Center for Law & Human Behavior

The University of Texas at El Paso

DHS SYMPOSIUM SERIES NO. 10

Failure Points in Smuggling Networks

October 25, 2017

Research in Brief

BTI Institute

Borders • Trade • Immigration

A Department of Homeland Security Center of Excellence

Center for Law & Human Behavior
The University of Texas at El Paso
500 West University Avenue
Prospect Hall, Room 226
El Paso, Texas 79968
Tel: (915) 747-5920
Email: clhb@utep.edu
Website: http://clhb.utep.edu
Follow us on Twitter @1CLHB

This symposium is supported by the U.S. Department of Homeland Security, Science and Technology, Office of University Programs under Grant Award Number DHS-14-ST-061-COE-00.

This page intentionally left blank

Introduction[1]

The Failure Points in Trafficking Networks project was developed to provide a better understanding of both the end state of failure and the process of failing of illicit smuggling and trafficking networks. Traditionally, the academic literature on illicit enterprise failure lacks a comprehensive framework for analysis and is rarely based on empirical evidence. This study bridged this gap by exploring potential reasons for failure through the collection of data of eight smuggling and trafficking networks across different commodities. Based on a broader understanding of the contexts and dynamics of illicit networks and their supply chains, the study identified some of the processes, locations, and reasons that those networks ultimately failed and are no longer operational. We highlight key similarities and differences found across the eight smuggling and trafficking networks and provide a set of implications relevant to law enforcement which may assist in the identification of network vulnerabilities and missed points for interdiction.

Methodology and Case Selection

To examine the failure of illicit trafficking networks, eight representative case studies were selected using six criteria:

- The primary commodity of the trafficking/smuggling network had to be least one of the following: narcotics, humans, RN, arms or wildlife.
- The trafficking/smuggling network must have crossed at least one secured international border similar to the United States.
- The trafficking/smuggling network consisted of at least three (3) inter-connected individuals.
- Information about the trafficking/smuggling network must be available via open source and/or field research.
- Priority was given to the most recent cases where information was available.
- The identified network must have suffered a disruption and/or failure within their supply chain. The reasons for the network failure and/or disruption had to be documented as well as the mechanisms by which they failed.

Over 100 smuggling and trafficking networks were initially identified, and 39 matched the criteria above. The final networks were selected to maximize diversity (in terms of commodity,

[1] The following is a modified excerpt from:
Brandon Behlendorf and Michelle Jacome. *Failure Points in Smuggling Networks*: Final Report. College Park, MD: START, 2015.
That study was supported by a contract from the U.S. Department of Homeland Security, Domestic Nuclear Detection Office (DNDO) for Task Order No. HSHQDC-13-J00368 under Contract No. HSHQDC-10-A-BOA36 with the National Consortium for the Study of Terrorism and Responses to Terrorism (START). Copies of that report are available by contacting the primary author at bbehlendorf@albany.edu.

geography and operations), relevance to project aims, and with input from funders and outside experts. The final selection consisted of:

1. Jacob Stuart Network (Narcotics): The Stuart DTO is classified as an international poly-drug bidirectional distribution operation that was responsible for trafficking approximately 1,000-2,000 pounds of marijuana and 100-200 kilos of cocaine per month across U.S./Canadian borders between 2006 and 2011.
2. Hernan Prada Network (Narcotics): Prada operated a decades-long conspiracy to import cocaine to the U.S. from Colombia through multiple routes and modalities between 1988 and 2006.
3. Soto-Huarto Network (Human): At least eight men operated safe houses throughout the Edinburg, Texas, area to hide groups of undocumented immigrants entering the U.S. from Latin American countries. The group was responsible for smuggling approximately 100 illegal immigrants per week and lasted until 2003.
4. Sister Ping Network (Human): Sister Ping ran a lucrative human smuggling operation between the Fujian Province, China and the United States (especially New York City) between 1980 and 2000.
5. Al-Kassar Network (Arms): Monzer Al-Kassar was the head of an international "embargo busting" arms trafficking network spanning from 1970 to 2007. Al-Kassar was known to provide weapons to terrorist organizations and embargoed countries.
6. Rodrigues-Duindam (Wildlife): This network carried out a bidirectional trafficking operation of Brazilian and European wildlife from Curitiba, Brazil, to Amsterdam, the Netherlands, transiting through northern Brazil and the Tri-Border Area between 1998 and 2010.
7. Dadayan Network (Nuclear): The Dadayan network was a small series of operations involving the transfer and attempted sale of HEU through Georgia and Armenia in 2003 and 2010.
8. Illich/Vagner Network (Nuclear): This network was a loose agglomeration of European suppliers and traders that emerged in 1993 and 1994 in response to a German sting operation targeting loose nuclear material. The network attempted to broker 6 purchasing deals of RN materials.

