tier is for organizations to jointly develop regional strategies perform hand-offs (such as when an after-care organization gets a tip on victims still in captivity), and share best practices and lessons learned.

The expectation for data on this tier is that information would be brutally honest and potentially embarrassing to their host organization, such as internal processes and metrics, but not inherently dangerous. Accordingly, many organizations can be included in this collaboration, subject to a vetting process. The vetting process examines whether a group or an expert truly has equities in the anti-trafficking world, a legitimate need-to-know, and rudimentary security processes.<sup>86</sup> The security expectation of the middle tier is that no actual traffickers would be on the network itself, though due to possible corruption in national anti-trafficking task forces and unintentional security breaches from NGO coalition members, the risk of leaks must be mitigated by limiting network data resolution and hence potential damage. (If specific places, names and dates are not known, then reprisals are much more difficult.)

---

<sup>86</sup> The volunteer crowd-sourcing model described later could provide *pro bono* IT & cybersecurity assistance to organizations that should be on the network but could not meet basic security requirements.

In many ways, this is the most critical tier. The middle tier provides access for the vast majority of stakeholders in the movement, transforming the anti-market of the NGO scramble into a simulated market, where organizations lead by sharing the most effective processes and data. Moreover, this tier connects the vast amount of information collected from member NGOs to the top tier of robust analytics, and to the ‘Social Movement’ tier where it provides socio-political capital.

### High-Access Tier: Social Networking

Finally, the ‘Social Movement’ tier focuses on breadth of membership at the expense of security and resolution. This tier is openly available to all, and requires no vetting. It primarily layers on extant platforms such as Facebook and Twitter, along with an open web presence. There is not a formal architecture for this tier, but a commitment instead for organizations to connect their social networks together as a movement. Data shared with this tier should be fit for wide consumption, giving the public a sense of the scope and the span of the trafficking problem, as well as the effectiveness of different approaches to the problem. It should include datasets with round numbers, pooled regions and approximate dates. The purpose for this tier is awareness and recruiting.

Since this is an entirely open tier, all information is considered to be publically available and compromised. Therefore, information should be presented in a way that presents no danger to anyone involved. For instance, instead of street addresses, information aggregated by towns or regions in a resolution of months instead of days prevents traffickers from identifying any specific person for reprisals. However, since this tier is used for recruiting and generating tips, security is still a concern. Since this network tier layers on existing social networks, a number of trusted agents could provide informal vetting functions through recommendations.

This tier is key to maintaining the sustained social support for the movement. Since most NGOs already have strong web presences and social brand names, a compact between NGOs would be the best way to synchronize the various different communities that comprise the counter-trafficking movement. Such a compact would allow more accurate data sharing—instead of an order of magnitude difference in trafficking estimates, these conversations would likely cause the discourse to converge around common benchmarks. Additionally, it would begin to connect the disparate activist social networks involved on this issue, to the benefit of all. This compact would also enable shared community standards for future developments, such as crowd-sourcing routine office tasks.

### Percolation & Filtration: Migrating Data Up and Down

In order to maintain the integrity of the data ecosystem, these three tiers must be synchronized. This is especially important when aggregating the massive amounts of data held by disparate NGOs, primarily on the balanced tier. Due to the risk of data compromise, the highest-security tier maintains the master database. Tips from lower-security tiers and intelligence native to the high-security tier are both integrated in this database. Investigations are accordingly conducted only at the high-security network tier.

It remains critically important to build shared situational awareness with the lower-security tiers. This is done through ‘filtration,’ where data is regularly aggregated at the top tier into lower resolution digest forms for the lower tiers. The ‘Balanced’ tier would receive information refreshed weekly, with data aggregated by city precincts and numbers rounded to factors of ten, as appropriate. This level of information would provide an adequate basis for coordination and strategizing, and while consistent analysis of these digests could reveal AHT strategies, the loss of an individual digest is unlikely to cause a

catastrophic compromise. A monthly digest is produced for the open 'high-access' tier, aggregated by cities and rounded to thousands. This low-resolution picture provides a scope of the problem adequate for contextualizing research and focusing advocacy, but with little ability for traffickers to exploit for reprisals.

Conversely, when data moves uphill from the lower tiers to higher, it undergoes 'percolation.' This involves an analytical challenge and an organizational challenge. For the former, data must be contextualized if one is to make sense of it. Most tips arrive without effective context, and the process of routing and situating the data is time-intensive. Therefore, top-tier analysts set categories in standardized tip forms for the lower tiers in order to automate initial routing and enable efficient aggregation.

As to the latter, **information reciprocity** is key to maintaining the open flow of data from lower tier networks to higher networks. If there is no perceived benefit to providing tips, then these sources will dry up. The additional time and security risk involved with data sharing must be balanced with an equivalent benefit. Governments or donors might put a data-sharing mandate on grants, as Microsoft Research has already encouraged, but there must be organizational incentives as well (Microsoft, 2012). Therefore, any data provided from a tip will be tagged with the name of the contributing organization in the meta-data. When an investigation is successfully concluded, these tags will be aggregated from all information used. All organizations that contributed will be provided a storyboard, which they can in turn provide to their donors as evidence of their effectiveness.

### **Conclusion: Building Scaffolding and Foundations**

This proposed framework provides scaffolding for an entire range of cyber-enhanced capabilities. Cyber superiority, much like air superiority, is useful primarily for its ability to facilitate other enterprises. If the forces of modern abolition overpower the forces of modern slavery in cyberspace, tremendous advantages in coordination and analysis can be gained. Losing cyberspace hurts traffickers in two ways. First, an enormously effective coordinating mechanism that is presently integral to the supply chain is lost. Second, their adversaries in law enforcement and NGOs will be consistently faster and more adaptive than themselves. By the time that traffickers diffuse a counter-tactic, the police have already adapted. If the adversary network approaches a public official, they would find the transparency of free-flowing open data deters corruption. Winning cyberspace yields returns both in cyberspace and in real-space.

Such a data ecosystem brings the power for justice into homes and streets, rather than only in institutions. **Crisis Mapping** partners well with this structure, letting citizens use data as a floodlight to illuminate trafficker sanctuaries. **Crowd Sourcing** multiplies the effectiveness of social mobilization, by providing myriad skills to actors in the movement. With an effective foundation of data sharing, the networks mobilized to combat trafficking in persons would become more adaptive and innovative than the networks that propagate trafficking in persons.

## Appendix A: References

### Chapter 1A References

Counterinsurgency, financial weakness. (2006). *Field Manuel 3-24 , 1-100-101*.

Crime, U. N. (2005). *2005 World Drug Report*. United Nations.

Crime, U. N. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. New York: United Nations.

DEA. (2008). *Member of Afghan Taliban convicted in U.S. court on narco-terrorism and drug charges*. Press Release, DEA.

Defense, D. o. (1991). *National Defense Authorization Act for Fiscal Year 1991*.

Fridovich, L. G. (2009, March 11).

Peters, G. (2009). *Seeds of terror*. New York, New York: St. Martin's Press.

Publication, J. (2009). *Joint intelligence preparation of the operational environment*. June: Joint Publication 2-01.3.

### Chapter 1B References

AFP. (2012, January 1). *Mexico loses \$50 billion a year in illegal outflows: Report*. Retrieved from Univision Noticias: <http://wires.univision.com/english/article/2012-01-30/mexico-loses-50-billion-a>

Althaus, D. (2009, October). Mexico confronts a drug addiction epidemic. *Huston Chronicle* .

Clapper, J. R. (2012, January 31). *Unclassified statement for the record on the worldwide threat assessment of the U.S. intelligence community for the senate select committee on intelligence*. Retrieved from Director of National Intelligence: [http://www.dni.gov/testimonies/20120131\\_testimony\\_ata.pdf](http://www.dni.gov/testimonies/20120131_testimony_ata.pdf), accessed 31 Jan 12.

CNN. (2010, January 27). *Mullen: Debt is top national security threat*. Retrieved January 30, 2012, from CNN: [http://articles.cnn.com/2010-08-27/us/debt.security.mullen\\_1\\_pentagon-budget-national-debt-michael-mullen?\\_s=PM:US](http://articles.cnn.com/2010-08-27/us/debt.security.mullen_1_pentagon-budget-national-debt-michael-mullen?_s=PM:US)

Department of Defense. (2011). *Department of Defense counternarcotics and global threats strategy*. <https://www.hsdl.org/?view&did=721746>.

