Crime Analysis & Investigation

Academic paper by Peter John Lynch (PJL) of Lynch Investigations & Countermeasures Pty Ltd.

Grad. Cert. Fraud Investigations (CSU)
Adv. Dip. Gov Fraud Control Management
Adv. Dip. Security Risk Management
www.pjlinvestigations.com.au

Introduction

Initiation of proactive investigations into cybercrime & terrorism should be advancing with the use of crime analysis and investigative practice that achieves positive outcomes.

There is evidence that cybercrime & terrorism has shown trends in the past where a proactive investigative and analytic approach has not always been utilised. Investigators need to apply technology to their working practices using a proactive approach and thereby limit the opportunities for those who commit offences.

Preparedness and prevention are the key points to the successful application of today's needed analysis and investigative practices. Crime analysis and investigative practice should be applied with a strategic approach using crime analysis tools from crime mapping and crime profiling applications.

There are databases containing information relating to profiles that hold crime offender's identity that needs analysing. There are needs to examine the crime related locations and to determine crime hot spots.

Crime mapping and criminal profiling are extremely useful methodologies in assisting the investigator to take a strategic approach using crime analysis and investigative practices to achieve positive outcomes with terrorism and cybercrime.

Terrorism

In the US in the early to mid 1990's there had been a large number of terrorist incidents. In 1993 there was the World Trade Centre bombing as well as a foiled plot to bomb US commercial aircraft transiting the Far East in 1995.

The World Trade Centre bombing involved a bomb laden van being driven into the parking garage of the World Trade Centre. In respect of this incident it is considered that proactive investigative practices were not occurring so much at that time, thus the opportunities were not limited for the terrorist attackers.

More terrorist attacks for example the Oklahoma City bombing and twenty-one individuals convicted of charges relating to the 1996 Montana Freeman siege. On August 7, 1998 in East Africa there were the US Embassy bombings. This attack was initiated by FBI on a particular physicist by the name of Lawrence A. Maltz who had been sending letters to the director of the FBI the US Department of State, the International Revenue Service, members of congress and the President.

Investigators revealed Maltz had contacted chemical companies regarding purchasing other agents that produce a nerve agent similar to sarin, investigations continued. Maltz had to temporarily relocate to Richmond, Virginia (FBI 1998).

US Department of Justice (1998, p.6) stated 'on April 8, 1998 FBI & associates arrested Maltz on warrant for violation of Title 18 of the US code (USC) Section 2332a (Threat to use a Weapon of Mass Destruction). Maltz agreed to questioning & pleaded guilty to a lesser charge – violating 18 USC 875 (Mail Threatening Communications).'

US Department of Justice (1998, p.6) stated 'on October 10, 1998 a US district judge sentenced Maltz to 16 months federal incarceration, followed by three years supervised release and ordered $3,000.00 fine maximum sentence allowed under federal sentencing guidelines.'

The example demonstrates the real and imminent threat by Maltz to society revealed through the initiation of ongoing strategic investigations. The crime analysis for the matter achieved positive results. The lead enabled the FBI Investigators and associates to continue with there strategic approach.

Terrorist attacks may not have leads due to the secrecy of the terrorist group's activities unlike the Maltz matter where leads allowed for a strategic approach to investigate and analyse the terrorist's activities for an arrest to occur.

By the year 1998 in the US ongoing strategic investigations were preventing acts of terrorism. Sentencing of offenders was occurring from past terrorist attacks and association to the crimes.

