

SEVER: SIGINT AND CRIMINAL NETWAR NETWORKS

A thesis
submitted to the faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Security Studies

By

Thomas Elfmont, BBA

Washington, DC
March 17, 2010

Copyright 2010 by Thomas Elfmont
All Rights Reserved

Table of Contents

Introduction	1
Netwar Theory	2
SIGINT in Netwar	4
Colombia and the Medellin Cartel	7
Colombian Netwar Lessons	12
Criminal Netwar Networks in Mexico	15
Mexico's SIGINT	20
Laws and Institutions	20
Communications Intercept System	22
Successes	27
Mexican Netwar Lessons	29
Considerations	31
Conclusion	32
Additional References	34

Introduction

On September 16, El Grito, the shout of independence, will cascade through Zocalo Plaza. Father Hidalgo made his famous cry in 1810 and triggered the revolt which toppled the colonial government. One hundred years later, Mexico had much to celebrate. As Porfirio Diaz cried in the plaza, he could visualize the telegraph lines, railways, universities and hospitals that marked three decades of economic growth under his leadership. Yet, he was blind to the revolution around the corner.¹

This year President Felipe Calderon will mark the two hundredth anniversary of El Grito, and the birth of Mexico. Proclamations for the heroes of the nation, the people, and independence will echo throughout the plaza as the palace bells ring. But as this echo fades, it is corruption, drugs, and violence which will continue to resonate in the people's ears. This time the revolution is not so distant.

Narco-trafficking organizations have become a threat to the rule of law in Mexico. The monopoly of violence is no longer limited to the state. Drug related deaths reached 5,612 in 2008 and 7,600 in 2009.² Despite assurances from the government that this is the result of better reporting, victimization surveys provide evidence that the opposite is true.³ The situation is deteriorating. Federal, state and municipal efforts to stem the violence have failed. The stability

¹ Krauze, Enrique. Mexico: Biography of Power. New York: Harper Perennial, 1998. Print.

² El Universal. "Ejecuciones Rompen Record." *El Universal*. 3 Dec 2008. Internet. <http://www.eluniversal.com.mx/notas/560074.html>

Brice, Arthur. "Deadliest Year in Mexico's War on Drugs." *CNN Online*. 1 Jan 2010. Internet. <http://www.cnn.com/2009/WORLD/americas/12/31/mexico.violence/index.html>

³ Instituto Ciudadano de Estudios Sobre la Inseguridad. National Survey on Insecurity. Mexico DF: ICESI, 2009. Internet. <http://www.icesi.org.mx/documentos/encuestas/encuestasNacionales/ENSI-6.pdf>

of the Mexican government has suffered due to the increasing influence of narco-trafficking organizations.

Narco-trafficking organizations have evolved throughout the information age. These organizations have become decentralized, flexible network structures as determined by Netwar theory. New national security laws, the creation of the Ministerial Federal Police, and the installation of signals intelligence (SIGINT) systems, were tools specifically created to counter this threat to Mexico. The extent to which SIGINT degrades criminal Netwar networks has not been researched. This thesis will demonstrate that SIGINT increases the low cost of communication which criminal Netwar networks require in order to survive in a competitive marketplace. Case studies of Colombia and Mexico provide evidence.

Netwar Theory

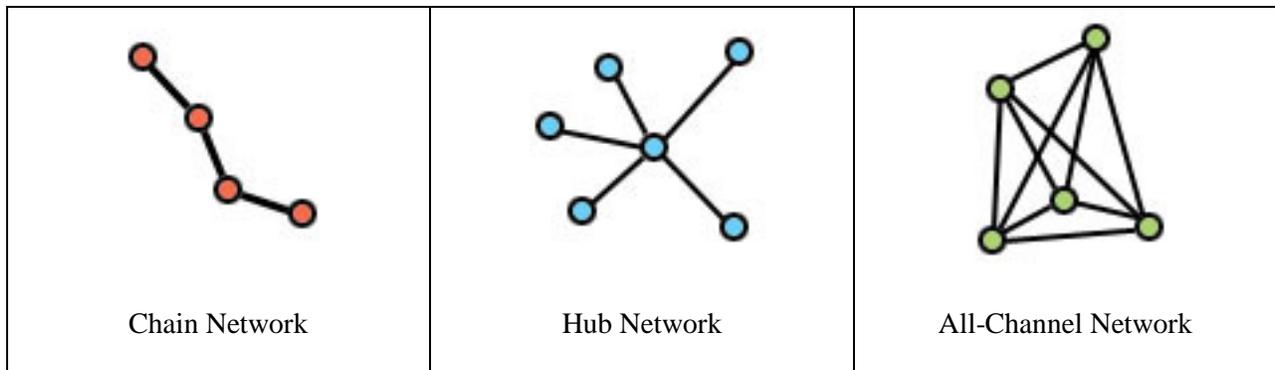
Netwar refers to conflict in which a combatant is organized along networked lines of operational control and other communications. The information age has brought about the rapid transformation of low intensity conflict, crime and activism. This revolution of information and communication systems has allowed terrorist, criminal, and activist organizations to quickly adapt to a new global environment. Low intensity conflict strategies have evolved from a sequential Chess like game, to something free-flowing like Go.⁴ The demarcation between offense and defense has been blurred. Frontlines are non-existent. The objective is no longer to decapitate the enemy's King, but to attain greater control over the battlespace.⁵

⁴ Arquilla, John and Ronfeldt, David. The Advent of Netwar. Santa Monica: Rand, 1996. Print. pp vii

⁵ The Advent of Netwar. pp viii

The information revolution has favored and strengthened network forms of criminal organizations, while making it harder for hierarchical types to compete.⁶ Hierarchical types of organizations such as the Palestinian Liberation Organization, Sicilian Mafia, and Medellin Cartel have given way to networks such as Hamas, Asian Triads, and Mexican narco-traffickers.

These networks can be chain, hub, all-channel, or a hybrid of each. A chain network is typified by smuggling operations where the connections travel end-to-end between intermediaries. A hub has each actor communicating with a central node in the network. An all-channel network has full communication links between each actor. A hybrid network is a combination of any of the former, with a mix of hierarchical or autonomous attributes.⁷



Netwar designs have significant strengths over hierarchical organizations. An adaptable, flexible, and versatile organization can maximize opportunities. Differentiation and interoperability help prevent the dismantling or destruction of an entire network hinging on one

⁶ The Advent of Netwar. pp 4

⁷ The Advent of Netwar. pp vii

actor or node. Third, stealth and the ability to swarm create robust defensive and offensive capabilities.⁸

Information and communication are *the* two factors that have allowed criminal organizations to adopt Netwar designs. Communication technologies are necessary to communicate between and coordinate actors, collect intelligence on the environment and opponents, and broadcast messages to the target audience.⁹ These communication technologies run the spectrum from human runners, to satellite telephones and encrypted data. Criminal Netwar networks rely on communication in order to become more flat and decentralized. Communication is the key determinant in the ability of a criminal organization to evolve into a criminal Netwar network.