Department of Justice. (2011). *National drug threat assessment*. National drug intelligence center.

Department of Justice. (2011). *The economic impact of illicit drug use on American society*. National Drug Intelligence Center.

Director of National Intelligence. (2011). *The threat to U.S. national security posed by transnational organized crime*. [www.dni.gov/nic/NIC\\_toc.html](http://www.dni.gov/nic/NIC_toc.html).

Friedman, G. (2011). *The next decade-Where we've been...and where we're going*. New York, New York: Doubleday.

Homeland security council. (October 2007). *National strategy for homeland security*.

Horwitz, S. (2012, November 4). Mexican drug cartels establish networks in U.S. cities. *Washington Post* , p. 4.

Joint Warfighting Center. (2011). *Commander's handbook for attack the network (Version 1.0)*. Suffolk, VA: Joint Doctrine Support Division.

Keppel, S. (2012, October 4). 5 things you didn't know about the U.S.-Mexican relationship.

Kerlikowske, R. G. (2011). *A shared responsibility: Counternarcotics and citizen security in the Americas*. Subcommittee on Western Hemisphere, Peace Corps, and Global Narcotics Affairs. Senate Committee on Foreign Relations.

Malkin, E. (2012, January 10). With stake in stability, businesses in Mexico help city shaken by violence. *The New York Times* .

McCaffrey, B. R. (2011). *The hybrid threat: Crime, terrorism, and insurgency in Mexico*. Mexico: Drugs, crime, and the rule of law, U.S. Army War College Center for Strategic Leadership. George Washington University Homeland Security Policy Institute.

McCaffrey, B. R., & Scales, R. H. (2011, September). Texas border security: A strategic military assessment. *Colgen LP* .

McChrystal, S. A. (2011, March/April). It takes a network. *Foreign Policy* .  
[http://www.foreignpolicy.com/articles/2011/02/22/it\\_takes\\_a\\_network](http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network).

Miroff, N., & Booth, W. (2012, January 26). Security contractors see opportunities, and limits, in Mexico. *The Washington Post* .

Narconon international. (2012, January 31). *Mexico drug addiction treatment*. Retrieved from Narconon international: <http://www.narconon.org/drug-information/mexico-drug-addiction.html>

National Gang Intelligence Center. (2011). *National gang threat assessment--Emerging trends*.

Ngai, M. M. (2013, January 29). Reforming immigration for good. *The New York Times* .

Obama, B., & Harper, S. (2011, December). United States-Canada Beyond the Border: A shared vision for perimeter security and economic competitiveness, action plan.

O'Neil, S. (2012, November 25). Column: Mexico isn't a gangland gunbattle. *USA Today* .

Padgett, T. (2011, November 30). Mexico's Pena Nieto talks to TIME: 'We can move beyond the drug war'. *TIME* .

Reforma. (2012, November 20).

Rumelt, R. (2011, June). The perils of bad strategy. *McKinsey Quarterly* .

Southern Pulse. (2013, January 29). *Southern pulse networked intelligence*. Retrieved from Southern Pulse: [www.southernpulse.com](http://www.southernpulse.com)

The White House. (2011). *Executive order 13581: Blocking property of transnational criminal organization*. <http://www.whitehouse.gov/the-press-office/2011/07/25/executive-order-blocking-property-transnational-criminal-organizations>.

The White House. (2011, July 25). *Remarks at the White House release of strategy to combat transnational organized crime*. Retrieved from The White House: <http://www.whitehouse.gov/the-press-office/2011/07/25/remarks-white-house-release-strategy-combat-transnational-organized-crim>

United Nations Convention against Transnational Organized Crime. (2012, October 12). *Conference of the parties to the United Nations Convention against Transnational Organized Crime*. Retrieved from UN Office of Drugs and Crime: [http://www.unodc.org/documents/treaties/organized\\_crime/COP6/CTOC\\_COP\\_2012\\_CRP/CTOC\\_COP\\_2012\\_CRP5.pdf](http://www.unodc.org/documents/treaties/organized_crime/COP6/CTOC_COP_2012_CRP/CTOC_COP_2012_CRP5.pdf)

United States and Mexican Governments. (1998). *US/Mexico bi-national drug strategy*.

Vazquez, C. P. (2005). *The political constitution of the Mexican United States*. Instituto de Investigaciones Juridicas. Universidad Nacional Autonoma de Mexico.

Villagran, L. (2013, January 25). As Mexico's traffickers ship drugs north, they leave addicts in their wake. *The Christian Science Monitor*.

Wilson, C. E. (2011). *Working together--Economic ties between the United States and Mexico*. Mexico Institute. Woodrow Wilson International Center for Scholars.

#### Chapter 1C References

Department of Defense. (2012). DOD counternarcotics and global threats strategy.

Department of Justice. (2012). *National drug threat assessment 2011*. JIATF West Brief to the Interdiction Committee.

The White House. (2011, July 19). *Strategy to combat transnational organized crime*. Retrieved from [whitehouse.gov](http://www.whitehouse.gov)

United Nations Office on Drugs and Crime. (2012). *World drug report 2012*.

#### Chapter 1D References

Farah, D. (2012). Transnational organized crime, terrorism, and criminalized states in Latin America: An emergin tier-one national security priority. Strategic Studies Institute Monograph.

Killebrew, R. (n.d.). Criminal insurgency in the Americas. *Prism*, 2 (3).

Naim, M. (2005). *Illicit: How smugglers, traffickers and copycats are hijacking the global economy*. New York, New York: Anchor Books.

The White House. (2012). *National security strategy* .

## Chapter 1E References

Authier, A. A. (2013). A study of the military intelligence support to domestic law enforcement in counterdrug and counterterrorism operations. U.S. Army Command and Staff College.

Department of Justice. (2008). *Overview of the law enforcement strategy to combat international organized crime*. Department of Justice.

Department of Treasury. (2012). *Treasury designates key member of the brothers' circle criminal organization*. Department of Treasury.

Donadio, R. (2012, October 9). Italy: City government dissolved over possible mafia ties. *The New York Times* .

European Monitoring Centre for Drugs and Addiction. (2013, January). *EU drug markets report: A strategic analysis*. Retrieved from European Monitoring Centre for Drugs and Addiction: <http://www.emcdda.europa.eu/publications/joint-publications/drug-markets>

EUROPOL. (2011). *EUROPOL organized crime threat assessment*. EUROPOL.

FBI. (2013). *Italian organized crime*. U.S. Federal Bureau of Investigations.

Keefe, P. R. (1012, June 15). Cocaine incorporated. *New York Times Magazine* .

The Holland Times. (2012, October 12). *Drugs haul made near Rotterdam: Cocaine hidden in bananas*. Retrieved from The Holland Times: <http://www.thehollandtimes.nl/article/336/drugs-haul-made-near-rotterdam-cocaine-hidden-in-bananas%20%28accessed%2015%20February%202013%29%20%20Keefe,%20Patrick>

United Nations Office on Drugs and Crime. (2012). *Cocaine and heroin prices in Europe*. United Nations.

United Nations Office on Drugs and Crime. (2011). *The global Afghan opium trade: A threat assessment*. United Nations.

United Nations Office on Drugs and Crime. (2010). *The globalization of crime: A transnational threat assesment*. United Nations.

United Nations Office on Drugs and Crime. *The globalized illegal economy*. United Nations.

United States European Command. (n.d.). *JICTC: Joint interagency counter-trafficking center*. Retrieved February 15, 2013, from EUCOM: <http://www.eucom.mil/organization/command-structure/JICTC>

## Chapter 2 References

Brewer, J. (2011). Mexico Needs Tough Conspiracy Laws to Fight Organized Crime. *Mexidatainfo*.

Burns, L. E., Keefe, J. D., Kurtz, J. H., King, T. W., Simpkins, W. B., & Ploszaj, C. S. (December 2011). *Multijurisdictional, Interagency Operations Lessons Learned Project*. Alexandria, VA: Institute for Defense Analyses.