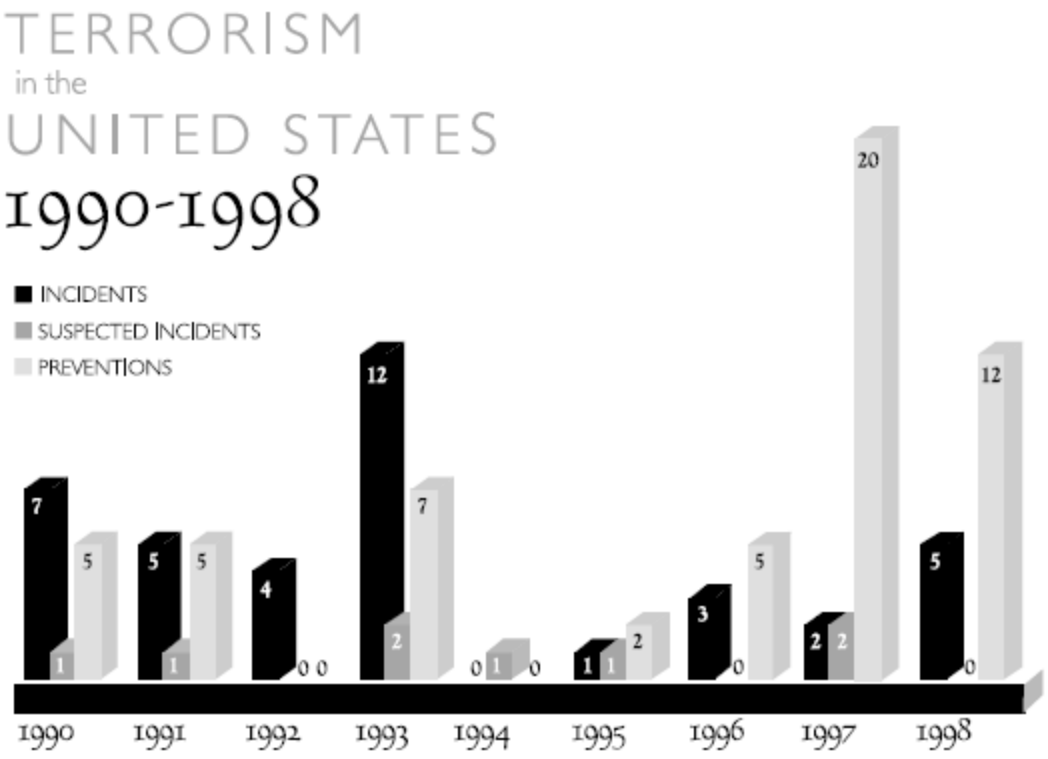
US Department of Justice (1998, p.7) stated, 'on October 29, 1998 the jury found Johnnie Wise & Jack Abott Grebe, Jr guilty of two counts of threatening to use a weapon of mass destruction' targeting a local court judge with a device involving the Aids virus, Rabies and the biological agent Anthrax. Oliver Dean Emigh was acquitted as it was unclear if he had knowledge of the plot. Strategic investigations and crime analysis activities occurred prior to allowing a disastrous advent to occur.

US Department of Justice (1998, p.9) stated 'on April 1998, Eyad Mahmaud Ismail Najim was sentenced to two hundred and forty years in prison with no chance of parole for the 1993 February World Trade Centre bombing. Najim was found guilty of driving the explosive laden van into the World Trade Centre.'

US Department of Justice (1998, p.10) stated 'in addition to this in 1998 there was sentencing of Terrell P. "Terry" Coon for in 1996 he was found to be plotting to blow up the FBI Clarksburg fingerprint facility in 1996; the list goes on as there were at least another eight major convictions for terrorist offences in the US in 1998.'

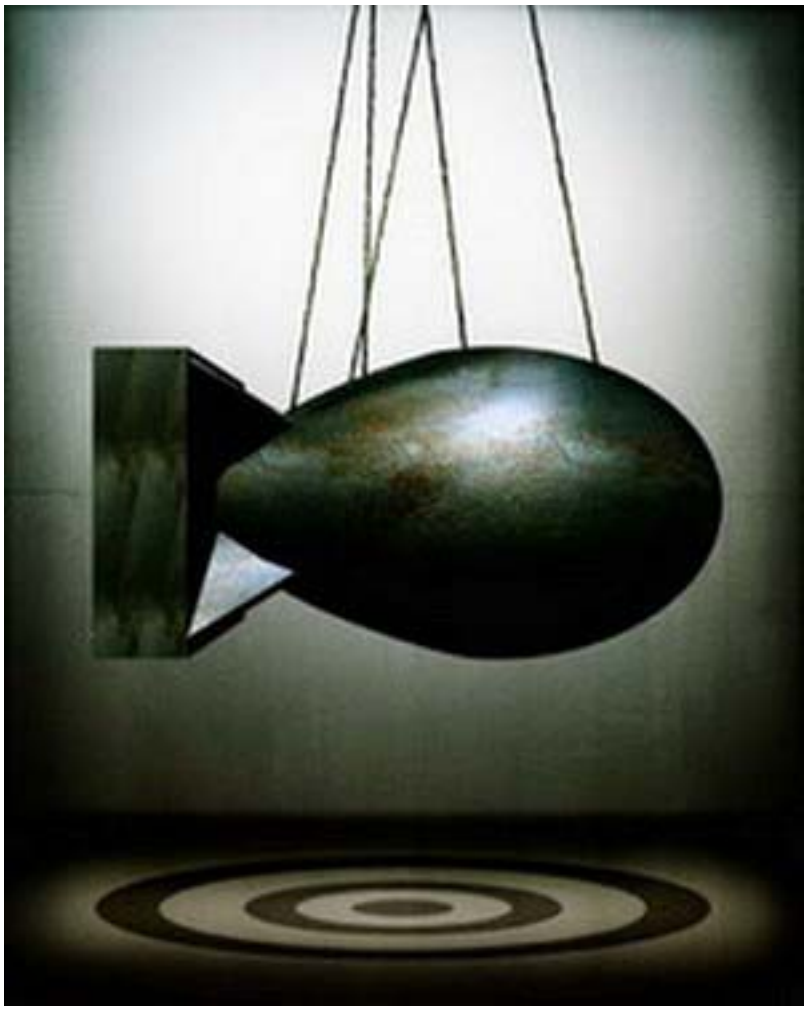
The reactive approach, of which the investigations have occurred, has placed notorious criminals behind bars away from the public. The imprisonment provides society with some justice while maintaining security of the world's most vulnerable targets.