For each network, data was collected about each individual, location, role in the organization, and relationships (external and internal) and was coded according to a standardized framework. Additionally information was collected on environmental factors and other attributes that facilitate the movement of the commodity. Finally, the process by which the network failed was also documented. The information was retrieved from open source documents including court documents, newspaper articles, books, and other academic literature. One of the key limitations of this comparative study is that activities about clandestine networks are limited. The information that was collected primarily represents the actions of law enforcement and their surveillance processes.

Conceptualizing Network Failure

While there is no clear consensus on the definition of failure for illicit organizations, we conceptualize failing as *a process whereby endogenous and exogenous disruptions at key points in their operations (nodes, links, supply, and demand) can reduce an organization's capabilities and increase their likelihood to cease operations.* Regarding illicit smuggling and trafficking, it is best typified by the cessation of the majority of activities and/or the inability to continue operations from the same suppliers to the same demand with the same members through the same channels.[2]

Previous Models of Failure: In order to understand failure as an end state that emerges from a longer process of failing, it is important to review the literature on organizational failure. This literature focuses on the exogenous environment and/or the endogenous organizational/leadership characteristics as potential causes contributing towards failure.[3]

- Exogenous Factors: are disruptions related to the external environment of a technological, regulatory, economic or demographic nature. These may include: introduction of new competitors into the market,[4] technological uncertainty or product innovations, and fluctuation in customer behavior.[5]
- Endogenous Factors: are disruptions related to the organization's perception of the external environment and the ability to shape management practices.[6] The endogenous perspective argues that mental models of the organization and its environment, [7] coupled with the existing power structures and ability to implement or enforce change, determines the firm's ability to respond adequately to its external environment. [8]

Security/Efficiency Tradeoff: When comparing to licit enterprises, illicit enterprises are likely to have lower capitalization, fewer personnel, and less formal management—all characteristics that under the licit business framework would indicate a higher risk of failure. Operating in a clandestine environment, illicit enterprises have to take into consideration its visibility to law

---

[2] J. Freeman, G. Carrol and M. Hannan. "The Liability of Newness: Age Dependence in Organizational Death Rates," American Sociological Review. (1983). Vol. 48, No. 5: 694.

[3] W.R. Scott. *Organizations: Rational, Natural and Open Systems.* (1995). Englewood Cliffs, NJ: Prentice Hall; J. Schumpeter. The Logic of Organizational Irrationality." *Administration and Society*. (1942). Vol. 21: 31-33. B. Jovanovic and S. Lach. "Entry, exit and diffusion with learning by doing." *American Economic Review.* (1989). Vol. 79:690–699. S. Slater and J. Narver. "Does competitive environment moderate the market orientation performance relationship?" *Journal of Marketing.* (1994). Vol. 58:46–55. K. Mellahai and A. Wilkinson. "Organizational failure: A Critique of Recent Research and a Proposed Integrative Framework." *International Journal of Management Reviews*. (March 2004). Vol. 5/6:1-23.

[4] M.T. Hannan and J.H. Freeman. "Structural inertia and organizational change." *American Journal of Sociology*. (1989). Vol. 49: 149-164.

[5] P. Anderson and M. Tushman "Organizational Environments and Industry Exit: The Effects of Uncertainty, Munificence, and Complexity." *Industrial and Corporate Change*. (2001). Vol. 10: 657-711.

[6] M.A. Mone, W. McKinley and V.L. Barker. "Organizational decline and innovation: A contingency framework." *Academy of Management Review.* (1998). Vol. 23: 115-132.

[7] J. Argenti. *Corporate collapse: The causes and symptoms.* (1976). New York. John-Wiley.