Code of Federal Regulations. (31 C.F.R. Parts 536 and 598). *Foreign Narcotics Kingpin Sanctions Regulations*.

Department of State. (11 March 2010). *Human Rights Report: Mexico*. Washington, DC: Department of State Bureau of Democracy, Human Rights, and Labor.

Franco, A. A. (20 April 2005). *Gangs and Crime in Latin America, Hearing before the Subcommittee on the Western Hemisphere of the Committee on International Relations*. Washington, DC: House of Representatives.

Maltz, D. S. (17 November 2011). *Narcoterrorism and the Long Reach of US Law Enforcement*. Statement before the Subcommittee on Terrorism, Nonproliferation, and Trade, Committee on Foreign Affairs, US House of Representatives.

Silver, M. (27 May 2010). *US-Mexico Security Cooperation: Next Steps for the Merida Initiative*. Testimony from Mariko Silver, Deputy Assistant Secretary for Policy, Office of International Affairs, Department of Homeland Security to a Joint Hearing before Committees on Homeland Security and Foreign Affairs, House of Representatives.

United States Code. (21 U.S.C. '1901-1908, 8 U.S.C. '1182). *Foreign Narcotics Kingpin Designation Act*.

US Agency for International Development. (August 2011). *Merida Pillar II: Rule of Law*. Washington, D.C.: US Agency for International Development.

White House. (21 October 1995). *Executive Order 12978, Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers*.

White House. (July 2011). *Strategy to Counter Transnational Organized Crime: Addressing Converging Threats to National Security*. Washington, DC: White House

### Chapter 3 References

Andreas, P. (2013). *Smuggler nation*. New York, New York: Oxford University Press.

Berdal, M., & Malone, D. (2000). *Greed and grievance: Economic agendas in civil wars*. Lynn Rienner.

Collier, P. (1999). *Doing well out of war*. The World Bank.

Fearon, J. (2004). Why do some civil wars last much longer than other? *Journal of Peace Reserach* , 41 (3), 275-301.

Olson, M. (1965). *The logic of collective action*. Cambridge: Harvard University Press.

The World Bank. (2011). *Crime and violence in Central America*.

United Nations Office on Drugs and Crime. (1998). *Economic and social consequences of drug abuse and illicit trafficking*.

Williams, P. (2008). *From the new middle ages to a new dark age: The decline of the state and U.S. strategy*. Strategic Studies Institute.

Zartman, W. (2005). *Rethinking the economics of war: The intersection of need, creed, and greed*. Washington DC: The Woodrow Wilson Center Press.

#### Chapter 4 References

Barabasi, A. L. (2003). *Linked: How everything is connected to everything else and what it means*. New York, NY: Plume Books.

Brewer, J. (2011). Mexico Needs Tough Conspiracy Laws to Fight Organized Crime. *Mexidatainfo* .

Burns, L. E., Keefe, J. D., Kurtz, J. H., King, T. W., Simpkins, W. B., & Ploszaj, C. S. (December 2011). *Multijurisdictional, Interagency Operations Lessons Learned Project*. Alexandria, VA: Institute for Defense Analyses.

Clarke, R., & Lee, S. (2008). The PIRA, D-Company, and the crime-terror nexus. *Terrorism and Political Violence* , 20 (3), 376-395.

Code of Federal Regulations. (31 C.F.R. Parts 536 and 598). *Foreign Narcotics Kingpin Sanctions Regulations*.

Department of State. (11 March 2010). *Human Rights Report: Mexico*. Washington, DC: Department of State Bureau of Democracy, Human Rights, and Labor.

Dishman, C. (2001). Terrorism, crime, and transformation. *Studies in Conflict and Terroris* , 24 (1), 43-58.

Franco, A. A. (20 April 2005). *Gangs and Crime in Latin America, Hearing before the Subcommittee on the Western Hemisphere of the Committee on International Relations*. Washington, DC: House of Representatives.

Freeman, L. C. (1977). A set of measures of centrality based on betweenness. *Sociometry* , 40 (1), 35-41.

Helfstein, S., & Wright, D. (2011). Covert or Convenient? Evolution of terror attack networks. *Journal of Conflict Resolution* , 55, 785-813.

Kenney, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, Government bureaucracis and competitive adaptation*. University Park, PA: Pennsylvania State University Press.

Killebrew, B., & Bernal, J. (2010). *Crime wars: Gangs, cartels, and U.S. National Security*. Center for a New American Security, Washington, DC.

Lowe, P. (2006). Counterfeiting: Links to organized crime and terrorist funding. *Journal of Financial Crime* , 13 (2), 255-257.

Makarenko, T. (2004). The crime-terror continuum: tracing the interplay between transnational organized crime and terrorism. *Global Crime* , 6 (1), 129-145.

Maltz, D. S. (17 November 2011). *Narcoterrorism and the Long Reach of US Law Enforcement*. Statement before the Subcommittee on Terrorism, Nonproliferation, and Trade, Committee on Foreign Affairs, US House of Representatives.

Moore, G. (1979). The structure of a national elite network. *American Sociological Review* , 44 (5), 673-692.

Naylor, R. (2002). *Wages of crime: Black markets, illegal finance, and the underworld economy*. Ithaca, NY: Cornell University Press.

Newman, M. (2005). Power laws, pareto distributions, and Zipf's Law. *Contemporary Physics* , 46, 323-351.

Picarelli, J. T., & Shelley, L. (2002). Methods not motive: Implications of the convergence of international organized crime and terrorism. *Police Practice and Research: An International Journal* , 3 (4), 305-318.

Rollins, J., & Wyler, L. S. (2010). *International terrorism and transnational crime: Security threats, U.S. policy, and considerations for Congress*. Congressional Research Service.

Rowley, T. J. (1998). Moving beyond dyadic ties: A network theory of stakeholder influences. *Academy of Management Review* , 22 (4), 887-910.

Sanderson, T. M. (2004). *Transnational organized crime: Blurring the Lines*. SAIS Review.

Shaw, M., & Kemp, W. (2012). *Spotting the spoilers: A guide to analyzing organized crime in fragile states*. International Peace Institute, New York.

Silver, M. (27 May 2010). *US-Mexico Security Cooperation: Next Steps for the Merida Initiative*. Department of Homeland Security to a Joint Hearing before Committees on Homeland Security and Foreign Affairs, House of Representatives.

Tichy, N. M., Tushman, M. L., & Fombrun, C. (1979). Social network analysis for organizations. *The Academy of Management Review* , 4 (4), 507-519.

United States Code. (21 U.S.C. '1901-1908, 8 U.S.C. '1182). *Foreign Narcotics Kingpin Designation Act*.

US Agency for International Development. (August 2011). *Merida Pillar II: Rule of Law*. Washington, D.C.: US Agency for International Development.

White House. (21 October 1995). *Executive Order 12978, Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers*.

White House. (July 2011). *Strategy to Counter Transnational Organized Crime: Addressing Converging Threats to National Security*. Washington, DC: White House.

Williams, P. (1998). Terrorism and organized crime: Convergence, nexus, or transformation. In G. Jervas, *Report on Terrorism* (pp. 69-92). Stockholm: Swedish Defence Research Establishment.

## Chapter 5 References

Kenney, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, Government bureaucracis and competitive adaptation*. University Park, PA: Pennsylvania State University Press.

Shaw, M., & Kemp, W. (2012). *Spotting the spoliters: A guide to analyzing organized crime in fragile states*. International Peace Institute, New York.

## Chapter 6 References

Al Arabiya News. (2013, January 26). Qaeda commander Belmokhtar claims mass-hostage taking in Algeria. *Al Arabiya News* .

Chrisafis, A., Borger, J., McCurry, J., & Macalister, T. (2013, Jauary 25). Algeria hostage crisis: The full story of the kidnapping in the desert. *The Guardian* .

FBI. (2010, September 15). *Manhattan U.S. attorney charges Long Island man with engaging in hawala activity that funded attempted Times Square bombing*. Retrieved from FBI: <http://www.fbi.gov/newyork/press-releases/2010/nyfo091510a.htm>

Financial Action Task Force (FATF). (2011). *Organised maritime piracy and related kidnapping for money*.

FinCen. (2007). *National money laundering strategy*. U.S. Interagency Money Laundering Threat Assessment.