Throughout the early 1990's to the mid 1990's it can be observed from the bar graph statistics below, that very little terrorist prevention occurred in proportion to the terrorist attacks that occurred in the US. This certainly shows a trend towards incident driven investigations not assisting with detecting & preventing the terrorist attacks on society that did occur through the early years of the 1990's.



TERRORISM IN THE UNITED STATES 1998

Source: US Department of Justice, Federal Bureau of Investigation.



CHRONOLOGICAL SUMMARY OF INCIDENTS IN THE UNITED STATES 1990-1998

DATE	LOCATION	INCIDENT TYPE	GROUP
1-12-90	Santurce, P.R.	Pipe Bombing	*Brigada Internacionalista Eugenio Maria de Hostos de las Fuerzas Revolucionaries Pedro Albizu Campos* (Eugenio Maria de Hostos International Brigade of the Pedro Albizu Campos Revolutionary Forces)
1-12-90	Carolina, P.R.	Pipe Bombing	*Brigada Internacionalista Eugenio Maria de Hostos de las Fuerzas Revolucionaries Pedro Albizu Campos* (Eugenio Maria de Hostos International Brigade of the Pedro Albizu Campos Revolutionary Forces)
2-22-90	Los Angles, Calif	Bombing	Up the IRS, Inc.
4-22-90	Santa Cruz County, Calif.	Malicious Destruction of Property	Earth Night Action Group
5-27-90	Mayaguez, P.R.	Arson	Unknown Puerto Rican Group
9-17-90	Arecibo, P.R.	Bombing	Pedro Albizu Group Revolutionary Forces
9-17-90	Vega Baja, P.R.	Bombing	Pedro Albizu Group Revolutionary Forces
2-3-91	Mayaguez, P.R.	Arson	Popular Liberation Army (PLA)
2-18-91	Sabana Grande, P.R.	Arson	Popular Liberation Army (PLA)
3-17-91	Carolina, P.R.	Arson	Unknown Puerto Rican Group
4-1-91	Fresno, Calif.	Bombing	Popular Liberation Army (PLA)
7-6-91	Punta Borinquen P.R.	Bombing	Popular Liberation Army (PLA)
4-5-92	New York, N.Y.	Hostile Takeover	*Mujahedin-E-Khalq* (MEK)
11-19-92	Urbana, Ill.	Attempted Firebombing	Mexican Revolutionary Movement
12-10-92	Chicago, Ill.	Car Fire and Attempted Firebombing	Boricua Revolutionary Front (two incidents)
2-26-93	New York, N.Y.	Car Bombing	International Radical Terrorists
7-20-93	Tacoma, Wash.	Pipe Bombing	American Front Skinheads

Source: US Department of Justice, Federal Bureau of Investigation.

The World Trade Centre & the Pentagon in the US on September 11, 2001 and the attacks in Bali on October 12, 2002 introduced a new and confronting dimension to international security. The Australian Government knows that Al Qaida had an active interest in carrying out a terrorist attack in Australia before September 11, 2001 and that we remain a target today.

The Australian Government takes a good view that strong intelligence capabilities are fundamental to the effectiveness of our national counter terrorism arrangements (Australian Government 2004).

Preparedness and Prevention

This is in fact how crime analysis and investigation using a proactive approach can assist to identify the threats and risks of terrorism to this country and to determine the necessary proactive arrangements to be implemented, by the use of strong intelligence capabilities.

The legislative framework of Australia has been strengthened to enhance the capacity of intelligence and law enforcement agencies to detect, investigate, & prosecute terrorists, terrorist organisations and those who seek to train and associate with terrorist groups. There is now a better intelligence capability to detect and disrupt terrorist activity, including through the obstruction of terrorism financing.

It has been known that money laundering has been a source of funds used to assist in the resources used in terrorism.

Forensic accounting and forensic cybercrime investigations are practices that can be used, using a proactive approach to detect and prosecute for funds being supplied to be used for terrorist activities. A proactive investigative strategy is required to be applied for detecting and monitoring these clandestine activities to prevent the horrific attacks that the world has suffered through the many and devastating attacks of terrorism.