SIGINT in Netwar

The strength of a Netwar network is determined by its form of organization, doctrine, technology, and social ties.¹⁰ Modern criminal networks are generally organized along a core and periphery. The core initiates activities and provides direction to the entire network.¹¹ These actors are more closely linked to each other than in the periphery. The periphery are the workers of the organization, and exploit the “strength of weak ties” in order to protect the core and ongoing operations.¹²

⁸ The Advent of Netwar, pp 10

⁹ The Advent of Netwar, pp 15

¹⁰ The Advent of Netwar, pp vii

¹¹ Williams, Phil. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: Rand, 2002. Print. pp 72

¹² Networks and Netwars: The Future of Terror, Crime, and Militancy. pp 73

Actors within the core and periphery include organizers, insulators, communicators, guardians, extenders, monitors, and crossovers. Organizers form the core steering mechanism of the network. Insulators transmit orders from the organizers in order to prevent infiltration of the core. Communicators ensure communiqués flow across the network and provide feedback. Guardians prevent defections and infiltration of the network. Extenders recruit new members or negotiate with other networks. Monitors ensure the effectiveness and flexibility of the network. Crossovers are members of the criminal network that also serve in legal institutions or the government.¹³

SIGINT provides the intelligence necessary to identify the core and periphery of a criminal network, and each actor's role. "Mapping" creates the knowledge necessary to understand the operations of the criminal network. By determining the true core of a criminal network, law enforcement can attempt to disrupt, reduce, or destroy the center of gravity.

Netwar theory contends that an all-channel network is the most robust form of network, and that the information revolution has accelerated its adoption by criminal organizations. The all-channel network has no central core, node, cell, or actor whose removal would destroy the organization. Instead, it relies on the ability to quickly and cheaply communicate between separate actors. Decisions are made by consensus, and require back and forth communication in order to operate. This reliance on communication technology, over the strengths of organization, doctrine and social ties, make SIGINT particularly useful in determining the composition and disposition of a network. All-channel networks have no hierarchy to decapitate, but their reliance on communication can be heavily exploited by SIGINT.

¹³ Networks and Netwars: The Future of Terror, Crime, and Militancy. pp 82-84

Criminal networks in the Netwar age have expanded their tentacles into legitimate political structures and the fabric of society.¹⁴ Businesses are used in order to launder money or provide fronts. Political, judicial, and law enforcement systems are corrupted or infiltrated by crossovers in the criminal Netwar network. SIGINT can be used to monitor the communications of these crossover agents, in a counterintelligence role that mitigates corruption and infiltration.

Due to the “headless” nature of all-channel criminal Netwar networks, the use of force must focus on the disruption of networks rather than their destruction.¹⁵ This disruption can best be achieved through an interagency approach. This approach must involve networked structures on behalf of the state.¹⁶ In SIGINT, this approach would be a combination of intelligence sharing, and networking structures to maximize counterintelligence efforts through compartmentalization and oversight.

SIGINT operations in Colombia and Mexico have demonstrated Netwar strategies by both narco-trafficking organizations and state actors. The Medellin Cartel was a hybrid of chain and hub networks which controlled the narcotics trade for 20 years. SIGINT was used to disrupt and eventually destroy this network through an interagency approach which increased the communication and operational costs of the Medellin Cartel until it was no longer profitable in a competitive market.

Mexican narco-trafficking organizations have evolved towards the all-channel form of network as the information age has progressed. No individual criminal Netwar network dominates the narco-trafficking market, and organizations are continually adapting their

¹⁴ The Advent of Netwar, pp 62-63

¹⁵ The Advent of Netwar, pp 44

¹⁶ Networks and Netwars: The Future of Terror, Crime, and Militancy. pp 16

structure, forms of communication, and operations. La Familia, Los Zetas, the Gulf, Juarez and Sinaloa Cartels, are the larger of thousands of criminal Netwar networks. The large hierarchical networks of the past have broken down into multiple all-channel networks, which are leaderless and operate multiple profit centers from drug trafficking to kidnapping, assassination, and robbery.

Mexico's constantly evolving criminal Netwar networks are at odds against a new interagency and networked SIGINT system. The Communications Intercept System is an attempt to exploit Mexican narco-traffickers heavy reliance on communications. Mexico and the United States are using SIGINT to identify network structures and actors, disrupt the core, and increase the communication costs of narco-trafficking organizations. This strategy first came to fruition in Colombia.

Colombia and the Medellin Cartel

The Medellin Cartel reached unprecedented heights in the late 1980s. The organization made more than 60 million U.S. dollars a day, and *Forbes* listed its chief as the seventh richest man in the world at its peak.¹⁷ Pablo Escobar was known as one of the most ruthless criminals in the world. The enterprise he built became a vertically integrated business model of production, transportation, and wholesale of narcotics. Although more dominant and hierarchical than any of the Mexican organizations today, the context was very similar.

In 1987 U.S. Ambassador Charles Gillespie began warning Washington that the violence in Colombia was threatening to topple the state. The National Security Council would begin

¹⁷ *Forbes*. "The World's Billionaires." *Forbes*. Vol. 146, Iss. 2. 1990. Print. pp 121

preparation of a strategy to shore up the government, and the President of Colombia would declare martial law.¹⁸

Kidnappings, assassinations, and warfare between the Medellin and Cali Cartels were an outright plague during the late 1980s. By 1989, pipe bombings became prevalent and escalated into a three way war between the cartels and government. The police attempted to arrest Pablo Escobar in multiple raids, but he was always tipped off in advance due to corruption and the infiltration of government forces by crossovers. In retaliation, Escobar would set off car bombs targeting government officials such as General Miguel Maza, the head of the Colombian intelligence agency.¹⁹

The violence in Colombia reached a tipping point after the murder of a presidential candidate and the bombing of a civilian airliner. Luis Galan was an outspoken enemy of the drug cartels, and the expected victor of the upcoming presidential election. He was gunned down by one of Escobar's men at a campaign rally. The bombing of Avianca Flight 203 resulted in the death of all passengers in order to kill Galan's successor.²⁰ These two actions would result in a swift response by the United States.

President George Bush undertook a direct approach to shore up assistance for the government of Colombia. National Security Directive 18 called for more than \$250 million in intelligence, military, and law enforcement assistance over five years. A small number of U.S.