[8] R. Greenwood and C.R. Hining. "Understanding Radical Organizational Change: Bringing Together the Old and the New Institutionalism." *Academy of Management Review*. (1996). Vol. 21. No. 4. 1022-1054.

enforcement and balance the tradeoff between security and efficiency. [9] Illicit enterprises may ensure secrecy by insulating the organization's most critical components and actors through a hierarchical command-and-control structure, yet these structures are considerably less efficient than more decentralized network structures common to illicit smuggling and trafficking. [10] Overall, the requirement to balance secrecy and efficiency within criminal enterprises dramatically changes the available options illicit organizations have for responding to internal and external disruptions compared to licit enterprises. [11]

Interdiction

The primary reason for failure described in the literature on illicit networks is the purposive interdiction of law enforcement to target key nodes and actors. The interdiction process itself contains five dimensions that are relevant to understand its role in initiating failure or responding to vulnerabilities presented by different networks. These dimensions include methods, patterns, targets, vulnerabilities, and responses to interdiction.

The Methods of Interdiction: There are two methods of interdiction: the active and passive use of surveillance, and the active engagement of the network through informants and infiltration.

- Surveillance*:* The use of both passive and active surveillance was an important component in determining when and how successful interdiction efforts would be across the networks examined. Communications surveillance was widespread, especially the use of wiretaps. Authorities tended to focus on the buyers of the illicit commodity to monitor communications and discover additional network members as they moved back through the supply chain. Vehicle tracking (both manual and electronic) was used in several of the networks, and in more recent cases video surveillance supplemented the wiretaps as intelligence gathering methods.
- Active Engagement: Nearly all of the networks in this study had some level of active infiltration and engagement by law enforcement through the use of informants and undercover agents. Active engagements were somewhat difficult to maintain when networks crossed a number of different jurisdictions, and coordination was needed across agencies to maintain continual engagement with networks. In some cases, engagement was opportunistic, the result of an informant coming to law enforcement or a piece of evidence made available.
- Arrest and Seizure: Arrests and seizures were a third strategy of interdiction utilized in all of the networks in this study. In many cases, arrests were conducted at the end of an attempt by undercover agents to purchase the illicit commodity, and resulted in the removal of those nodes immediately associated with the transaction. One strategy which would be

[9] C. Morselli, C. Giguère, and K. Petit, "The Efficiency/Security Trade-off in Criminal Networks." *Social Networks*. (2007). Vol. 29: 143-153.
[10] W. Baker and R. Faulkner. "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry." *American Sociological Review.* (1993). Vol. 58: 837–860.
[11] R. Lindelauf, P. Borm, and H. Hamers. "The Influence of Secrecy on the Communication Structure of Covert Networks." *Social Networks.* (2009). Vol. 31: 126–137.

less relevant for more dangerous commodities (like RN) used wiretaps and other surveillance to identify trafficking routes, seized the product en route, and then attempted to convince the individual interdicted to either inform on network operations or gather additional surveillance through audio recordings of meetings and transactions.

***The Pattern of Interdiction*:** One key observation which emerged over the course of our study was the regularity or pattern of the interdiction process. We found three unique operational tempos across these eight networks; tempos which shaped the nature and timing of interdiction efforts and are relevant to understanding the sequencing of failure:

- Sporadic disruption- A number of interdiction attempts in these networks were not coordinated across law enforcement agencies nor were they necessarily targeted at dismantling the network. Sporadic disruptions tended to be the result of situational law enforcement where officers noticed things out of place or activities that were unexpected.
- Patient degradation- Law enforcement would conduct lengthy surveillance and network infiltration operations that patiently attempted to degrade the networks capabilities or resources. Intentional and strategic, these operations were designed to build the evidentiary case against an organization for prosecution, as well as use surveillance to gather intelligence about the extent of network operations and members
- Rapid dissolution- Almost all of the networks experienced a rapid process of arrest and seizures in a shortened time frame which prevented the ability of networks to adapt and respond to these interdiction efforts. These "rapid dissolutions" involved arrests coordinated and sequenced in order to generate the greatest reduction in capabilities, and usually arrested the key leader of the network last.

