Information Superiority: Law Enforcement vs. Transnational Criminal Organizations

Marwan Al-Zarouni

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
E-mail: marwan@marwan.com

Abstract

New types of crimes and criminal organizations emerge from the knowledge age bringing with them a set of new challenges for law enforcement agencies. One type of these organizations is Transnational Criminal Organizations (TCOs). This paper will discuss the concept of information superiority and the network centric concept and how they relate to law enforcement agencies. It will also discuss the form and structure of both, TCOs and law enforcement agencies and the effect of that form on their operations. It will also discuss emergent technologies and trends such as cybercrime and its effects on both TCOs and law enforcement. It will also outline how traditional hierarchies can fail in fighting TCOs. The paper will then define the structures and technologies needed to be embraced by law enforcement in order to compete with TCOs. Finally, the paper will outline some of the methods in which to analyse effective law enforcement practices and inter-organizational effectiveness.

Keywords

Law Enforcement, Cybercrime, Organized Crime, Information Warfare, Transnational Criminal Organizations (TCOs), Information Superiority, Network Centric Organization, Sociometry.

INTRODUCTION

The classical example of the continuous battle between good and evil is the example of "cops and robbers". Whenever cops were able to solve crimes and catch criminals in a certain way, robbers would manage to find a new way of going about their business and evade being caught. This eternal battle between cops and robbers has taken a whole new dimension in the knowledge age. An age in which knowledge is power and whoever achieves information superiority gains ultimate power.

DEFINING INFORMATION SUPERIORITY

The basic concept of information superiority is "the ability to use cyberspace while denying or exploiting your opponent's use of it" (Jacobs, 1997). Information superiority requires the "capability to collect, process, and disseminate an uninterrupted flow of information" (DoD, 2002). Information superiority is therefore reliant on organizational efficiencies and is based on speedy and efficient information systems, both of which are at the core of the network centric concept.

DEFINING ORGANIZED CRIME

Organized Crime is "criminal activities organized and coordinated on a national scale, often with international connections. These corporate criminal organizations are often protected by corrupt politicians and law enforcement officers, and legal advice; they profit from such activities as gambling, prostitution, and the illicit use of narcotics (Lagasse, Goldman, Hobson, & Norton, 2003)".

TCOs – Form and Structure

Organized crime has traditionally only greatly affected certain states such as Italy, the United States and Japan. It was in most cases limited in reach to the national level. In the last few years, however, organized crime has evolved into a new form referred to as Transnational Criminal Organizations (TCOs). This evolution was a natural consequence of many events and global changes that occurred. One such event is the end of the cold war and the collapse of the justice system in the former Russian State. Also, the breakdown of barriers between east and west and the development of free trade areas in Western Europe and North America and the emergence of global financial and trading systems have all contributed to forming an ideal environment to incubate TCOs (Williams, 1995).

TCOs are ideally suited to exist and prosper in international systems due to their networked form and structure (Ibid). TCOs are highly evolutionary and flexible in nature and adapt sophisticated hybrids of all-channel, star, and chain network structures. They continually exploit trends that enhance interconnectivity among their nodes and often form odd alliances and partnerships that ensures their survivability (Arquilla & Ronfeldt, 1996,p 61). An excellent example of the embracing of new technologies by TCOs is their involvement and participation in cybercrime.

TCOs and Cybercrime

TCOs are exceptionally adaptive to change and continually seek new opportunities for new illegal enterprises and activities. Therefore, the evolution of the Internet and e-commerce represented TCOs with an ideal environment to exploit and offered TCOs enormous new prospects for illicit profits (Williams, 2001).

The transnational nature of the Internet offered TCOs with a transparency in location. This gave TCOs the opportunity of remotely carrying out businesses in strong states that they could not have been able to exist or prosper in previously. All this while physically residing in weaker states that shielded them from the reach of the law. This offers TCOs with a high degree of protection and reduces their risk of being prosecuted (Shelley, 2003, p. 303-312).

Unlike traditional organizations, TCOs do not need to develop technical skills to exploit the Internet for profit. All they do is hire individuals from the hacking community to do the job for them. These individuals are subjected to the traditional criminal system of rewards and punishments to carry out tasks for the TCOs and provide the technical expertise needed to carry out cyber-criminal acts (Williams, 2001). The location of these individuals is irrelevant due to the global nature of the Internet. Often, TCOs seek technical expertise from individuals residing in the former Russian states or the Indian subcontinent. While some of these individuals work for the TCOs willingly, others are unaware of their employers, whereas others just do it because well-paid legitimate employment in their field of expertise is rare in their region of the world (Shelley, 2003, p. 303-312).