¹⁸ United States. Department of Defense. Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. The Andean Strategy – Its Development and Implementation: Where We are Now and Where We Should be Going. Washington: GPO, 1991. Print.

¹⁹ Strong, Simon. Whitewash: Pablo Escobar and the Cocaine Wars. London: Macmillan, 1995. Print. pp 131-133

²⁰ Bowden, Mark. Killing Pablo. Penguin Books: New York, 2001. Print. pp 59

Special Forces were also authorized to train Colombian police and military units in rapid strike tactics.²¹ This directive started the expanding role for U.S. forces in Colombia.

The National Police created a new unit called the Bloque de Búsqueda (Search Bloc) in cooperation with U.S. trainers. The Search Bloc was forced to operate independent of other police organizations due to their obvious corruption and infiltration by the cartels. Thirty out of the two hundred members of the Search Bloc were killed in the first fifteen days of duty. These assassinations were largely aided by the local police.²² In conjunction with the bombing of government infrastructure, the message was given that the Medellín Cartel could attack whenever and wherever it wanted. The rule of law was unenforced.

The U.S. Army would deploy Delta Force operatives in order to train the Search Bloc, and Centra Spike in order to support their operations. Centra Spike was a SIGINT unit designed to eavesdrop on communications and determine their point of origin. Airborne equipment would be used to intercept target signals, and triangulate them in order to provide an immediate location.²³ This system monitored cell phones and different types of radio frequencies.

Jose Rodriguez Gacha was considered to be the chief leader of the Medellín Cartel, and its most violent criminal at this time. Centra Spike's first target would be Gacha. Gacha came under significant pressure in the fall of 1989 as he was thought to be responsible for the Avianca bombing. He evaded arrest by traveling between rural estates, but Centra Spike was able to monitor and pinpoint his cell phone and radio transmissions. A radio transmission requesting prostitutes at his location would provide the intelligence necessary for the raid which killed him.

²¹ United States. Executive Branch. National Security Directive 18. Washington: GPO, 1989. Print.

²² Killing Pablo. pp 67

²³ Killing Pablo. pp 73

The SIGINT provided by Centra Spike not only killed a top member of the Medellin Cartel, but provided the intelligence necessary to map the network. Phone interceptions following the death of Gacha were monitored in order to chart the power structure of the cartel. Most of these phone calls led to Pablo Escobar.²⁴ SIGINT enabled Centra Spike to identify Pablo Escobar as the core actor of the network. It also demonstrated the hub network design of the Medellin Cartel.

Centra Spike would continue to exploit SIGINT, and hand the results over to the Colombians. Most of this intelligence would be squandered due to the infiltration of the Search Bloc by Medellin Cartel crossovers. Escobar was tipped off multiple times, and eventually walked out of his self created prison despite the presence of four hundred guards and soldiers.²⁵ The tip offs and brazen escape would lead to a heavier counterintelligence role for Centra Spike's SIGINT operators. They would also continue to monitor the Medellin Cartel.

By 1992, Escobar and the Medellin Cartel began to use various methods of communication to avoid interception. Escobar went from communicating unhindered, to using as many as eight different cell phones and scrambling devices.²⁶ Not only did the cost of communication go up, but the inability to directly communicate with lieutenants led to increasing autonomy within the network. The Medellin Cartel was forced to adapt their Network design in order to combat disruption by SIGINT.

In 1993, Centra Spike's increased counterintelligence role helped identify crossovers within the Search Bloc. Calls placed from within the police headquarters alerted Escobar's men

²⁴ Whitewash. pp 223-224

²⁵ Killing Pablo. pp 141

²⁶ Killing Pablo. pp 145

to an upcoming raid.²⁷ This intelligence would help eliminate infiltrators among the leadership of the Search Bloc. Centra Spike, Delta Force, and the top leadership of the Search Bloc began to compartmentalize and provide oversight of intelligence. State forces were evolving towards a Netwar network alongside the Medellin Cartel.

As Escobar and his men became more aware of eavesdropping methods, they were forced to adapt their forms of communication. Escobar would utilize elaborate and impromptu codes that required specific dates, places, and events to be memorized. This became problematic for his associates who did not have the same skills of memory.²⁸ By forcing the use of these codes, communication within the Medellin Cartel became more disrupted.

As the hunt for Escobar continued by state actors, a new network emerged to challenge the Medellin Cartel. Los Pepes was a leaderless, all-channel or hybrid network, which sought to kill Escobar and his minions. The National Police, prominent families of Medellin, Cali Cartel, and others were sought to be involved in this loose network with a common objective. Los Pepes were certainly involved with the police, and had access to at least some of the SIGINT provided by Centra Spike. The death squad attacked the white collar network of the Medellin Cartel according to the organizational maps provided by Centra Spike. Medellin Cartel members that provided important information through SIGINT were left unharmed.²⁹

Centra Spike's interceptions increased to the point where Escobar almost never communicated via electronic methods. He was forced to rely on human messengers as SIGINT

²⁷ Killing Pablo. pp 172

²⁸ Killing Pablo. pp 175

²⁹ Killing Pablo. pp 194

continued to intercept his communications, and provide his whereabouts.³⁰ Ultimately, he was forced to use short wave radios in order to communicate with his son and help his family find asylum in another country.

The noose slowly tightened around Escobar and the Medellin Cartel's neck. Los Pepes was able to dismantle the organization from the periphery in, using their sources as well as SIGINT provided by Centra Spike. The interception of electronic communications and locational targeting, forced cartel members to operate on the run. This also made them more vulnerable to other forms of intelligence, such as human infiltration. Operating on the run, and vulnerable to all but face to face communication, the Medellin Cartel started to lose money. Soon, the network was unable to communicate and operate effectively, and became unprofitable in a competitive marketplace.

Colombian Netwar Lessons

1. Netwar Networks Evolve.

The Medellin Cartel was a hybrid of chain and hub Netwar designs caught in the beginning of the information revolution. The chain network provided the vertical processes necessary to produce and distribute narcotics along the periphery, while the hub provided the core central direction. The Medellin Cartel would attempt to adapt to a more decentralized and autonomous organization similar to an all-channel design, but was effectively unable to do so. An all-channel network requires the ability to communicate between each actor, which SIGINT disrupted. The increasing isolation of its leadership created more autonomy, but the network was never able to adapt faster than the restrictions SIGINT and the Cali Cartel placed on it.