Fleishman, J. (2013, January 21). Algeria hostage death toll rises to 37. *Los Angeles Times* .

Freeman, C. (2013, January 27). Revealed: How Saharan caravans of cocaine help to fund al-Qaeda in terrorists' North African domain. *The Telegraph* .

Hernandez, D. (2012, December 14). Fine in HSBC case equal to drug war aid to Mexico. *The Los Angeles Times* .

Kaplan, D. E. (2005, December 5). Paying for terror. *U.S. News and World Report* .

Keteyian, A. (2013, January 16). Mexican drug cartels fight turf battles in Chicago. *CBS Evening News* .

Markovic, V. (In Press). Drug trafficking. In J. Albanese, *The encyclopedia of criminology*. Hoboken, NJ: Wiley-Blackwell.

Markovic, V. Product counterfeiting operations of organized crime groups. In E. Shanty, *Organized crime: An international encyclopedia*. Santa Barbara, CA: ABC-CLIO.

Markovic, V. (2011). The nexus between terrorism and organized crime. In A. Duyan, & M. Kibaroglu, *Defence against terrorism*. NATO Peace and Security Series.

Markovic, V., & Ward, R. (2012). Terrorism and organized crime. In A. Duyan, *Defence against terrorism: Different dimensons and trends of an emerging threat*. NATO Science for Peace and Security Series.

Nanjappa, V. (2010, May 14). How Hawala money funds terror in India, abroad. *Rediff News* .

National Security Council. (2011). *Transnational organized crime: A growing threat to national and international security*. National Security Council Strategy to Combat Transnational Organized Crime.

Outlook India. (1997). *Dawood Inc.*

Raman, B. (2003). *Dawood Ibrahim: The global terroris*. South Asia Analysis Group.

Rollins, J., & Wyler, L. S. (2012). *Terrorism and transnational crime: Foreign policy issues for Congress*. Congressional Reserach Service.

The Times of India. (2008, December 18). Dawood directly involved in the Mumbai attack: Russia intelligence. *The Times of India* .

United Naitons Security Council. (2011). *Small Arms: Report of the Secretary General*.

United Nations Office on Drugs and Crime. (2012). *Global report on trafficking in persons*. New York: United Nations.

United States Coast Guard. (2008). *All hands messages: Update to accident inovloving CG-6505*. Department of Homeland Security.

USA Today. (2009, March 2008). Mexican cartels plague Atlanta. *USA Today* .

## Chapter 7 References

Ackerman, Gary A. *The Radiological and Nuclear Smuggling Threat Assessment Tool (RN-STAT): Development and Implementation*, College Park, MD, START, 2011.

i2 Group, *Whitepaper: Analyst's Notebook 8 Social Network Analysis*, Issue 3, June 2010

## Chapter 8 References

Abreau, C., Granato, S., & Winter, B. (2013). Counterintelligence Analyst Supervisor, Yakima Police Department; Chief of Police, Yakima Police Department; Lieutenant, Yakima County Sherrif's Departmetn. (M. Zalesny, Interviewer)

Hells' Angels (2009). Former Vice President; Individual now in federal witness protection program.

Bowden, M. (2002). *Killing Pablo: The hunt for the world's greatest outlaw*. New York, New York: Penguin Group.

Canadia Security Intelligence Service. (2000). *Transnational criminal activity: A global context*.

DeFeo, G. (2009, December 8). Chief Inspector, Special Advisor to the Chief of Police, Montreal Police Department.

Dowling, J., & Pfeffer, J. (1975). Organizational legitimacy: Social values and organizaitonal behavior. *The Pacific Sociological Review* , 8 (1), 122-136.

EUROPOL. (2008). *EU organised crime threat assessment*. EUROPOL.

Faiola, A. (2013, January 22). Sting operations reveal mafia involvement in renewable energy. *The Washington Post* .

Flanigan, S. T., & Abdel-Samad, M. (2013). Hezbollah's social jihad: Nonprofits as resistance organizations. *Middle East Policy Council* .

Gosselin, D. (n.d.). Detective Commander, Boston Police Department.

Lamar, W. (n.d.). President, Lamar Associates; Member, Blackfoot Tribe; Former FBI Agent.

Manwaring, M. G. (2007). *A contemporary challenge to state sovereignty: Gangs and other illicit transnational criminal organizations in Central America, El Salvador, Mexico, Jamaica and Brazil*. Carlisle: Strategic Studies Institute.

Marcella, G. (2009). *Democratic governance and the rule of law: Lessons from Colombia*. Carlisle: Strategic Studies Institute.

Margolis, S. (2009). Head, Organized Crime Unit, Los Angeles Police Department.

Maurer, J. G. (1971). *Readings in organizational theory: Open-systems approaches*. New York, NY: Random House.

Miller, P. (n.d.). Chief of Police, Ventura Police Department.

National Intelligence Council (2008, November). *Global Trends 2025: A transformed world*. NIC 2008-003, ISBN 978-0-16-081834-9.

National Intelligence Council (2012, December). *Global Trends 2030: Alternative worlds*. NIC 2012-001, ISBN 978-1-929667-21-5.

Reina, E., Delgado, J., Garcia, V., & Lopez, I. (2010). Director of Public Safety; Chief of Police, Tohono O'odham Nation Tribal Police; Tohono O'odham Nation Tribal Police; Vice Chairman, Tohono O'odham Nation.

Shaw, V. (2008). In a time of rapid social change: Organized crime in Asia and the Pacific. *International Journal of Social Inquiry*, 1 (1), 29-46.

Thomas, A., Sunday, T., & O'Neal, D. (n.d.). Chief of Police, St. Regis Mohawk Tribal Police; Lieutenant and Intelligence Officer, St. Regis Mohawk Tribal Police; U.S. Border Patrol, Nassena NY Station, previously stationed on SW US Border.

United Nations. (2004, December). *A more secure world: Our shared responsibility*. Report of the High-Level Panel on Threats, Challenges and Change.

United Nations Office on Drugs and Crime. (2012, October). *Digest of organized crime cases: A compilation of cases with commentaries and lessons learned*. Prepared in cooperation with The Government of Colombia, The Government of Italy, and INTERPOL. Publishing and Library Section, United Nations Office at Vienna, Austria.

U. S. Department of Justice, Office of Justice Programs. National Institute of Justice. (2004, November). Transnational Organized Crime.

Wells, M., Moniere, K., Leary, R., Lair, M., Poisson, R., & Zimmerman, J. (2009). Senior Investigator, NY State Police, NY State Intelligence Center (NYSIC); Department of Homeland Security Liaison Officer to NYSIC; NYSIC.

White House (2011). *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*. July, 2011.

Wikipedia. (2013). *Pablo Escobar*. Retrieved from Wikipedia: [en.wikipedia.org/wiki/Pablo\\_Escobar](http://en.wikipedia.org/wiki/Pablo_Escobar)

Williams, P. (2009). Director, Metropolitan Bureau of Investigation, Orange County, Florida.

Zalesny, M.D. and Numrich, S.K. (2011). *Net Wars on US Borders*. Report presented to Principal Deputy, Deputy Assistant Secretary of Defense, Rapid Fielding. January 20, 2011.

## Chapter 9 References

Andersen, M.E. (2011). A Roadmap for Beating Latin America's Transnational Criminal Organizations, *Joint Force Quarterly*. Retrieved from <http://www.ndu.edu/press/latin-america-transnational-criminal.html>

Assolini, F. (2012, October 1). The tale of one thousand and one DSL modems, *Secure List*. Retrieved from [http://www.securelist.com/en/blog/208193852/The\\_tale\\_of\\_one\\_thousand\\_and\\_one\\_DSL\\_modems](http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems)

Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5), 857-869. doi: 10.1016/j.chb.2010.03.013

Broadhurst, R., and Le, V.K. (2012). Transnational Organized Crime in East and South East Asia. In A. T. H. Tan (Ed.), *East and South-East Asia: International Relations and Security Perspectives*. London: Routledge International.

Choo, K.R.. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organized Crime*, 11, 270-295. doi: 10.1007/s12117-008-9038-9

Clark, J. (2012, August 17). Shamoon malware infects computers, steals data, then wipes them, *ZDNet News*. Retrieved from <http://www.zdnet.com/shamoon-malware-infects-computers-steals-data-then-wipes-them-7000002807/> The dangers of the Internet. Invisible Sieve. (2011, June 30). *The Economist*.