***Targeting of Interdiction**:* When conducting interdiction operations, law enforcement have four targets within these networks: key leaders[12], brokers/coordinators[13], facilitators[14], and

[12] Typically, these nodes are referred to as leaders, although the accuracy of this moniker is debatable. Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Error and attack tolerance of complex networks." *Nature* 406, no. 6794 (2000): 378-382); Béla Bollobás and Oliver Riordan, "Robustness and vulnerability of scale-free random graphs." *Internet Mathematics* 1, no. 1 (2004): 1-35; Paolo Crucitti, Vito Latora, and Massimo Marchiori, "A topological analysis of the Italian electric power grid." *Physica A: Statistical Mechanics and its Applications* 338, no. 1 (2004): 92-97; Wayne Baker and Robert Faulkner, "The social organization of conspiracy: illegal networks in the heavy electrical equipment industry." *American Sociological Review* 58, no. 12 (1993): 837–860; Duncan McAndrew, "The structural analysis of criminal networks." In: David Canter and Laurence Alison (eds.), *The Social Psychology of Crime: Groups, Teams, and Networks, Offender Profiling Series, III* (Aldershot, UK: Dartmouth, 1999): 53–94; Malcom K. Sparrow, "The application of network analysis to criminal intelligence: An assessment of the prospects." *Social Networks* 13, no. 3 (1991) 251–274.

[13]Jennifer Xu and Hsinchun Chen, "The topology of dark networks." *Communications of the ACM* 51, no. 10 (2008): 58-65; Carlo Morselli and Julie Roy, "Brokerage Qualifications in Ringing Operations." *Criminology* 46, no. 1 (2008): 71–98; Carlo Morselli and Cynthia Giguere, "'Legitimate Strengths in Criminal Networks.'" *Crime, Law and Social Change* 45, no. 3 (November 2, 2006): 185–200.

[14] Carlo Morselli and Cynthia Giguere, "'Legitimate Strengths in Criminal Networks'." *Crime, Law and Social Change* 45, no. 3 (October 2006): 185–200. Phil Williams, "Transnational Criminal Networks." In, John Arquilla and David Ronfeldt (eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND Corporation, 2001): 61.

low-level members.[15] Across the eight networks, the primary targets for interdiction were key leaders and low-level members. Interdictions focused on surveying and gathering intelligence on key leaders to build an evidentiary case, while low-level members were targeted for "flipping" or intelligence gathering. Brokers/coordinators were targeted sporadically, and often near the end of interdiction operations. Most importantly, suppliers were rarely targeted in any of the networks; a missed opportunity to disrupt network operations early.

***Network Vulnerabilities to Interdiction**:* Networks can also have structural, operational, and supply chain functions which create vulnerabilities to interdiction efforts.

- Structural Vulnerabilities: The study identified three main structural vulnerabilities: delegation of authority to subcontractors and partners; lack of redundancy; and visibility of key actors.
- Operational Vulnerabilities: Three operational vulnerabilities were identified across the studied networks: primitive and inconsistent use of concealment methods; lack of secrecy; and centralized documentation. These vulnerabilities were present across most networks at varying levels.
- Supply Chain Vulnerabilities: Different structural elements of the supply chain may also result in vulnerabilities. The study identified three: localized supply; exposed transportation and distribution methods; and fluctuating demand.

The Response to Interdiction: Once the interdiction process has begun, there are a number of ways in which groups can respond that can either strengthen their position or increase their vulnerability to failure. These responses can involve changes in operations, network structure, or protocols and practices to improve secrecy and reduce the likelihood of subsequent detection.

- Adaptive Responses:[16] We found that six of the networks showed a resilient capacity (to varying degrees) when responding to the interdiction process and those responses are best categorized across the following dimensions:
    - *Strategic and technological improvements*: Improvements were primarily focused on the development of new communication protocols or concealment methods to evade detection of future routes.

[15] Alexandra Natapoff, *Snitching: Criminal Informants and the Erosion of American Justice* (New York, NY: New York University Press, 2009). Sean S. Everton, "Tracking, Destabilizing and Disrupting Dark Networks with Social Networks Analysis." (Naval Postgraduate School, 2008): 182; Also see: Pamela A. Popielarz and J. Miller McPherson, "On the edge or in between: Niche position, niche overlap, and the duration of voluntary association memberships." *American Journal of Sociology* 101, no. 3 (1995): 698-720. Stark, Rodney, and William Sims Bainbridge. "Networks of faith: Interpersonal bonds and recruitment to cults and sects." *American Journal of Sociology* 86, no. 6 (1980): 1376-1395.