³⁰ Killing Pablo. pp 208

The Cali Cartel and Los Pepes exploited their weak hub core, and strong all-channel periphery to maximum advantage against the Medellin Cartel. They also utilized the strength of a Netwar networks' ability for stealth in order to conceal their true core and periphery.³¹ The Cali Cartel's hybrid form of network utilized the "strength of weak ties" to adapt and avoid the hierarchy which SIGINT helped decapitate in the case of the Medellin Cartel.

The decapitation of large hierarchical networks does not result in a reduction of violence. The death of the Medellin Cartel and expansion of the Cali and other cartels, demonstrated that smaller, more nimble networks will spring up as a large network is defeated.³² The demise of a hierarchical, chain, or hub network is only likely to lead to a more dispersed all-channel network. Criminal Netwar networks continue to adapt to their environment.

2. Increase Communication and Operational Costs.

The Netwar model for low intensity conflict is flexible and adaptable. As such, it is all but invulnerable to outright destruction by force. Instead, the use of force should be used to disrupt the network rather than destroy it. The Medellin Cartel went from unhindered access in all forms of communication, to relying on human messengers. Combined with locational tracking, SIGINT identified each actor in the network, what they were doing, and where they were going. Once Colombia was able to identify and attack the core of the network, the center of gravity for the Medellin Cartel was lost. The disruption of business communications and operations made it uncompetitive in the market. Unlike terrorist and activist Netwar network models, criminal networks can only survive if profitable. SIGINT increased communication and operational costs until the Medellin Cartel became uncompetitive in the marketplace.

³¹ Networks and Netwars: The Future of Terror, Crime, and Militancy. pp 74

³² Networks and Netwars: The Future of Terror, Crime, and Militancy. pp 365

3. It Takes a Network to Defeat a Network.

The Colombian-U.S. approach to defeating the Medellin Cartel relied on interagency cooperation and the creation of compartmentalized networks. Transnational criminal networks such as the Medellin Cartel seek to exploit national boundaries with different jurisdictions. They also seek to create “shadow states” in which they can operate with impunity.³³ The Colombians were unable to challenge the Medellin Cartel on their own, due to infiltration and corruption. A separate agency in the form of the U.S. military was necessary to facilitate intelligence. This interagency approach allowed Colombia to focus on kinetic operations, while the U.S. provided intelligence support.

This approach utilized the compartmentalization of information to reduce the threat of espionage within its own network. The collection, analysis, and dissemination of information were networked to maximize the application of counterintelligence. Embedded trainers acted as insulators by disseminating information for the organizers in Centra Spike. These protective actors minimized the risk of defection or infiltration of crossovers in the network. By utilizing the strengths of each agency, minimizing the dissemination of SIGINT, and using SIGINT for counterintelligence, the Colombia-U.S. effort adapted to the changing Netwar environment. This interagency approach became a Netwar network in its own right.

4. The Risk of Abuse.

The death of Pablo Escobar and the Medellin Cartel is marred by the legacy of Los Pepes. Although there is no definitive proof, the Search Bloc was most likely infiltrated by members and sympathizers of the death squad. The dissemination of SIGINT must be

³³ The Advent of Netwar. pp 63

compartmentalized within cells or nodes in the network. Without an adequate balance between access and security, SIGINT is likely to fall into the hands of those that can use this intelligence without regard to the law. Limitations must also be placed according to judicial requirements for wiretapping and other forms of SIGINT collection.

Criminal Netwar Networks in Mexico

Mexican narco-trafficking organizations have developed in accordance with Netwar theory. Netwar theory contends that transnational criminal networks will exploit the information age by evolving into all-channel networks. These networks rely on the low cost of information and communication to become adaptable, versatile, interoperable, redundant, stealthy, and robust. Mexican narco-trafficking organizations have evolved from chain networks, to all-channel networks.

During the 1970s and early 1980s, the Colombian cartels were able to transport narcotics to the United States directly by plane or boat. As U.S. law enforcement increased efforts in airports, the coastline of Florida, and the Caribbean, new routes were needed to get narcotics into the United States. The original Mexican cartels were middlemen in the exchange of narcotics from Colombia and the Andes to the United States. These chain networks received payment from the Colombians in exchange for transit across the U.S.-Mexico border. The narcotics would be transported end-to-end between intermediaries, until it reached its final destination.

Payments to Mexican chain networks were made in cash during the early days of narcotics smuggling. This form of payment was soon replaced by an easier method – a cut of the narcotics being transported. Mexican chain networks would now have to distribute and wholesale their narcotics, in addition to the transportation services they were already providing.

Mexican narco-trafficking organizations evolved into a hybrid design of chain and hub networks during the late 1980s and 1990s. The expansion of duties from transportation to distribution opened up new profit centers such as retail sales and other drugs such as methamphetamines. In order to provide expanded services and products, the Mexican narco-trafficking organizations would require a new network design.

The information age and increased trade with the United States allowed Mexican narco-trafficking organizations to quickly adapt to new network designs. Hybrid networks harnessed the strengths of the chain, hub, and all-channel designs. Transportation would continue to utilize the chain model, but with insular cells which communicated to a central actor in a hub. These hubs would operate with limited autonomy, but also communicated with separate networks that formed cells of the larger criminal Netwar network. One small gang at the periphery may transport narcotics to other gangs, who then communicate operations to a central cell, who is part of the core decision making unit. Modern narco-trafficking organizations in Mexico typify a hybrid of chain, hub, and mostly all-channel networks with a core and periphery.

Seven major cartels with enforcement arms and shifting alliances are responsible for the majority of narco-trafficking in Mexico today.³⁴ These organizations have become all-channel or hybrid networks with a flat hierarchy. Marijuana production is one example of the recent evolution of this design. Marijuana producers in California, the Pacific Northwest, and East Coast of the United States are increasingly linked to each other, yet maintain affiliations with larger networks in Mexico to coordinate their activities.³⁵ Autonomy within subordinate units

³⁴ United States. Congressional Research Service. Colleen W. Cook. Mexico's Drug Cartels. Washington: GPO 2008. Print. pp 1

³⁵ Mexico's Drug Cartels. pp 5

and the coordination of effort, demonstrates a type of consensus decision making that only exists in an all-channel network without centralized leadership.

These loose ties of communication have also extended to prison and street gangs within the United States. These gangs help with wholesale and retail operations, and allow narco-trafficking networks to exploit weak ties. The Latin Kings, Mara Salvatrucha (MS13) and other gangs compete with each other in the United States while Mexican narco-trafficking networks remain impartial observers.³⁶ The ability to maintain or adapt flexible alliances is a strength used by criminal Netwar networks.