Dignan, L. (2012, August 9). Meet Gauss: The latest cyber-espionage tool, *ZDNet News*. Retrieved from <http://www.zdnet.com/meet-gauss-the-latest-cyber-espionage-tool-7000002405/>

Eccarius-Kelly, V. (2012). Surreptitious Lifelines: A Structural Analysis of the FARC and the PKK. *Terrorism and Political Violence*, 24(2), 235-258. doi: 10.1080/09546553.2011.651182

Farah, D. (2012). Fixers, Super Fixers and Shadow Facilitators: How Networks Connect *Convergence: Illicit Networks in the Age of Globalization*. Washington DC: National Defense University Press.

Farber, D. (2012, December 11). The Facebook vote and a nation-state in cyberspace, *CNET News*. Retrieved from [http://news.cnet.com/8301-1023\\_3-57558361-93/the-facebook-vote-and-a-nation-state-in-cyberspace/](http://news.cnet.com/8301-1023_3-57558361-93/the-facebook-vote-and-a-nation-state-in-cyberspace/)

Finnigan, G. C., Hanson-Smith, V., Stevens, T. H., & Thornton, J. W. (2012). Evolution of increased complexity in a molecular machine. *Nature*, 481(7381), 360-364. doi: 10.1038/nature10724

Gostev, A. (2012, December 18). Kaspersky Security Bulletin 2012. Cyber Weapons., *SecureList*. Retrieved from [http://www.securelist.com/en/analysis/204792257/Kaspersky\\_Security\\_Bulletin\\_2012\\_Cyber\\_Weapons](http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons)

GReAT, (Kaspersky Lab Expert). (2012, July 17). The Madi campaign - Part I, *SecureList*. Retrieved from [http://www.securelist.com/en/blog/208193677/The\\_Madi\\_Campaign\\_Part\\_I](http://www.securelist.com/en/blog/208193677/The_Madi_Campaign_Part_I)

Greenberg, A. (2012, October 19). DARPA-Funded Radio HackRF Aims To Be A \$300 Wireless Swiss Army Knife For Hackers. *Forbes*.

Holland, J. (1995). *Hidden Order*. New York: Helix Books.

Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. *Terrorism and Political Violence*, 24(2), 337-354. doi: 10.1080/09546553.2011.648350

Iran readies domestic Internet system, blocks Google. (2012, September 23). *Reuters News Service*. Retrieved from <http://www.reuters.com/article/2012/09/23/net-us-iran-internet-national-idUSBRE88M0AO20120923>

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *J Inf technol*, 25(2), 109-125. doi: 10.1057/jit.2010.6

Lee, T. B. (2012, July 5). How software-defined radio could revolutionize wireless, *ArsTechnica*. Retrieved from <http://arstechnica.com/tech-policy/2012/07/how-software-defined-radio-could-revolutionize-wireless/2/>

Longmire, S. (2011, September 6). The Mexican TCO threat has entered cyberspace, *Homeland Security Today*. Retrieved from [http://www.hstoday.us/index.php?id=483&cHash=081010&tx\\_ttnews%5Btt\\_news%5D=19169](http://www.hstoday.us/index.php?id=483&cHash=081010&tx_ttnews%5Btt_news%5D=19169)

OnlineTrustAlliance. BOTNETS. (January 8, 2013). <http://www.otalliance.org/resources/botnets/index.html>

Osborne, C. (2012, December 17). The 'Great Firewall of China' reinforced, prevents encryption, *ZDNet News*. Retrieved from <http://www.zdnet.com/the-great-firewall-of-china-reinforced-prevents-encryption-7000008883/>

Peterson, T. (2012, September 28). Rise of the Machines, on the Web: Bots account for 10% of U.S. traffic, says Solve Media, *AdWeek Technology News*. Retrieved from <http://www.adweek.com/news/technology/rise-machines-web-144044>

Phneah, E. (2013, January 3). Japan ministry information reportedly stolen in cyberattack, *ZDNet News*. Retrieved from <http://www.zdnet.com/japan-ministry-information-reportedly-stolen-in-cyberattack-7000009323/>

Picarelli, J. T. (2012). Osama bin Corleone? Vito the Jackal? Framing Threat Convergence Through an Examination of Transnational Organized Crime and International Terrorism. *Terrorism and Political Violence*, 24(2), 180-198.

Protalinski, E (2012, August 1). Facebook: 8.7 percent of users are fake, *CNET News*. Retrieved from [http://news.cnet.com/8301-1023\\_3-57484991-93/facebook-8.7-percent-are-fake-users/](http://news.cnet.com/8301-1023_3-57484991-93/facebook-8.7-percent-are-fake-users/)

Qing, L.Y. (2012, December 20). 3 in 5 pirated software in Southeast Asia malware-ridden, *ZDNet News*. Retrieved from <http://www.zdnet.com/3-in-5-pirated-software-in-southeast-asia-malware-ridden-7000009052/>

Rasmussen, S. (2012). News as a Service: Thirteen Danish Online Newspapers Adapting to the Social Web (pp. 1-22): IGI Global.

Roberts, P. F. (2012, December 27). Mr. Mitnick, I presume? Africa's coming cyber crime epidemic, *IT World*. Retrieved from <http://www.itworld.com/security/331276/mr-mitnick-i-presume-africas-coming-cyber-crime-epidemic>

Semantec. (2012, July 18). The Madi Attacks: Series of Social Engineering Campaigns, *Semantec Security Response*. Retrieved from <http://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns>

Sharma, D. (2013). Growing overlap between terrorism and organized crime in India: A case study. *Security Journal*, 26(1), 60-79. doi: 10.1057/sj.2011.33

Tarakanov, D. (2012, September 11). Shamoon The Wiper: further details (Part II), *SecureList*. Retrieved from [http://www.securelist.com/en/blog/208193834/Shamoon\\_The\\_Wiper\\_further\\_details\\_Part\\_II](http://www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II)

Weissenstein, M. (2011, December 27). <http://news.yahoo.com/mexicos-cartels-build-own-national-radio-system-200251816.html>, *Associated Press*. Retrieved from <http://news.yahoo.com/mexicos-cartels-build-own-national-radio-system-200251816.html>

## Chapter 10 References

Astorga, L. (2004). Géopolitique des drogues au Mexique. *Hérodote*, (1), 49-65.

Christensen, C. M. (1997). *The innovator's dilemma: when new technologies cause great firms to fail*. Harvard Business Press.

Goddard, B.T. (2012) *How to fix a broken border: disrupting smuggling at its source. Part II of III*. Immigration Policy Center.

Calvillo, E., & Nieto-Gómez, R. (2010). The Case of "Illicit Appropriation" in the Use of Technology. *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives*. IGI Global

Campbell, H. (2009). *Drug war zone: Frontline dispatches from the streets of El Paso and Juarez*. University of Texas Press.

Fitjar, R. D., & Rodríguez-Pose, A. (2011). When Local Interaction does not Suffice: Sources of firm innovation in urban Norway.

Fugate, A. (2012). *Narcocultura: a threat to Mexican National Security? (Master's thesis)*. Naval Postgraduate School, Monterey, CA

Gilman, Goldhammer, J., & Weber, S. (2011). *Deviant globalization: black market economy in the 21st century*. Continuum.

Lewis, Ted. (2011). *Bak's Sand Pile: Strategies for a Catastrophic World*. Agile Press.

Montoya, Miguel Angel (2007) *Ayer médico, hoy narco: el mexicano que quiso ser Pablo Escobar*. Editorial Oveja Negra.

Nieto-Gómez, R. (2011). The Power of "the Few": A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment. *Homeland Security Affairs*, VII.

Norton, Quinn (N.A.) *The next humans: Body hacking and human enhancement*.

Parunak, H. (2005). *Expert assessment of human-human stigmergy*. Defence Research and Development Canada

Porter, M. E. (1998). *Clusters and the new economics of competition* (Vol. 76, pp. 77-90). Boston: Harvard Business Review.

UNODC. (2009). *World Drug Report 2009, Cocaine*.