[16] René M. Bakker, Jörg Raab, and H. Brinton Milward, "A Preliminary Theory of Dark Network Resilience." *Journal of Policy Analysis and Management* 31, no. 1 (December 2012): 55.

- *Differentiated operations and structure:* Some networks, especially those who experienced a substantial seizure or interdiction, moved to re-orient infrastructure and operations around a compartmentalized model of management.
- *Shifted Operations to New Routes:* When one route was interdicted, several networks responded by developing alternative routes through new locations to the same destination.
- *Shifted Operations towards New Priorities:* Even though not prominent in all networks, the loss from a specific seizure or arrest can alter the ability of networks to maintain profitability or prioritized the need to accelerate some operations to repay financial losses from the seizure.

- Failure to Adapt: There were a number of incidents where the networks were unable to adapt successfully for primarily two reasons: either the network had no time / personnel / capacity to adapt, or the network committed a strategic miscalculation which resulted in future disruptions and failure.
  - *Problems of Capacity or Capability:* Some of the networks were unable to respond to interdiction efforts due to a lack in capabilities or the rapid nature of the interdiction strategy.
  - *Strategic Miscalculation:* In response to an interdiction, networks sometimes made a strategic miscalculation to choose untested routes or trust unverified partners, both which increased their vulnerability to law enforcement.

Outside the Interdiction

The interdiction process, and the network responses to interdiction, shaped some of the reasons why specific networks failed. Alongside the interdiction process, there are other structural or operational changes that networks experienced; changes which substantially reduced their ability to keep network members or maintain continued shipments of illicit commodities. For the networks in this study, six different exogenous or endogenous changes relevant to their failure occurred outside of interdiction. These changes include:

- Supply Interruption (Exogenous): Significant increases or decreases in the supply of contraband – whether in the production, manufacturing, or transportation phases.[17]
- Demand Interruption (Exogenous): Significant decreases or increases in consumer or end-user demand for a particular service, product, technology, or consumable good. [18]
- Desertion/Defection (Endogenous): Network member removing themselves from the illegal enterprise to join a competitor, inform to law enforcement, or leave the illicit lifestyle completely.[19]

[17] Helen Peck, "Drivers of supply chain vulnerability: an integrated framework." *International Journal of Physical Distribution and Logistics Management* 35, no 4 (2005): 210-232.
[18] Bruno Gruselle, "Proliferation Networks and Financing." *Fondation Pour La Recherche Strategique, March* 3 (2007). http://www.frstrategie.org/barreFRS/publications/rd/2007/RD_20070303_eng.pdf.

- Strategic Miscalculations (Endogenous): Strategic decision by network leadership which, in hindsight, results in any other reason for change, including interdiction.
- Dissension (Endogenous): Disagreement between network members (situational or extended) which can lead to intragroup violence, increased visibility and vulnerability to interdiction.
- Error/Accident (Endogenous): Unintentional mistakes by a network member.

Overall Reason for Failure

From the comparative case study, we find that the reasons for failure for the eight networks under study are varied. Individuals could defect, errors are made, or law enforcement makes an arrest, all of which could start a chain of events which lead a network to failure. Across the eight networks, though, we do see two key findings regarding failure. In a majority of cases, it was actions that occurred before the interdiction process which either made the network vulnerable to interdiction or led directly to the interdiction itself. Second, the majority of networks experienced at least one strategic miscalculation on behalf of group leadership which contributed to their failure, irrespective of whether the response was to interdiction or an action which occurred prior to interdiction.

- Failures Primarily Induced by Interdictions
  - *Stuart* — Interdiction → Strategic Miscalculation
  - *Vagner/Illich* — Interdiction alone
- Failures Primarily Induced Prior to Interdiction
  - *Al-Kassar* — Changing Demand → Strategic Miscalc. → Vulnerability → Interdiction
  - *Dadayan* — Strategic Miscalculation → Vulnerability → Interdiction
  - *Prada* — Error → Interdiction
  - *Soto-Huarto* — Strategic Miscalculation → Dissension → Interdiction
  - *Rodrigues-Duindam* — Desertion → Interdiction
- Failures Induced by Both
  - *Sister Ping*

    Interdiction: Interdiction → Strategic Miscalculation → Vulnerability → Interdiction

    Outside Int.: Supply Disruption → Strategic Miscalc. → Dissention → Death → Error