Several of the U.S. and Mexican narco-trafficking organizations also support the theory that criminal Netwar networks will exploit borders and jurisdictions. Kidnapping, assassination, and violent crime from these networks exist on both sides of the border.³⁷ The tripling of U.S.-Mexico trade under the North American Free Trade Agreement, and lack of adequate border security has made this possible.³⁸ The border has become a “revolving door” of criminal activity.³⁹ Mexican narco-trafficking networks have exploited borders according to Netwar theory.

The adaptation of narco-trafficking networks to an all-channel design created the necessity for specialized actors. This specialization creates differentiation and redundancy, but can also create splintering groups. The organizers, insulators, communicators and other actors of

³⁶ Mexico's Drug Cartels. pp 6

³⁷ Quinones, Sam and Serrano, Richard. “Mexico Drug Wars Spill Across the Border.” *Los Angeles Times*. 16 Nov 2008. Internet. <http://www.latimes.com/news/nationworld/world/latinamerica/la-na-cartels16-2008nov16,0,464574.story>

³⁸ United States. U.S. Agency for International Development. Central America and Mexico Gang Assessment. Washington: GPO 2006. Print. pp 108

³⁹ Central America and Mexico Gang Assessment. pp 19

a network have sometimes formed rival networks. Two major guardian actors in Mexico became subsidiary networks, and eventually rival networks of their hosts. The larger of the two is a former Special Forces group called Los Zetas.

Los Zetas were a Mexican Army Special Forces group trained by U.S. Special Forces under the Zedillo administration. The group defected en-masse to the Gulf Cartel in order to provide the Netwar role of guardian within the network. This cell would be used to protect narco-trafficking routes and pick off enemies of the Gulf Cartel. Eventually, it became powerful enough to challenge its parent network.⁴⁰ The Negros, Pelones, La Familia, and other former guardians are also new, all-channel networks that have evolved from their original role as an actor within a parent network.

The constant splintering of narco-trafficking organizations is further proof that the all-channel design is becoming more prevalent. Large subsidiaries like Los Zetas have defected, as well as small actors at the periphery. In California, breakaway cells from large narco-trafficking organizations have become specialized actors autonomous from the larger network. A small cell affiliated with the Arrellano-Felix Cartel decided to switch from trafficking to kidnapping in order to maximize their gain and increase autonomy.⁴¹ This was not decided by central leadership, but by consensus within the all-channel cell.

The breakup of large, vertical, and hierarchical networks into increasingly small, horizontal, and all-channel networks has not reduced the threat of narco-trafficking to Mexico or the United States. In addition to the robust defense provided by their interoperability,

⁴⁰ Mexico's Drug Cartels. pp 12

⁴¹ Littlefield, Dana. "17 Indicted in Violent Crime Spree." *San Diego Union Tribune*. 14 Aug 2009. Internet. <http://www.signonsandiego.com/news/2009/aug/14/17-indicted-violent-crime-spree/>

redundancy, and headless nature, Mexican narco-trafficking networks have offensive capabilities. Recent events have demonstrated the use of stealth and swarming.

Mexican narco-trafficking networks rely on stealth in their everyday operations to exist. The use of swarming is a tactic described by Netwar in order to maximize the collective action of decentralized actors. Narco-trafficking networks made a direct attack on the Mexican Army in six cities and two states on April 2, 2010.⁴² The scope and breadth of the attack was unprecedented. Gunmen in armored cars mounted a direct assault on Army barracks, and created roadblocks to prevent escape and reinforcement. Several other ambushes and raids were also coordinated in the two states. The attacks were initiated at the same time, and unattributed to a specific organization. Mexican narco-trafficking networks have demonstrated that swarming and stealth are potent offensive capabilities of a Netwar design.

This decade has seen the breakup and splintering of what were once large and dominant narco-trafficking organizations in Mexico. Even the larger cartels now have thousands of actors that make up hundreds of autonomous networks that communicate amongst each other. This leaderless form of activity operates as a swarm without central leadership. Mexican narco-trafficking organizations have evolved into all-channel networks in order to harness the strengths outlined by Netwar theory. Mexican narco-trafficking organizations have become criminal Netwar networks. The Mexican government has enacted reforms in order to disrupt and reduce the threat of these networks.

⁴² Wilkinson, Tracy. "Mexico Drug Gangs Turn Weapons on Army." *Los Angeles Times*. 30 Mar 2010. Internet. <http://www.latimes.com/news/nationworld/world/latinamerica/la-fg-mexico-gunbattles2-2010apr02,0,5886596.story>

Mexico's SIGINT

Laws and Institutions

The Mexican judicial, law enforcement and national security apparatus are under continuous reform. President Vicente Fox created the National Security Law in 2005 in order to create a national security system after 71 years of one party rule.⁴³ This focus on national versus regime security emphasized the need to maintain “the integrity, stability, and permanence of the Mexican State...”⁴⁴

The threat of organized crime and use of intelligence to combat it is prevalent in the National Security Law. Organized crime is considered a threat to the state, by which the Mexican government can use the Army and Navy to impede its progress.⁴⁵ The institutions legitimized by the act include the National Security Council and the Center for Investigations and National Security (CISEN). CISEN is the primary government agency for generating national security intelligence in Mexico.

CISEN is an autonomous organization within the Ministry of the Interior. Its mission, duties, and appropriate interaction with other agencies are listed in the National Security Law. The interception laws provided for CISEN also apply to the Federal Police.

The use of SIGINT outlined in the National Security Law covers the development of specialized technology, dissemination of information, protection of that information, cooperation

⁴³ Chabet, Jorge. “Mexico: The Security Challenge.” *Canada and Mexico's Security in a Changing North America*. Queens-McGill University Press, 2006. Print.

⁴⁴ Government of Mexico. Executive Branch. National Security Law. Mexico DF: 2005. Internet. <http://www.ordenjuridico.gob.mx/Federal/Combo/L-65.pdf>

⁴⁵ Ibid.

between law enforcement and judicial agencies, due process, and use of any method for collection. The law goes on to include the process for legally obtaining a warrant from a Federal judge, which is not to exceed 180 days, and that all types of communication may be monitored.⁴⁶

The government of Mexico has undergone several systematic reforms of law enforcement, beginning in the 1990s. The most notable structural changes have taken place under the Vicente Fox and Felipe Calderon administrations. Two cabinet level departments administer federal law enforcement agencies. The attorney general's office is tasked with investigating and prosecuting federal crimes. Kidnapping, drug trafficking, arms trafficking, crimes against public health, and other major crimes fall under federal jurisdiction.