Retrieved from <http://www.unodc.org/documents/data-and-analysis/tocta/4.Cocaine.pdf>

Vogel, K. M. (2013). Intelligent assessment: Putting emerging biotechnology threats in context. *Bulletin of the Atomic Scientists*, 69(1), 43-52.

Wadhwa, Vivek, [washingtonpost.com](http://www.washingtonpost.com). "Industry clusters: The modern day snake oil" 14 July 2011

## Chapter 11 References

3D-Model.ch GmbH. "Grand Opening - Erster 3D Concept Store in der Schweiz." August 24, 2012. Accessed October 12, 2012. <http://www.3d-model.ch/2012/08/08/grand-opening-erster-3d-concept-stote-in-der-schweiz/>

3T RPD Ltd. "DMLS Material Specifications." Accessed February 6, 2013. <http://www.3trpd.co.uk/dmls/dmls-materials.htm>.

Biddle, S. "The Secret Online Weapons Store That'll Sell Anyone Anything." Gizmodo.com, July 19, 2012.

Bilton, R. "Staples introduces in-store 3D printing (but only in Europe)." VentureBeat (VB) News, November 29, 2012. Accessed December 10, 2013. <http://venturebeat.com/2012/11/29/staples-in-store-3d-printing/>.

Bitcoin-Central.net. "Important informations [sic] regarding our partnership with Aqoba," December 8, 2012. Accessed December 24, 2012. <https://www.bitcoin-central.net/s/aqoba-partnership>.

BitInstant LLC. "About BitInstant." Accessed January 17, 2013. <https://www.bitinstant.com/>.

Blockchain.info. "Bitcoin Market Capitalization." Accessed January 22, 2013. [http://blockchain.info/charts/market-cap?timespan=1year&showDataPoints=false&daysAverageString=50&show\\_header=true&scale=0](http://blockchain.info/charts/market-cap?timespan=1year&showDataPoints=false&daysAverageString=50&show_header=true&scale=0).

British Broadcasting Corporation. "3D printers could create customised drugs on demand." BBC News Technology, April 18, 2012. Accessed January 29, 2013. <http://www.bbc.com/news/technology-17760085>.

Brown, R. "MakerBot pulls 3D printable gun parts from Thingiverse." CBS News Online, December 20, 2012. Accessed January 10, 2013. [http://www.cbsnews.com/8301-205\\_162-57560237/makerbot-pulls-3d-printable-gun-parts-from-thingiverse/](http://www.cbsnews.com/8301-205_162-57560237/makerbot-pulls-3d-printable-gun-parts-from-thingiverse/).

Brown, R. "You Don't Bring a 3D Printer to a Gun Fight—Yet." C|net News, September 6, 2012. Accessed October 11, 2012. [http://news.cnet.com/8301-11386\\_3-57499326-76/you-dont-bring-a-3d-printer-to-a-gun-fight-yet/](http://news.cnet.com/8301-11386_3-57499326-76/you-dont-bring-a-3d-printer-to-a-gun-fight-yet/)

Caldwell, M. "Physical Bitcoins by Casascius." Accessed January 17, 2013. <https://www.casascius.com/>.

LTC Carlson, Lonnie. Ph.D., materials engineering. Interview by Regan Damron. February 25, 2013.

Christin, N. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace." Carnegie Mellon University: Carnegie Mellon INI/CyLab Working Paper, 2012.

Cox, M. "Mobile Labs Build On-the-Spot Combat Solutions." Military.com News, August 17, 2012. Accessed December 19, 2012. <http://www.military.com/daily-news/2012/08/17/mobile-labs-build-on-the-spot-combat-solutions.html>.

Dearen, J. and Oliver, J. "Click, Print, Shoot: Downloadable Guns Possible." The Age Online, December 26, 2012. Accessed January 4, 2013. <http://www.theage.com.au/technology/technology-news/click-print-shoot-downloadable-guns-possible-20121226-2bvn5.html>.

defdist (pseudonym). "DefDist Printed AR Mag – Part II." WikiWep DevBlog, January 12, 2013 (approx.). Accessed February 7, 2013. <http://defdist.tumblr.com/post/40395998801/defdist-printed-ar-mag-part-ii>.

defdist (pseudonym). [No Title]. WikiWep DevBlog, February 2, 2013 (approx.). Accessed February 7, 2013. <http://defdist.tumblr.com/post/42144739147/full-redesign-of-the-30-round-ar-mag-body-and>;

DefenseDistributed.com. "Our Plan." Accessed January 18, 2013. <http://defensedistributed.com/proofgun-2/>.

DXLiberty (pseudonym), "DefDist Printed Cuomo Mag - Part I." YouTube.com, February 2, 2013. Accessed February 7, 2013. <http://www.youtube.com/watch?v=JyYSqBA9BKw>.

DXLiberty (pseudonym). "DefDist Printed AR Lower – Part II." YouTube.com, December 25, 2012. Accessed January 8, 2013. <http://www.youtube.com/watch?v=RFhIxy5AXM>.

European Central Bank. "Virtual Currency Schemes," October 2012. Accessed November 13, 2012. <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

formatC2 (pseudonym). February 3, 2013. Comment on DXLiberty (pseudonym), "DefDist Printed Cuomo Mag - Part I." YouTube.com, February 2, 2013. Accessed February 7, 2013. <http://www.youtube.com/watch?v=JyYSqBA9BKw>.

GKS Services Corp. "GKS Expands 3D Scanning Capabilities of Internal Geometries with CT Scanning." Laser Design, Inc., 2013. Accessed February 20, 2013. [http://www.gks.com/services/ct\\_scanning/project\\_news/286/](http://www.gks.com/services/ct_scanning/project_news/286/).

GPI Prototype. "Direct Metal Laser Sintering - DMLS - By GPI Prototype." YouTube.com, February 27, 2010. Accessed November 16, 2012. <http://www.youtube.com/watch?v=88BPml8cGAo>.

Greenberg, A. "Stronger Anonymity Comes to iPhone With Tor-Enabled App." Forbes.com, November 18, 2011. Accessed September 4, 2012. <http://www.forbes.com/sites/andygreenberg/2011/11/18/stronger-anonymity-comes-to-the-iphone-with-tor-enabled-app/>.

Greenemeier, L. "NASA Plans for 3-D Printing Rocket Engine Parts Could Boost Larger Manufacturing Trend [Video]." Scientific American, November 9, 2012. Accessed November 15, 2012. [http://www.scientificamerican.com/article.cfm?id=nasa-3-d-printing-sls-rocket-engine&WT.mc\\_id=SA\\_CAT\\_TECH\\_20121113](http://www.scientificamerican.com/article.cfm?id=nasa-3-d-printing-sls-rocket-engine&WT.mc_id=SA_CAT_TECH_20121113)

Hanrahan, J. "Is Bitcoin the Future of Money, or Just the Future of Buying Internet Drugs?" Vice Beta, September 17, 2012. Accessed October 26, 2012. [http://www.vice.com/en\\_uk/read/printable-guns-grey-matters-and-masked-hackers](http://www.vice.com/en_uk/read/printable-guns-grey-matters-and-masked-hackers).

HaveBlue.org. "Gunsmithing with a 3D Printer – Part 2." July 1, 2012. Accessed October 23, 2012. <http://haveblue.org/?p=1321>.

Henke, B. and Damron, R. "Trends in Online Anonymity: Implications for Security and Stability." USEUCOM: Deep Futures QuickLook, September 27, 2012. <https://partners.eucom.mil/J2Home/S/DeepFutures/Document%20Library/QuickLooks/QuickLook%20-%20Anonymity%20Online.pdf>.

Hopkinson, N. "Additive Manufacturing: What's happening and where are we going with printing in the third dimension?" October 2010, pp.19-22. Accessed December 11, 2013. <http://teachfind.com/becta/printer-friendly-additive-manufacturing-neil-hopkinson-15>.

i.materialise.com. "Material Comparison." Accessed January 21, 2013. <http://i.materialise.com/materials/compare>.

International Powder Metallurgy Directory. "Laser sintering - Versatile Production of Tooling Inserts, Prototype Parts and End Products from Metal Powder." January 12, 2011. Accessed December 10, 2012. <http://www.ipmd.net/articles/articles/001087.html>.