Missed Points

While each network eventually failed, there were a number of missed points where interdiction efforts could have disrupted network operations either more completely or at an earlier point within the process. By "missed points," we are not highlighting errors in the interdiction process or ill-advised investigative efforts. For all of these networks, it was insightful and

[19] Frank Bovenkerk, "On leaving criminal organizations," 2011, *Crime, Law and Social Change* 55, no. 4 (2011): 261-276. Menachem Amir, "Aging and aged in organized crime." *Journal of Offender Counseling Services Rehabilitation* 13, no. 2 (1989): 61-85.

proactive efforts by law enforcement to survey network operations, insert undercover agents, and ultimately target interdictions that ensured network operations cease and members are arrested. Rather, given what we know about the network and its operations post-hoc, what strategies or points of disruption *could* law enforcement have targeted if they knew the full scope of network operations. These points include:

- Suppliers: Suppliers were a common vulnerability that were rarely targeted. Especially for irregular shipments (arms and nuclear material), targeting suppliers would have created considerable disruptions for network operations. The geographic concentration of some suppliers made the targeting of specific areas where supply originates another opportunity for some networks. Although difficult to execute given political and jurisdictional concerns, the targeting of suppliers remains the most potentially effective method for disrupting network operations and leading them to their failure.
- Brokers/Coordinators: Although targeted in several interdiction efforts among the eight case studies, several key brokers remained operational long after discovery. In some cases, key brokers provided the earliest connection to suppliers within the network, and disruption of these brokers at earlier periods might have dismantled the entire operation.
- Transporters: Although the most interdicted segment of the illicit supply chains, a number of smuggling attempts by transporters were not interdicted, especially some where officials inspected the vessel en route and failed to discover the illicit commodity.
- Distributors and Buyers: These endpoints of supply chains were important connections between the final customers of the illicit commodity and the network's retail/distribution systems. For two of the networks, distributors essential to the network's operations were targeted last, presenting missed opportunities for disruption.
- Facilitators: Facilitators, or those public servants who either directly participated in network operations or were bribed to let a shipment pass, were prevalent in a number of the networks in this study. Their involvement circumvented existing detection efforts through a number of means and, in some cases, prolonged the ability of a network to operate. Although these individuals were eventually caught, their cooptation of inspection points and regulatory systems allowed millions in illicit goods into the United States and Europe.
- Key transactions or transfers: The two nuclear smuggling networks had key transfers or transactions which were missed opportunities for discovery of network operations or seizure of the nuclear material. In one network (Vagner/Illich), brokers would use third parties to test samples of the RN material for potential buyers, often without acknowledging the illicit nature of the operation. The Dadayan network physically separated themselves from the HEU they were conveying at a key border crossing, leaving it unattended for several hours.
- Ports of Entry: A number of the networks in the study utilized official Ports-of-Entry to smuggle; for all but one network, however, the commodity itself was never discovered at the POE. In the one case where there was an actual interdiction as the commodity was

transiting through a POE, the discovery was based on an anonymous tipoff prior to the vehicle arriving at the POE rather than POE detection capabilities.

- Between Port of Entry: Of the networks in this study, only a few crossed international borders between POEs, but their numerous crossings were interdicted only a handful of times.
- International Transportation Hubs: Four of the eight networks had key opportunities for interdictions at international airports missed during the course of their operations, either due to failure to alert to the illicit commodity or the corruption of airport personnel to evade detection.
- Storage Location: Most of the networks required storage facilities during the transportation / distribution process, yet they were rarely if ever interdicted.

Beyond these missed opportunities, seven of the networks[20] were analyzed concerning each member's potential for interdiction. Two interdiction strategies were assessed: node removal and deterrence messaging. First, each network member was analyzed regarding the potential fragmentation[21] of the network which could result from their removal from the network structure. The fragmentation potential for the networks varied across commodity, structure and number of nodes removed. In some cases, removing one node would result in a very high fragmentation of the network (al-Kassar), while one node removed in other networks would lead to low fragmentation potential (Stuart and Vagner/Illich). Across all seven networks, the removal of two or more nodes considerably increased the potential fragmentation of the network, and represents a possible alternative interdiction strategy for future counter-trafficking efforts.