The key law enforcement agency under the attorney general's office is the Ministerial Federal Police. It has recently been renamed from the former Federal Investigations Agency. Modeled after the United States' Federal Bureau of Investigation, the agency replaced the corrupt and inefficient Federal Judicial Police. A Special Anti-Organized Crime Unit, and the Office of the Special Prosecutor for Crimes Against Health are organizations that specifically target narco-trafficking. The organized crime unit was created in 1996 in order to address the increasingly coordinated criminal networks in Mexico. The Crimes Against Health Office was specifically designed to prosecute drug trafficking organizations. It has been reorganized multiple times in response to corruption charges, including kidnapping and extortion. The final federal law enforcement organization is the Office of the Deputy Attorney for Special Investigation of Organized Crime. This organization is broken down into six departments which cover: crimes against public health, terrorism and arms trafficking, money laundering and

⁴⁶ National Security Law.

counterfeiting, human trafficking, kidnapping, and robbery. Many of these organizations have multiple overlapping responsibilities.⁴⁷

The Federal Police Act of 2009 outlines the organization and operation of Federal Police agencies in Mexico. Several articles relate directly to the capture of SIGINT. The Federal Police have the powers and duties to engage in surveillance, monitoring, and tracking of the Internet, monitor information in society, integrate databases, intercept communications, and specific actions necessary for a communications intercept warrant.⁴⁸

Much of the national security and police laws developed in the past decade refer to the use of SIGINT by federal authorities in CISEN or the Federal Police. The classified nature of SIGINT systems leaves significant gaps in our knowledge of the capability and use of this form of intelligence. The Federal Police's Communications Intercept System is the only SIGINT system described in public material.

Communications Intercept System

Mexican narco-trafficking organizations represent a threat to both Mexico and the United States. Ninety percent of the narcotics in the United States are transported through Mexico.⁴⁹ The United States has formed a response to this threat. A "comprehensive aid package", the \$1.4 billion Merida Initiative focuses on drug interdiction. Funding includes: eTrace weapon tracking databases, communication servers, x and gamma ray scanners, one naval surveillance plane, five

⁴⁷ Government of Mexico. Executive Branch. National System of Public Security Law. Mexico DF: 2009. Internet. [http://www.ordenjuridico.gob.mx/Federal/PE/APF/APC/SSP/Decretos/2009/02012009\(1\).pdf](http://www.ordenjuridico.gob.mx/Federal/PE/APF/APC/SSP/Decretos/2009/02012009(1).pdf)

⁴⁸ Government of Mexico. Executive Branch. Federal Police Act. Mexico DF: 2009. Internet. <http://www.ordenjuridico.gob.mx/Federal/Combo/L-45.pdf>

⁴⁹ United States. Department of State. International Narcotics Control Strategy Report. Washington: GPO 2010. Print. pp 437

helicopters, and U.S.-Mexico joint crime fighting and training projects.⁵⁰ Within the publicized modernization of servers and databases is a little known SIGINT system.⁵¹

The Communications Intercept System was created to establish “a lawful interception solution that will provide the Government of Mexico...with the capability to intercept, analyze, and use intercepted information from all types of communications systems operating in Mexico. The requested system for information collection and analysis will help deter, prevent, and mitigate acts of federal crimes in Mexico that include narcotics trafficking and terrorism. The Communications Intercept System will strengthen the United States Government’s and Mexico’s protective posture to disseminate timely and accurate, actionable information to each countries respective federal, state, local, private, and international partners.”⁵²

The Communications Intercept System was designed to match the communications environment in Mexico. America Movil and Telmex International are the primary telecommunications companies in the country.⁵³ Carlos Slim Elu controls more than 70% of Mexico’s communications infrastructure. Despite the near monopoly, several forms of telecommunications networks still exist. The Communications Intercept System was designed to exploit Public Switched Telephone Networks (PSTN), Time Division Multiple Access (TDMA),

⁵⁰ United States. Cong. Senate. Merida Initiative Program Description Reference Document Mexican Security Cooperation. Hearings 110 Cong., 2d Sess. Washington: GPO, 2008.

⁵¹ Enriquez, Sam. “Mexico to Boost Tapping of Phones and Email with U.S. Aid.” *Los Angeles Times*. 25 May 2007. Print.

⁵² United States. Department of State. Solicitation S-INLEC-06-R-4042. Washington: GPO 2007. Internet. https://www.fbo.gov/index?s=opportunity&mode=form&id=fbfd348cc3f2ac6be01a8840bf0abbac&tab=core&_cview=1

⁵³ Reuters. “Mexico Cable Operators Attack Slim’s Telecom Tie Up.” *Reuters Wire*. 18 Jan 2010. Internet. <http://www.reuters.com/article/idUSN1816283420100118>

Global Systems for Mobile (GSM), Integrated Digital Enhanced Networks (iDEN), and Code Division Multiple Access (CDMA) phone networks. These systems include every phone service provider in Mexico: Telmex, Telcel, Nextel, Telefonica, Unefon, and IUSACell. Packet data may be intercepted through the Prodigy Internet Service Provider network, which provides more than 92% of Mexico's internet service. Monitoring of Cisco Voice Over Internet Protocol (VOIP) lines at Federal Police offices are also included. The Communications Intercept System can monitor almost any form of electronic communication.

The Communications Intercept System's central monitoring station has real time and off-line playback, fax and packet data decoding, stores all calls for at least 25,000 hours, and has cellular location and tracking. The database in the monitoring station can accommodate 8,000,000 sessions, and monitor and record 60 calls simultaneously. Four facsimiles can also be decoded simultaneously. The monitoring station is a joint Mexico-U.S. network.

Specific tools of analysis are also included in the system. Voice data banks are used for analysis, comparison, recognition and identification. The system has the ability to analyze calls and automatically generate links between them. Additionally, the system has the tools necessary to track cellular targets on a map.

The entire system has been designed in distinct stages. The first stage is the establishment of baseline infrastructure to give the Federal Police operational capability. The second is unknown to the researcher. The third stage covers the internal VOIP system, and locational tracking capabilities to be exercised at the discretion of the U.S. Government. The fourth stage will cover any additional cellular service providers.⁵⁴

⁵⁴ Solicitation S-INLEC-06-R-4042.

The contract for the Communications Intercept System was awarded to Verint Technology in February 2007⁵⁵. Verint considers itself a leader in actionable intelligence. Their products range from workforce optimization, to communications intelligence. The Verint portfolio describes a scalable package between strategic and tactical intelligence.⁵⁶

Analysis of the U.S. Department of State's statement of work for the Communications Intercept System outlines a new, interagency, networked approach to combating criminal Netwar networks. Several advances seem to have been made since efforts in Colombia.

First, mass interception allows for the monitoring of all types of communication in order to track trends and map organizations. The information age has allowed criminal Netwar networks to evolve towards all-channel communication methods, which are rarely one way. The Communication Intercept System can monitor all forms of electronic communication, which all-channel networks require to communicate and make decisions by consensus. It also does this on a much larger scale than before.