John S. (pseudonym). "I want to purchase my first bitcoins anonymously." Bitcoin Forum, May 4, 2012. Accessed December 20, 2012. <https://bitcointalk.org/index.php?topic=79288.0>.

Keiser, M. Russia Today. "Keiser Report: GIABO! (E154)." YouTube.com, June 9, 2011. Accessed November 15, 2012. <http://www.youtube.com/watch?v=qJlKl4LbeQo#at=720>.

KneecapSniper (pseudonym). "AR 15 Printing." YouTube.com, October 8, 2012. Accessed October 22, 2012. <http://www.youtube.com/watch?v=4DeDx76l9sA>. (Image captured at T=00:31);

KneecapSniper (pseudonym). "Firing printed AR15 Lower Receiver with 5.45 upper." YouTube.com, January 28, 2013. Accessed February 1, 2013. <http://www.youtube.com/watch?v=uQz2aNGDoh0>.

KneecapSniper (pseudonym). "Firing rifle with printed lower." YouTube.com, August 12, 2012. Accessed October 22, 2012. <http://www.youtube.com/watch?v=E9CuejI6YvE>. (Image captured at T=01:49.)

Koebler, J. "Online Black Market Drug Haven Sees Growth Double." U.S. News and World Report, August 7, 2012.

Kotler, S. "Vice Wars: How 3D Printing Will Revolutionize Crime." Forbes online, July 31, 2013. Accessed February 7, 2013. <http://www.forbes.com/sites/stevenkotler/2012/07/31/the-democratization-of-vice-the-impact-of-exponential-technology-on-illicit-trades-and-organized-crime/>.

kunkmiester (pseudonym). "Manufacturing Tolerances." WeTheArmed.com. Accessed January 16, 2013. <http://wethearmed.com/general-firearms-discussion/manufacturing-tolerances/>

Leigh, S, Bradley, R., Pursell, C., Billson, D. & Hutchins, D. "A Simple, Low-Cost Conductive Composite Material for 3D Printing of Electronic Sensors." PLOS ONE, November 12, 2012. Accessed February 27, 2013. <http://www.plosone.org/article/info:doi/10.1371/journal.pone.0049365?imageURI=info:doi/10.1371/journal.pone.0049365.g003#pone-0049365-g003>

Limer, Eric. "3D Printed Optics Could Light Up the Gadgets of the Future." Gizmodo.com, October 6, 2012. Accessed February 27, 2013. <http://gizmodo.com/5949572/3d+printed-optics-could-light-up-the-gadgets-of-the-future>.

MAC-11 (pseudonym). "Remaining completely ANONYMOUS." Black Hat World: Black Hat Seo Forum, January 4, 2013. Accessed January 22, 2013. <http://www.blackhatworld.com/blackhat-seo/proxies/518505-remaining-completely-anonymous.html>.

Meyer, D. "US military working on backpack-sized, £440 3D printer." ZDNet Tech, November 12, 2012. Accessed December 19, 2012. <http://www.zdnet.com/-7000007257/>.

Mosher, D. "First 3-D Printing Store Opens In U.S." Popular Science, September 19, 2012. Accessed October 12, 2012. <http://www.popsci.com/diy/article/2012-09/first-3-d-printing-store-opens-world-dominaton>.

National Intelligence Council's Global Trends 2030 report. Office of the Director of National Intelligence. National Intelligence Council. "Global Trends 2030: Alternative Worlds." December 2012. NIC 2012-001. <http://www.dni.gov/nic/globaltrends>.

Office of Senator Dianne Feinstein. "Feinstein Introduces Bill on Assault Weapons, High-Capacity Magazines." Press Release, January 24, 2013. Accessed February 7, 2013. <http://www.feinstein.senate.gov/public/index.cfm/2013/1/feinstein-coalition-introduce-bill-on-assault-weapons-high-capacity-magazines>.

Oxford US English Dictionary Online. "3D Printing." Oxford University Press, 2012. Accessed September 21, 2012. [http://oxforddictionaries.com/definition/american\\_english/3D+printing](http://oxforddictionaries.com/definition/american_english/3D+printing).

Optomec. "Printed Electronics Applications for 3D Printing." [No date.] Accessed February 27, 2013. <http://www.optomec.com/Additive-Manufacturing-Applications/Printed-Electronics-for-3D-Printing>

Osborne, Charlie. "Printable Organs? Breakthrough: 3D Printed Stem Cells." Smartplanet.com, February 6, 2013. Accessed February 19, 2013. <http://www.smartplanet.com/blog/bulletin/printable-organs-breakthrough-3d-printed-stem-cells/12126>

Planes, A. "The Death of Manufacturing is Coming ... Eventually." The Motley Fool, February 6, 2012. Accessed January 4, 2013. <http://www.fool.com/investing/general/2012/02/06/the-death-of-manufacturing-is-coming-eventually.aspx>.

Raskin, M. "Dollar-Less Iranians Discover Virtual Currency." Bloomberg Businessweek, November 29, 2012.

rechar Inc. "Shop-in-a-box- an off-grid, open-source factory built from a 20' shipping container." Accessed November 12, 2012. <http://www.re-char.com/shop-in-a-box/>.

Samarrai, F. "Student Engineers Design, Build, Fly 'Printed' Airplane." UVA Today, October 5, 2012. Accessed October 20, 2012. <http://news.virginia.edu/content/student-engineers-design-build-fly-printed-airplane>.

Sissons, A. and Thomas, S. "Three Dimensional Policy: Why Britain needs a policy framework for 3D printing." Big Innovation Centre, October 16, 2012. Accessed November 6, 2012. <http://biginnovationcentre.com/Publications/23/Three-Dimensional-Policy-Why-Britain-needs-a-policy-framework-for-3D>.

Solid Concepts, Inc. "3D Printing." Accessed January 10, 2013. <https://www.solidconcepts.com/3d-printing/>.

South Eastern and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons (SEESAC). "SALW in South Eastern Europe, Parliamentary Handbook 2010," p. 7. Accessed October 23, 2012. [www.seesac.org/uploads/studyrep/SALW\\_engleski.pdf](http://www.seesac.org/uploads/studyrep/SALW_engleski.pdf).

Sporting Arms and Ammunition Manufacturers' Institute, Inc. "Specifications and Information." Accessed December 19, 2012. [http://www.saami.org/specifications\\_and\\_information/index.cfm](http://www.saami.org/specifications_and_information/index.cfm)

Subject matter expert (SME), Joint Interagency Counter Trafficking Center (JICTC). Interview by Regan Damron and Brian Henke. November 8, 2012. Source declined individual attribution due to sensitivity of subject matter.

sudo-su (pseudonym). "How to be completely anonymous online." Slashgeek.net, June 15, 2012. Accessed November 19, 2012. <http://www.slashgeek.net/2012/06/15/how-to-be-completely-anonymous-online/>.

Syverson, P. "Practical Vulnerabilities of the Tor Anonymity Network." U.S. Naval Research Laboratory, Center for High Assurance Computer Systems. In Advances in Cyber Security: Technology, Operation, and Experiences, edited by D. Frank Hsu and Dorothy Marinucci. USA: Fordham University Press, (forthcoming) 2013. Accessed January 21, 2013.

The Tor Project. "Download Tor." Accessed January 18, 2013. <https://www.torproject.org/download/download.html.en>;

The Tor Project. "Tor Metrics Portal: Users." Accessed January 21, 2013. <https://metrics.torproject.org/users.html>.

Thompson, Cadie. "How 3D Printers Are Reshaping Medicine." TechEdge: A CNBC Special Report, October 10, 2012. Accessed February 19, 2013. [http://www.cnbc.com/id/49348354/How\\_3D\\_Printers\\_Are\\_Reshaping\\_Medicine](http://www.cnbc.com/id/49348354/How_3D_Printers_Are_Reshaping_Medicine).

Unicorn (pseudonym). "Tolerance, how the term is misued [sic] in gunspeak." AR15.Com LLC. Accessed January 16, 2013. <http://www.ar15.com/archive/topic.html?b=6&f=2&t=321101>

Virtanen, M. "NY's Cuomo sets sights high on gun control." Wall Street Journal online, January 10, 2013. Accessed February 7, 2013. <http://online.wsj.com/article/AP2c1321842f5d4cacb427c3c519e71abc.html>.