Rather than identifying how many nodes to remove, a second analysis calculates what proportion of the network will be reached if X number of nodes are targeted with information that diffuses across Y steps away. Individuals with a greater potential for influencing other members based on their structural position within the network may also have considerable intelligence on network operations or can disseminate deterrence messaging targeting the network more quickly or effectively. Across the seven networks, we find that focusing information operations on one to three key nodes could reach a considerable portion of each network, depending on assumptions. Overall, combining these efforts to target networks through a number of approaches could result in a more effective and efficient interdiction process for law enforcement.

[20] The eighth case study, the Soto-Huarto network, is an all-channel network where each actor would provide an equal opportunity for fragmentation and influence. Therefore, it is excluded from this section.
[21] Stephen P. Borgatti, "Identifying sets of key players in a social network." Computational and Mathematical Organization Theory 12, no. 1 (April 2006): 21-34.

Implications

1. **No one reason for network failure**

   Overall these networks failed for a variety of reasons and in a variety of different sequences. In some cases interdiction was the primary reason for failure, while other networks experienced an internal change prior to interdiction that made them vulnerable to failure.

   Implication: Tailor interdiction strategies

   Given that there is no one method or reason for failure, it highlights the need for specific, tailored interdiction strategies which capitalize on each networks unique structure and vulnerabilities for the disruption and failure. In some cases, a patient surveillance strategy will provide key information on the network's background, structure, and vulnerabilities for interdiction. Other networks will need more active and rapid interdiction to prevent the movement of the particular commodity itself from one country to another.

2. **The process of failing often begins prior to interdiction**

   In a majority of cases, it was actions that occurred before the interdiction process which either made the network vulnerable to interdiction (by changing something in their operations or structure) or led directly to the interdiction itself. This process was often initiated by at least one strategic miscalculation on behalf of group leadership, which either led directly to interdiction or made a network vulnerable to the interdiction process through reduced operational security.

   Implication: Focus intelligence gathering on profiling leadership and identifying network stressors

   Since illicit networks generally centralize their strategic decision-making within a few leaders, it is the mistakes or miscalculations that these leaders make which provide key opportunities for interdiction processes to encourage failure. This suggests that efforts to profile key leaders using available information gathered in the investigation would help identify points and opportunities where interdiction could provoke a strategic miscalculation, leading the network to initiate their own failure. In addition, where possible, intelligence collection should rapidly move to assess the overall trajectory of network operations to determine how to best provoke strategic miscalculations by group leadership.

3. **Smuggling networks are dependent on key subcontractors and third parties**

   Although networks may be resilient to some interdiction efforts, this study finds that they are reliant on specific roles when optimizing their supply chain that present key vulnerabilities. While the transportation of illicit commodities may be the easiest role to replace, several networks used specialized transporters to optimize their shipments; transporters that other illicit networks also used. Moreover, these networks delegated

tactical decision-making to these professionalized services, exposing their networks to mistakes or errors made within these networks. This was especially true the further segmented the commodity's transportation was from key leadership. In addition, other networks (including RN networks) used third parties to test the enrichment of the nuclear material prior to an attempted transaction. These third parties were usually professionally-trained nuclear scientists with the skills to provide approved testing procedures, and were rarely identified or interdicted within those operations.

Implication: Focus interdiction efforts on surveilling or arresting key third parties and subcontractors.

By targeting third parties and subcontractors, interdiction efforts can remove critical segments of network operations that are much more difficult to replace. Although many people can operate vehicles or provide transportation for a single load, relatively few can effectively operate continuous shipments of illicit commodity through a specific route without detection; removing these subcontractors could reduce network capabilities substantially. It is important to note that networks can respond through the development of alternative routes or locations, but this response period is often measured in weeks or months, rather than days. This is especially true for larger shipments which cannot be divided and disseminated into smaller loads. Thus, removing a key subcontractor, coupled with other interdiction strategies, could degrade a network's capabilities and prevent them from rebuilding key competencies.