The Internet is used by TCOs as an instrument and medium for many organized-crime activities be it traditional or cutting edge. These include all kinds of theft, whether from online banks or of intellectual property, fraud, exploiting vulnerabilities relating to communications for profit, or as targets for extortion (Williams, 2001).

The anonymity and instant communication features of the Internet greatly enhance its value for TCOs. It offers them with an ideal medium for both secure and mass communications. The Internet technology therefore heightens and enhances the network centric concept that serves TCOs well and facilitates their communication activities.

DEFINING LAW ENFORCEMENT

Law Enforcement, or police, is “an organizational system consisting of public and private agents concerned with the enforcement of law, order, and public protection. In modern cities their duties cover a wide range of activities, from criminal investigation and apprehension to crime prevention, traffic regulation, and maintenance of records (Lagasse et al., 2003)”.

Law Enforcement – Form and Structure

The form and administration of the police system varies in different countries. In Europe, especially on the Continent, it tends to be centralized. In the United States however, there is decentralization. Metropolitan police have the widest functions, and state police are chiefly concerned with traffic control and rural protection (Ibid). In the Middle-East and North Africa, a mixture of both centralized and decentralized administration exists.

The fight against crime on the international level is coordinated by the International Criminal Police Commission, popularly known as Interpol. Interpol is basically a worldwide clearinghouse for police information. The Interpol however, does not apprehend criminals directly. Also, Interpol often avoids involvement in crimes that deal with political, military, religious, or racial matters. The Interpol however, has been most successful with regard to counterfeiting, forgery, smuggling, and the narcotics trade (Ibid).

Arab Interior Ministers' Council (AIMC) is the Arabian equivalent of Interpol and has similar principal services for its member countries in the Middle-East and North Africa. AIMC and Interpol collaborate together and have signed a memorandum of understanding in 1999 that governs mutual consultation and co-ordination, exchange of information, reciprocal representation, technical co-operation, and entry into force, its modification and duration (Interpol, 1999).

The form of police at all levels including local, national, regional, and international is far from the network centric form. It is heavily based on bureaucracy and is highly hierarchal. Even police operations and activities are highly hierarchal in nature.

Law enforcement agencies by nature are very territorial and heavily rely on jurisdictions. Even in small countries were there are no borders between states and cities within those states, jurisdictions are highly enforced and respected by law enforcement professionals. Information disclosure and flow between those states is highly filtered and restricted at a high level.

An example of police jurisdiction and how it affects information flow is the use of search warrants in policing. For example, if a company is suspected of illegal activities, and it is functions at the national level, local law enforcement does not have the right to uncover records of information on their activities in other states even with a local police warrant and a separate warrant for those records is usually requested from other states. This slows down and sometimes disrupts information flow and therefore does not facilitate information superiority.

Law Enforcement and Cybercrime

An excellent example of law enforcement's resistance to change and adaptation of new technologies is the example of law enforcement's reaction to cybercrime. Until today, jurisdiction issues still exist and Internet is highly unregulated. Regulating the Internet is not an easy task, especially when you factor in issues of privacy and the reliability of digital evidence. The international nature of the Internet and the lack of harmonize national laws adds to the task's complexity.

International cooperation in law enforcement in regards to cybercrime is currently being handled through a series of extradition and mutual legal assistance treaties (MLATs). These treaties allow law enforcement agencies to share information and evidence with each other on the international level. For MLATs and extradition treaties to go into effect there is usually a requirement of dual criminality. This means that the cybercrime involved must be designated as a crime in both jurisdictions, which is not usually the case. In other words, international cooperation is enormously facilitated by convergence of what is criminalized in national jurisdictions (Williams, 2001). This brings us back to the classical issue of jurisdictions.

Law Enforcement vs. TCOs - Hierarchy vs. NCOs

Hierarchies have a difficult time fighting networks. This has been historically proven in many conflicts in the past. One of the best examples relating to law enforcement versus TCOs is found in the failings of many law enforcement agencies to defeat transnational criminal cartels engaged in drug smuggling, as in Colombia. This demonstrates both the defensive and offensive robustness of the network form and the failure of traditional hierarchal structures in facing them (Arquilla & Ronfeldt, 2001, p15).