One weakness of an all-channel network is that decision making by consensus is more protracted than by a single actor, and can be disregarded more easily.⁵⁷ Increasing the difficulty of all forms of communication not only increases operational costs, but increases the possibility for communication failures and misperception.

⁵⁵ United States. Department of State. Award S-INLEC-07-M-0002. Washington: GPO 2007. Internet. <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=452c714167df2a77ab69e8e51925be42>

⁵⁶ Verint. Investor Relations. 10 April 2010. Internet. http://verint.com/corporate/section2a.cfm?article_level2_category_id=15

⁵⁷ Sangiovanni, Mette and Jones, Calvert. "Assessing the Dangers of Illicit Networks." *International Security*. Vol. 33, No. 2. 2008. Print. pp 21

Second, it takes a network to defeat a network. Mexico and the United States have undertaken an interagency approach. Plataforma Mexico increases intelligence sharing between Mexican law enforcement agencies in order to network their efforts together. Liaison mechanisms establish ties between agencies in both nations. On a regional scale, international law enforcement cooperation has been fostered between Mexico and Panama and Guatemala.⁵⁸

Third, the Communications Intercept System can be combined with the rapid response of forces in Merida funded helicopters. The ability to pass actionable intelligence to tactical units, allows law enforcement to be more operationally flexible than before. Colombia demonstrated the effectiveness of rapid tactical movement against criminal Netwar networks. Mexico can use SIGINT provided by the Communications Intercept System to capture individual actors or intercept money, arms, and narcotics.

The tactical ability to capture actors and seize resources disrupts criminal Netwar networks. These actions generate blame amongst actors and cells in the network, instead of focusing on avoiding future mistakes.⁵⁹ The excessive risks taken by criminals to recoup losses helps SIGINT and other intelligence collection methods further exploit the paranoia of the network.

The Communications Intercept System is part of a broad, interagency SIGINT network that reduces the strengths of criminal Netwar networks. Each of the Netwar network strengths is attacked. First, the organization is reduced because stealth is lost as the network actors are mapped. Second, doctrine must adapt to avoid communication or operational interception by

⁵⁸ International Narcotics Control Strategy Report. pp 438 and Merida Initiative Program Description Reference Document Mexican Security Cooperation.

⁵⁹ “Assessing the Dangers of Illicit Networks.” pp 22

law enforcement. Third, communication technologies become more difficult to operate, and multiple methods have to be employed at increasing costs. Fourth, social ties are reduced as disruption leads to blame and paranoia between actors in the network. The Communications Intercept System was designed as a network, to disrupt criminal Netwar networks.

Successes

Mexico has captured and killed several narco-trafficking leaders over the past year. Miguel Angel Soto Parra of the Gulf Cartel and Arnoldo Rueda Medina of La Familia are just two recent successes.⁶⁰ Intelligence that leads to the capture of a high value target is kept secret in order to maintain the ability to use it in the future. The role of SIGINT in targeting high value targets has not been publicized, but is evident in recent operations.

Two recent successes provide examples of the extent which SIGINT disrupts criminal Netwar networks. Teodoro “El Teo” Garcia Simental was captured on January 13, 2010 in La Paz. El Teo was responsible for hundreds of killings and kidnappings over a two year reign of terror. Surveillance by the Drug Enforcement Administration provided the intelligence necessary for the arrest.⁶¹ U.S. agents cannot operate in Mexico, leaving SIGINT as the primary method for surveillance. This compartmentalized information was disseminated to Mexican law enforcement in order to make the arrest.

A demonstrable success of SIGINT against Mexican narco-trafficking organizations is the capture or killing of several members of the Beltran Leyva Cartel. The Beltran Leyva Cartel

⁶⁰ International Narcotics Control Strategy Report. pp 437

⁶¹ Marosi, Richard. “Mexican Drug Lord Teodoro Garcia Simental, Known for His Savagery, is Captured.” *Los Angeles Times*. 13 Jan 2010. Internet. <http://articles.latimes.com/2010/jan/13/world/la-fg-mexico-arrest13-2010jan13>

gained a competitive advantage over its competitors through influence in the government. The chief of Mexico's organized crime division, Mexican representative at Interpol, and other high level officials were employed by the Beltran Leyva Cartel.⁶² Access to top law enforcement officials allowed this criminal Netwar network to avoid targeting by the authorities, and disrupt or gain intelligence on their adversaries. Crossovers were also placed within the U.S. Embassy in Mexico City and 35 members of the Attorney General's Office would later be implicated.⁶³

A large counterintelligence effort by the Attorney General's office would lead to the arrest of the Beltran Leyva crossovers. The identification of these individuals was determined by SIGINT. Phones in the Attorney General's offices have been tapped. The Communications Intercept System monitors the VOIP lines in Federal Police offices. The system was built to network government agents and agencies in both Mexico and the United States. This was done to compartmentalize information and provide oversight. This self-monitoring has created a new strategy for SIGINT operations in Mexico. Crossovers in government have led to mapping criminal networks from the "in-out". Crossovers are identified communicating with extenders, who then speak with communicators, who communicate with the rest of the network, allowing SIGINT to map a structure.

The headless nature of an all-channel network makes it very difficult to identify that a network even exists, let alone what it looks like. It is easier for SIGINT to identify the

⁶² Ellingwood, Ken. "Mexico Traffickers Bribed Former Anti-Drug Chief." *Los Angeles Times*. 22 Nov 2008. Internet. <http://www.latimes.com/news/nationworld/world/latinamerica/la-fg-bribe22-2008nov22,0,5384359.story>

⁶³ Burton, Fred and Stewart, Scott. "Counterintelligence Implications of Foreign Service National Employees." *Stratfor*. 29 Oct 2008. Internet. http://www.stratfor.com/weekly/20081029_counterintelligence_implications_foreign_service_national_employees

crossovers and work backwards. This also places emphasis on those criminal networks which are powerful enough to exert influence over the government.

This approach would help disrupt the Beltran-Leyva Cartel in Monterrey. The head of operations, Omar Ibarra, and multiple other network members were arrested after SIGINT intercepted communications between the Cartel and a mayoral candidate.⁶⁴ The identification of extenders and crossovers helped lead to Omar Ibarra. He would then identify other actors in the network, policemen who were corrupted, and the location of drug-distribution points. The application of SIGINT created the conditions for further successful intelligence collection.