Wikipedia contributors. "FP-45 Liberator." Wikipedia, The Free Encyclopedia. Accessed November 15, 2012. [http://en.wikipedia.org/wiki/FP-45\\_Liberator](http://en.wikipedia.org/wiki/FP-45_Liberator).

Wright, A. "Exploring a 'Deep Web' That Google Can't Grasp." New York Times, February 22, 2009. Accessed January 3, 2013. <http://www.nytimes.com/2009/02/23/technology/internet/23search.html>.

## Chapter 12 References

Arquilla, J., and Ronfeldt, D. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. 1st ed. Rand Corporation, 2001.

Atkinson, R. "If You Don't Go After the Network, You're Never Going to Stop These Guys. Never.'" *The Washington Post*, October 3, 2007, sec. World. <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366.html>.

Borgatti, S.P.. *On Network Analysis in a Supply Chain Context*. A Functional Approach. Supply Chain Management, 2009.

Carr, J. *Inside Cyber Warfare: Mapping the Cyber Underworld*. 1st ed. O'Reilly Media, 2009.

Cockbain, E., Brayley, H., and Laycock, G. "Exploring Internal Child Sex Trafficking Networks Using Social Network Analysis." *Policing* 5, no. 2 (May 2011): 144–157.

Davis, D.B. *Inhuman Bondage: The Rise and Fall of Slavery in the New World*. Oxford University Press, USA, 2008.

Drescher, S. *Econocide: British Slavery in the Era of Abolition*. Univ of North Carolina Press, 2010.

Everton, S.F. *Disrupting Dark Networks*. Cambridge University Press, 2012.

Granovetter, M. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory* (1983).

Hafner-Burton, E. M, Kahler, M., and Montgomery, A. H.. "Network Analysis for International Relations." *International Organization* 63, no. 03 (July 2009): 559.

Kara, S. *Sex Trafficking: Inside the Business of Modern Slavery*. Columbia University Press, 2010.

Keck, M. E., and Kathryn Sikkink. *Activists Beyond Borders: Advocacy Networks in International Politics*. Cornell University Press, 1998.

Microsoft Research, "The Role of Technology in Human Trafficking," <http://research.microsoft.com/en-us/collaboration/focus/education/human-trafficking-rfp.aspx>, accessed 13 December 2012.

Olson, M. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Harvard University Press, 1965.

Petrunov, G. "Managing Money Acquired from Human Trafficking: Case Study of Sex Trafficking from Bulgaria to Western Europe." *Trends in Organized Crime* 14, no. 2–3 (March 2011): 165–183.

Quirk, J. *The Anti-Slavery Project: From the Slave Trade to Human Trafficking*. University of Pennsylvania Press, 2011.

Raab, J. "Dark Networks as Problems." *Journal of Public Administration Research and Theory* 13, no. 4 (October 2003): 413–439.

Rees, S. *Sweet Water and Bitter: The Ships That Stopped the Slave Trade*. UPNE, 2011.

## Appendix B: Acronyms

AA	Acetic Anhydride
AHT	Anti-Human-Trafficking
AOR	Area of Responsibility
AQIM	al-Qaeda in the Islamic Maghreb
ASG	Abu Sayyaf Group – Philippines
ATFC	Afghanistan Threat Finance Cell
AtN	Attack the Network
BMPE	Black Market Peso Exchange
BRIC Countries	Brazil, Russia, India, and China
C-TCO	Counter Transnational Criminal Organizations
CAD	Computer-Aided Design
CARSI	Central American Regional Security Initiative
CBP	Customs and Border Protection
CCMDs	Combatant Commands
CDRUSSOCOM	Commander US Special Operations Command
CHS	Confidential Human Source
CI	Counter-Intelligence
CIA	Central Intelligence Agency
CN	Counter-Narcotics
CN&GT	Counter Narcotic and Global Threats
CO	Criminal Organizations
COTAT	Criminal Organization Threat Assessment Tool
CP	Counter-Proliferation
CT	Counter-Terrorism

CTF	Counter Threat Finance
CTFI	Counter Threat Finance Intelligence
CTN:	Counter Threat Networks
DASD-CN/GT	Deputy Assistant Secretary for Counternarcotics & Global Threats
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DMLS	Direct Metal Laser Sintering
DOD CN&GTS	Department of Defense Counternarcotics and Global Threats Strategy
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
ELN	Ejército de Liberación Nacional (Colombia) National Liberation Army
EM	Electromagnetic
FARC	Revolutionary Armed Forces of Colombia
FBI	Federal Bureau of Investigations
FCC	Federal Communications Commission
FM	Frequency Modulation
GoM	Government of Mexico
GPS	Global Positioning Services
GSPC	Groupe Salafiste pour la Prédication et le Combat
HPSCI	House Permanent Subcommittee on Intelligence
HSI	Homeland Security Investigations
HuJI	Harkat-e-Jihad-al-Islami

ICITAP	International Criminal Investigative Training and Assistance Program
ICT	Information and Communications Technologies
ICT	Information and Communications Technologies
IED	Improvised Explosive Device
IGO	Intergovernmental Organization
IMU	Islamic Movement of Uzbekistan
IPI	International Peace Institute
ISVG	Institute for the Study of Violent Groups
ITFC	Iraqi Threat Finance Cell
ITU	International Telecommunications Union
IW	Irregular Warfare
JIATF-S	Joint Interagency Task Force South
JIATF-W	Joint Interagency Task Force West
JIATF	Joint Interagency Task Force
JICTC	Joint Interagency Counter Trafficking Center
JIPOE	Joint Intelligence Preparation of the Operational Environment
KFR	Kidnap for Ransom
LEJ	Lashkar-e Jhangvi
LET	Lashkar-e Taiba
MANPADS	Man-Portable Air Defense Systems
NAFTA	North American Free Trade Agreement
NGOs	Non-governmental organizations
NSA	National Security Agency
NSC	National Security Council
OUSD(P)	Office of Under Secretary of Defense for Policy

PAC	People's Aman Committee
PGP	Pretty Good Privacy
QDR	Quadrennial Defense Review
RCMP	Royal Canadian Mounted Police
RFID	Radio Frequency Identification
RN-STAT	Radioactive/Nuclear Smuggling Threat Assessment Tool
RN	Radioactive/Nuclear
RPG	Rocket-Propelled Grenade
SALW	Small Arms and Light Weapons
SCA	Socio-Cultural Analysis
SEDENA	Secretaría de la Defensa Nacional; Mexican Secretariat of National Defense)
SEESAC	South Eastern and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons
SELEC	Southeast European Law Enforcement Center
SEMAR	Secretaria de Marina (Mexican Secretariat of the Navy)
SIMI	Students Islamic Movement of India
SLEIPNIR	Organized crime groups capabilities measurement matrix developed by the Royal Canadian Mounted Police
SLS	Selective Laser Melting
SMA	Strategic Multilayer Assessment
SME	Subject Matter Expert
SOD	DEA Special Operations Division
SSCI	Senate Select Committee on Intelligence
SSL	Secure Sockets Layer
SSP	Sipah-e-Sahaba Pakistan
SSRTO	Security, Stability, Transition, and Reconstruction Operations

SWDR	Software-defined radio
TCO	Transnational Criminal Organization
TFU	Threat Finance Units
TFWG	Terrorism Finance Working Group
TOC	Transnational Organized Crime
TON	Tohono O'odham Nation
TSL	Transport Layer Security
TT&P	Tactics, Techniques, and Procedures
TTP	Tehrik-e Taliban Pakistan
UNODC	United Nations Office on Drugs and Crime
USAID	U.S. Assistance and International Development
USCENTCOM	U.S. Central Command
USD(I)	Under Secretary of Defense for Intelligence
USEUCOM	U.S. European Command
USG	U.S. Government
USNORTHCOM	U.S. Northern Command
USPACOM	U.S. Pacific Command
VCs	Venture Capitalists
VEO	Violent Extremist Organization
WCIT	World Conference on International Telecommunications
WISRD	Whole-of-Society Information Sharing for Regional Display
WWII	World War Two