COUNTER NETWAR BY LAW ENFORCEMENT

It takes networks to fight networks (Ibid). This means that in order for law enforcement agencies and supporting organizations to achieve information superiority over TCOs they may have to adopt organizational designs and strategies like those of the TCOs.

This does not mean however mirroring the TCOs, but rather learning to draw on the same design principles that TCOs rely on for information superiority. These principles depend to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially by building new mechanisms for inter-agency and multi-jurisdictional cooperation (Ibid). This must include changing the mindset of law enforcement organization officials especially at the top levels from being concerned with information security and protection to being more concerned about effective information sharing and heightened shared awareness between agencies.

Whoever masters the network form first and best will gain major advantages (Ibid). In the case of law enforcement versus TCOs, it is apparent that TCOs are enjoying an increase in their power relative to law enforcement agencies. The early adaptation of the network form by TCOs allows them to compete and frequently have an information advantage over law enforcement and their supporting agencies.

This puts law enforcement agencies at a disadvantage point with regards to information superiority. For law enforcement to compete with TCOs in the Infosphere requires co-evolution in law enforcement's organization, doctrine, and technology.

Changes Needed by Law Enforcement

Changes in law enforcement should be at all levels. There should be intra-organizational, inter-organizational changes and at both, national and international level. These changes should rely on network centric approaches and structures. This does not however imply that hierarchy and hierarchal structures should be overhauled or removed altogether. But rather, there should be hybrids of both hierarchy and network forms. The challenge however is to come up with the perfect blend of both forms of organization to create an all-powerful structure that will not only serve as a competitor in the information sphere but rather dominate the information space and achieve information superiority.

This could be an unnatural and complex task for law enforcement as the environment in which it operates emphasises territorial type of authority. But with the emergence of the knowledge age, all this is about to change as law enforcement agencies are forced to cooperate and share information and sign agreements that facilitate and encourage effective and speedy information flow and sharing.

Improving structure and form of law enforcement agencies to facilitate the assimilation of critical information and its quick and secure delivery precisely when and where it's needed involves some changes like the ones listed below:

- Operational chains should be reviewed and made into more efficient chains with use of smaller operational chains and less hierarchal overheads. This involves giving more power and responsibility to operators at the lower end of the chains as well as providing them with current operational knowledge that gives them a heightened situational awareness.
- Trying to combat the heads of criminal organizations can prove to be ineffective against TCOs as these organizations are essentially hydra-headed. Kill one node and another one, or more, can pop up as replacements. A more effective way to combating them is combating the nodes at the operational level.

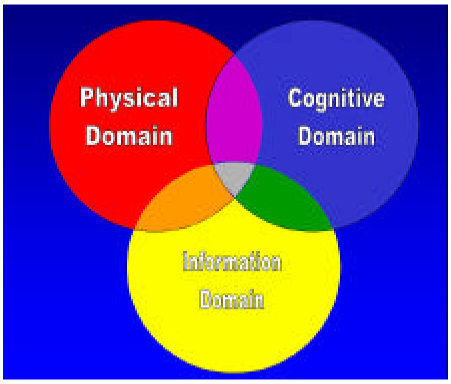

Figure 2: Domain Warfare domains (Folientitel, 2003).

- The concept of "Domain Warfare" should be employed by law enforcement. The idea of which is to affect the information domain in order to achieve desired effects in the physical and cognitive domains which serves as a contribution to effects based operations. Information has three basic functions: It is basis for the human cognition, it establishes knowledge and it is required for the automation and functionality of high-technology systems (Ibid). Affecting Information can therefore produce effects on the human cognition, available knowledge, and the functionality of systems as shown below:

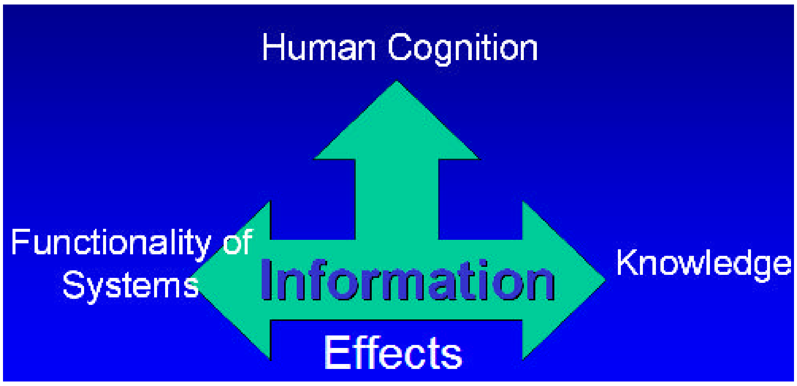

Figure3: Affecting the information domain leads to effects on human cognition, available knowledge and the functionality of systems (Ibid).