SIGINT and its ability to increase the effectiveness of other types of intelligence collection resulted in the capture of Carlos Beltran Leyva and death of Arturo Beltran Leyva.⁶⁵ Like Gacha before him, Arturo was monitored communicating with prostitutes on his cell phone before a raid. The capture of members of his network had also created the paranoia which led to his split from the Sinaloa Cartel, and its boss Joaquin “El Chapo” Guzman Loera.

SIGINT is providing the intelligence necessary for Mexico to disrupt criminal Netwar networks, and in the case of the Beltran Leyva Cartel, decapitate it.

Mexican Netwar Lessons

1. Netwar Networks Evolve

⁶⁴ Soldiers Nab Ex-Elite Cop Who Trained Hit Men in Northern Mexico.” *Latin American Herald Tribune*. 27 Jun 2009. Internet. <http://www.laht.com/article.asp?CategoryId=14091&ArticleId=338053>

⁶⁵ Booth, William. “Mexican Agents Arrest Brother of Beltran Leyva.” *Washington Post*. 4 Jan 2010. Internet. <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/03/AR2010010300390.html>

Mexican narco-trafficking organizations have built upon the increasing evolutionary nature of Netwar networks. The Medellin Cartel demonstrated an evolution towards a hybrid network design, while Mexican cartels have evolved into highly hybrid or all-channel networks.

The lack of centralized authority in all-channel networks makes them hard to identify, and even harder to map. The Beltran-Leyva example suggests that monitoring government forces and first identifying crossovers makes identification and mapping of a criminal network easier. All-channel networks cannot be defeated. Mexico has learned that the criminal Netwar networks which most heavily influence the state should be the primary target. Identifying crossovers and mapping a network outwards, is the best strategy to disrupt criminal Netwar networks in an all-channel environment.

2. It Takes a Network to Defeat a Network

Netwar theory describes an interagency, networked approach as the best strategy to defeat criminal networks. Mexico and the United States created a SIGINT system which has multiple mechanisms to limit the dissemination of information, compartmentalize information, and enforce cooperation with other agencies. Although not close to an all-channel network, communication has increased between government agencies. Both Mexico and the United States are working together to reduce criminal Netwar networks' ability to exploit multiple jurisdictions and adapt to new profit centers.

3. Increase Communication and Operational Costs

The Communications Intercept System has increased the cost of communication within criminal Netwar networks. All electronic forms of communication can be monitored, and criminal networks have to prevent the interception of their messages. This directly or indirectly

affects the four strengths of a Netwar network: organization, doctrine, communications technology, and social ties. Forcing stress on these four pillars can make operations more difficult, and results in losses to competitors.

All-channel Netwar networks are still able to avoid some interception, due to their diffuse and changing relationship between actors, and limited resources of the state. This results in an increase in communication costs due to paranoia, but not disruption. Disruption enables law enforcement to exploit mistakes that wouldn't have otherwise been made, or can be used to focus in on particularly important actors and networks.

Considerations

Interference

Mexico is historically sensitive to U.S. interference in its domestic affairs. The Mexican government has vowed to combat narco-trafficking organizations on their own. The U.S. plan to embed Drug Enforcement Agency members into Mexico's Federal Police was decisively crushed by the Mexican Ambassador to the United States.⁶⁶ The United States and other powers that may contribute SIGINT assets to other countries must be aware of the consequences. An interagency, networked approach may be unrealistic if one state does not trust the intentions of another. The United States has access to the SIGINT collected by the Communications Intercept System, which monitors Mexican government offices. This level of intelligence sharing is much deeper than many nations would accept.

⁶⁶ Booth, William. "U.S. to Embed Agents in Mexican Law Enforcement Units Battling Cartels in Tijuana." *The Washington Post*. 24 February 2010. Internet. <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/23/AR2010022305560.html?hpid=topnews>

CNN. "U.S. Says Agents Won't Embed With Mexican Police." *CNN*. 24 February 2010. Internet. <http://www.cnn.com/2010/WORLD/americas/02/24/mexico.us.agents/index.html>

Risk of Abuse

The Colombian intelligence agency Departamento Administrativo de Seguridad (DAS) has recently been implicated in a scandal regarding the use of SIGINT against opponents to President Uribe.⁶⁷ Mexico faces the same potential for abuse, despite strict laws concerning warrants necessary for SIGINT collection. U.S. law enforcement and intelligence oversight is attempting to minimize abuse that may prove inevitable. The Mexican Senate already accused CISEN of spying on them in 2008.⁶⁸ The emergence of death squads utilizing SIGINT in a fashion similar to Los Pepes would be a significant failure of the Communications Intercept System. SIGINT can be a double-edged sword.

Conclusion

Netwar theory describes the characteristics of criminal networks and their evolution in structure during the information age. The Medellin Cartel and Mexican narco-trafficking organizations both verify this theory. The Medellin Cartel was replaced by a more hybrid Netwar network in the form of the Cali Cartel. Mexican narco-trafficking organizations have taken over from the Colombians, utilizing the strengths of all-channel networks.

Netwar theory describes the impact of the information age on non-state actors. The information age has allowed criminal networks to evolve into more flexible, adaptable, and stronger designs. This evolution is contingent on the ability to communicate between actors in

⁶⁷ Semana. "The DAS is Still Recording." *Semana*. 21 February 2009. Internet. <http://www.semana.com/noticias-nacion/das-sigue-grabando/120991.aspx>

⁶⁸ Merlos, Andrea. "CISEN Advisor to Congress Lied." *El Universal*. 11 July 2008. <http://www.eluniversal.com.mx/notas/521735.html>

an all-channel network. This weakness can be exploited. SIGINT disrupts or increases the cost of communication in a criminal Netwar network.

Additional References

Astorga, Luis. "Mexico: Its Democratic Transition and Narco-Terrorism." *Canada Watch*. Universidad Nacional Autónoma de México, Special Edition Spring 2009. Print.

Berestein, Leslie. "More Federal Law Enforcement, But More Violence." *San Diego Union-Tribune*, 4 Jan. 2009. Internet.
<http://www3.signonsandiego.com/stories/2009/jan/04/n92388113654-more-federal-law-enforcement-more-vio/>

Cornelius, Wayne and Shirk, David. Reforming the Administration of Justice in Mexico. Notre Dame: Notre Dame Press, 2007. Print.

O'Neill, Shannon. "The Real War in Mexico." *Foreign Affairs* 88.4 (2009): 63-79. Print.

Sarre, Miguel. "Challenges Associated with the Judicial Reform." Woodrow Wilson International Center. Internet.
<http://www.wilsoncenter.org/news/docs/Sarre%20report.pdf>

Tokatlian, Juan Gabriel. "Preventing a Pax Mafiosa in the Americas." *The Fletcher Forum of World Affairs* 31.2 (2007): 57-67. Print.