4. Networks are vulnerable at their suppliers and first-stage brokers, yet these are rarely targeted

The networks in this study (except for human smuggling) all required the production and acquisition of an illicit commodity, which was usually handled outside of core network leadership. These suppliers (and those initial brokers who connected them to the larger network) were critical junctures at the beginning of complex supply chains which were susceptible to interdiction and disruption. Some networks relied on one key supplier, while others relied on one key region or facility for supply; both were opportunities for interdiction that were not exploited within the networks under study. These suppliers were especially important for illicit commodities with irregular shipments, e.g. the al-Kassar and Vagner/Illich networks, as either their availability triggered market demand, or they were needed at key moments to provide access to a specialized item. Disrupting either of these would have considerably reduced network capability to meet market demand, and would have hastened the network's ultimate failure.

Implication: Work with source countries to disrupt suppliers and first-stage brokers

Contextualized to the nature of each commodity, targeted efforts between U.S. and foreign partners focused on identifying and interdicting suppliers could reduce a number of networks' capabilities for trafficking. Many of these illicit commodities have specific locations or processes for supply that lend themselves to consolidated production by a few key entities, and targeting these production sites or personnel

could result in reduced trafficking flows downstream. It is important to also mention that targeting suppliers is not just limited to the final product; precursor components and chemicals necessary for production should also be targeted[22]. Targeting suppliers is difficult, as in nearly all of the cases in this study, their supply originated within countries that were either directly or indirectly out of the reach of U.S. authorities. Although challenging to execute, this implication could have the greatest impact on reducing trafficking activities across a number of networks.

5. Removal of two-or-more key leaders will substantially fragment network structure and operations

The networks in this study exhibited a considerable range of structures and operations. From the highly-centralized al-Kassar network to the decentralized Stuart and Vagner/Illich networks, the nature in which groups were designed to meet the specific demands of their markets and supply chains varied wildly. Regardless of structure, though, their strategic decision-making capabilities were centralized within key leaders of the network, making them prime opportunities for interdiction. Results from the fragmentation analysis in Section 10 suggest that the removal of one key leader within the networks could either fragment the network substantially (al-Kassar) or very minimally (Stuart and Vagner/Illich). Within the simulation, if one more key leader was removed, it increased this fragmentation potential for all networks dramatically, with at least 60% of the existing network structure fragmenting (and losing connection) as a result.

Implication: When targeting key leaders, consider targeting two or more

Thus, although many efforts focus on kingpin strategies targeting one key leader within an organization, the structure of these networks suggest that the simultaneous removal of two key leaders would lead to considerably more fragmentation than the network may have the resources to overcome. Those who serve multiple functions across the network, or those with specialized knowledge or access, should be priorities for these combined interdiction efforts. Although a number of domestic interdiction actions (including raids) can simultaneously remove many more actors than suggested here, the ability to remove two or more key actors outside of the United States is much more difficult and requires considerable cooperation from foreign partners.

6. Networks can be provoked to miscalculate, but requires keen knowledge of network operations

During the surveillance operations of several of the networks in this study, law enforcement conducted several acts intended to provoke the network into a strategic miscalculation. For example, when authorities surveilling the Stuart network seized a key shipment of cash to recruit an informant (which was successful), that seizure led network leadership to change operations (recouping the losses from the seizure) which exposed other members and provided valuable intelligence for interdiction. These attempts to

[22] Efforts underway to identify precursor chemicals for homemade explosives or methamphetamine production could serve as model methods in these cases.

provoke a network into overreaching or misjudging their operational environment can be very successful interdiction strategies, yet they require considerable knowledge of network operations to manage effectively. If this knowledge is not present, then provoking some operations could actually increase potential harm to public safety. Within the same network, when authorities seized a shipment of cocaine but did not allow a police report to be filed, that lack of evidence spurred distrust among network members, leading one leader to plan a violent assault on the person originally transporting the seized material.

Implication: Provocation strategies will need substantial surveillance capabilities

Agencies interested in utilizing provocation strategies within interdiction efforts will need to ensure sufficient resources in order to survey network operations effectively before the provocation is enacted.

About the Author

Dr. Brandon Behlendorf is an Assistant Professor in the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany.

For further information related to this work please contact Dr. Behlendorf at (518) 442-5782 or at bbehlendorf@albany.edu

Follow Dr. Behlendorf on Twitter @bbehlendorf

This page intentionally left blank

BTI Institute

Borders • Trade • Immigration

A Department of Homeland Security Center of Excellence

http://www.uh.edu/bti

Twitter: @CBTIR_UH

CENTER FOR LAW AND HUMAN BEHAVIOR

http://clhb.utep.edu

Twitter: @1CLHB