- Task forces and Ad-hoc teams should be created on demand to combat TCOs.
- Just-in-time tactics and convergent systems should be adapted by law enforcement. The effectiveness of these tactics is highly dependent on time. Thus, effort should be made to minimize down-time and increase operational tempo of convergent systems.
- Outsourcing of information technology expertise should be utilized. The physical location of such expertise is irrelevant as technologies such as the Internet can facilitate their use.
- Alliances with the industry and especially I.T. companies should prove very helpful in combating TCOs as these types of industry can provide technical assistance and cutting edge technologies and enormous resources that can benefit law enforcement in combating TCOs.
- Transparency, trust and careful information sharing between financial institutions and law enforcement can have an astonishing impact in identifying TCOs financial resources and combating money laundry and digital attacks on financial institutions. This is a difficult task as these institutions are usually hesitant in disclosing client information and also tend to not report digital crime in fear of loss of customer trust.
- Alliances with intelligence agencies and defence departments should be made to improve information richness and reach.
- Unconventional alliances between nations that do not usually co-operate in law enforcement (such as China and the U.S.) will play a vital role in defeating TCOs. As TCOs usually reside in one of these countries and conduct their operations in the other to avoid apprehension.
- Technical assistance and training from stronger states to improve the criminal justice capacities of weaker states, and helping their law enforcement agencies in becoming more effective crime fighters can play a critical role in combating TCOs. Such assistance not only helps build a framework for international law enforcement cooperation, but also enhances the ability of weaker states to control their own crime problems before they extend beyond their borders and into stronger states (Swartz, 2001).

The following are some of the ways to improve operational effectiveness by the use of technological means that enhance the network centric form:

- Technologies that enable information sharing and collaboration between agencies should be adapted and fully exploited.
- Data warehousing and mining, trend analysis tools, and artificial intelligence should play a vital role in identifying and apprehending criminals.
- Grid computing should be used by law enforcement agencies to increase overall situational awareness for operators.
- Clustering technologies should be used by law enforcement agencies to increase overall computational power available to each of their operational nodes when needed. This provides computational power on-demand and reduces time in conducting calculation intensive tasks.
- Reappraisal of rules of evidence, search and seizure, electronic eavesdropping to cover digitized information, modern computer and communication systems is a must (Williams, 2001). In addition to appropriate laws, it is also important that law enforcement agencies develop the capacity to implement such laws.

NYPD: A Success Story

In 1994, the New York Police Department (NYPD) underwent a dramatic change in organization, doctrine, and technology. This change significantly improved its operational effectiveness in fighting crime in all of its seventy eight precincts (Cebrowski, 1998).

This enormous success was due to changing the primary objective of the NYPD from focusing exclusively on big offenders, to focusing more on the operational level of criminal activities. This involved cracking down on petty crime, improving the physical environment, and removing guns from the streets. To do so, the police commissioner provided each of his precinct commanders with substantial operational authority to change doctrine, procedures, and organization, and held them accountable for their results. This changed the previously highly hierarchal police department into smaller “nodes” or operational units that operated in their perspective precincts. This dramatically increased their effectiveness in fighting crime (Ibid).

Information technology was effectively adapted by NYPD and increased competitive space awareness and created a common operational picture in each precinct and across precincts. Information sharing was required of all elements of the arrest-to-arraignment chain. This led to an increased awareness among all the members of a chain involved with any particular crime (Ibid).

The result of co-evolution of organization, doctrine, and technology in NYPD was the emergence of speed of command as a decisive operational capability. This enabled precinct commanders and their officers to identify trends much earlier and to take action to stop crimes before they occur (Ibid).

ANALYSING THE NETWORK FORM

Evaluating the effectiveness of inter-agency or intra-agency communication can become a complex task. It can be extremely difficult to measure success in adapting network centric methodologies and approaches without sound and proven measurement techniques.

Communication is highly a sociological issue. TCOs were historically reliant on tight kinship and trust coupled with loosely knit network structures to prosper over empires and early states (Arquilla & Ronfeldt, 2001). Some organizations like the AIMC and the Tampa Bay Economic Development Organizations use Social Network Analysis (Sociometry) as a way of analysing communication networks (Hagen, 1997). Sociometry studies the structural forms and relational contents that connect actors in complex networks spanning multiple levels of analysis (Knoke, 2003). Sociometry was selected by many law enforcement organizations as a way of analysing communicational effectiveness for its strength in assessing communication, relations, and cooperation, and inter-organizational environments. Sociometry can help law enforcement agencies in evaluating their own organizations and it can also be used as a tool in identifying and analysing structures and communicational effectiveness of organized crime and TCOs.

Another indicator of success of law enforcement in adapting network centric principles is crime rate statistics. A good example of that is the dramatic drop in crime rates in NYPD as a result of co-evolution of organization, doctrine, and technology. In New York, and over the period between 1993 and 1996, murder and non-negligent manslaughter dropped by almost half, robberies fell by nearly 43%, auto theft dropped by 47%, and felony assault by 25.65% (Cebrowski, 1998).

CONCLUSION:

In the knowledge age, change is inevitable, only those who adapt and embrace change will survive. In the information superiority race, TCOs seem to have fully adapted and embraced emergent technologies and law enforcement seems like it is still catching up. TCO's participation in cybercrime does not have to go unpunished, and there are already cases where international cooperation has been very effective. Indeed, successful cooperation can breed emulation and further success (Williams, 2001).

The race between law enforcement and TCOs for information superiority has just started and even though criminals got a head start in this race, this eternal race between cops and robbers will continue and once again law enforcement will eventually be able to stop more avenues for TCOs to prosper in. In this race however, there is no finish line, and only a timely information advantage can be achieved. Who gets that information advantage will ultimately be dependant on their operational efficiency in the physical, information, and cognitive domains.

REFERENCES:

Arquilla, J., & Ronfeldt, D. (1996). *The Advent of Netwar.* Santa Monica, CA: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND Corporation.

Cebrowski, A. K. (1998, January). Co-evolution: New York Police Department. *United States Naval Institute's Proceedings Magazine, 124/1/1,139*.

DoD. (2002). *Dictionary of Military and Associated Terms (JP1-02)*. Wasjongton, D.C.: Joint Chiefs of Staff.

Folientitel, K. (2003). *German Information Operations Initiatives*. Retrieved 11-April-2004, from www.act.nato.int/transformation/cde/cde03presentations/nhorizons_geinfops02_bo05nov.ppt

Hagen, G. (1997). An Analysis of Communication Networks Among Tampa Bay Economic Development Organizations. *Connections: Official Journal of the International Network for Social Network Analysis, 20*(2), 13-22.

Interpol. (1999). *Memorandum of understanding between the International Criminal Police Organization-Interpol and the General Secretariat of the Arab Interior Ministers' Council*, from http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/Arabministercouncil1999.asp

Jacobs, D. (1997). Attacks in Cyberspace a Lethal Threat. *Chips Magazine, April 1997*.

Knoke, D. (2003). *Intra- and Interorganizational Networks*. Retrieved 11-April-2004, from http://www.soc.umn.edu/~knoke/pages/INTRA-_&_INTERORGANIZATIONAL_NETWORKS.ppt

Lagasse, P., Goldman, L., Hobson, A., & Norton, S. R. (2003). *The Columbia Electronic Encyclopedia*. Farmington Hills, MI: Gale Group.

Shelley, L. I. (2003). Organized Crime, Terrorism and Cybercrime. In P. H. Fluri & A. Bryden (Eds.), *Security Sector Reform: Institutions, Society and Good Governance*. Baden Baden: Nomos.

Swartz, B. (2001). Helping the World Combat International Crime. *Global Issues: An Electronic Journal of the U.S. Department of State, 6*(2).

Williams, P. (1995). Transnational Criminal Organizations: Strategic Alliances. *The Washington Quarterly, 18*(1), 57-72.

Williams, P. (2001). Organized Crime and Cybercrime: Synergies, Trends, and Responses. *Global Issues: An Electronic Journal of the U.S. Department of State, 6*(2).

COPYRIGHT