The use of crime analysis and investigative practices between Australian law enforcement agencies is needed to investigate and disrupt money laundering via alternative remittance systems, consistent with legislative requirements.

By sharing information and intelligence on money laundering methods, this can improve law enforcement efficiency and effectiveness in combating organised crime. The existing and emerging criminal methodologies need to be understood through detection and investigations. The exchange of information on money laundering methods aids law enforcements understanding and assists all agencies to better position themselves to combat criminal activity, which is funds sourcing supply for resources for terrorist activities.

It is a requirement of law enforcement to combine knowledge of money laundering, tax evasion methodologies and investigative techniques in staying abreast of the latest crime analysis and investigative strategies to be used to combat money laundering systems that secure global terrorism.

In particular areas of money laundering through remittance systems it is a requirement of our investigators and law enforcement personnel to apply a strategic approach to achieve positive out comes through financial investigations.

Cybercrime

Crime analysis and the most current investigative practice must be used in the cybercrime environment continually as new patterns in cybercrime are developing periodically. There are issues with the introduction of crime prevention measures and the creation of new opportunities.

The introduction of credit cards has created a wave of crimes. The availability and access to credit card numbers via computers and the internet has been damaging to banks and retailers.

Where new security measures have been introduced in particular countries, offenders may choose to go to other countries with less sophisticated security. This is another reason criminal analysis and investigative practices must take a strategic technological approach and move to the areas where cybercrime is more likely to occur. The investigative and law enforcement personnel and teams need to take a proactive approach to move

in on the crimes that have been displaced, while keeping informed of the current trends and patterns from a crime analysis perspective.

Crime analysis and investigative practices can achieve positive outcomes where jurisdictional crimes are occurring by investigation teams keeping up with the legislative changes, as the offenders may commit crimes in jurisdictions where the penalties for the crime being committed do not exist or legislative changes are occurring, that may or may not allow for the offenders to be arrested. Also the offender may not be able to be extradited for the offence due to legislative jurisdictional boundaries.

Smith, RG Wolanin, N & Worthington G (2003, p.2) stated 'Onel de Guzman, who allegedly propagated the "Love Bug" virus, was unable to be prosecuted in the Philippines because the Electronic Commerce Act which prohibits computer hacking only came into force after his actions took place and was not retrospective.'

Jiggins, S (2000, p.5) stated 'the rapid growth of internet crime from the internet and electronic commerce has the potential for huge increases in crimes of acquisition including fraud are a reality. Fraud has been found to be the most expensive crime in the Australian community costing around $3-$3.5 billion per year in monetary terms at 15.3 – 17.9 per cent of total crime cost (Walker 1997, p.6).

Exchange of intelligence is the key for assisting with best investigative practices and crime analysis with the coordination of investigation operations occurring locally and globally in combating the ever changing method of cybercrime techniques.

There should be more emphasis placed on increasing the role of the private sector being involved with government, community and law enforcement for the benefit of all parties. Ongoing investigations and analysis of the potential electronic crime environment would have to occur using a strategic approach towards cybercrime to identify current trends, emerging issues and problems in the electronic cybercrime environment.

Emerging issues can include increased miniaturisation, increasing global connectivity, improved cryptographic methods, potential difficulties posed by encryption.

There should also be a number of investigative tools for overcoming the variety of electronic systems. There is a requirement to monitor the potential impact of smart cards e-cash and stored wealth will be needed, as with the impact of global positioning systems and robots.

Information availability to the public has increased due to electronic technology including the potential to use the information from the internet for the manufacture of weapons of mass destruction.

By taking this strategic approach through crime analysis and investigation techniques, there are key aspects to consider for the future environment, these include reducing the cost of the internet, increasing the awareness of electronic evidence also rapidly increase storage capacity and to increase technical complexity, all positive aspects of a developing technological environment.

In many cases of computer crime an investigative analysis is required in real time tracing of internet communications across jurisdictional boundaries, to assist the process of tracing and tracking down sophisticated users who commit unlawful acts on the internet, while hiding there true identities. An investigative analysis in real time tracing needs to be used for gathering evidence useful for the prosecution of persons involved with cybercrime from these cases.

An example of the initiatives by the US includes National Infrastructure Protection Centre and computer squad teams. National cybercrime training partnerships and a computer analysis response team, including an Internet fraud complaint center.

The US would also be drafting a bill for key legislation to allow for the ability to retain and preserve data (Jiggins, S 2000).

Crime Analysis

Crime analysis is a valuable tool for the investigator that can be used to achieve positive outcomes when investigating terrorism & cybercrime. MJ, Palmiotto CSU Readings (1988, p.86) stated 'crime analysis is primarily concerned with the identification of short term patterns of criminal behavior or events and associated characteristics.' Crime analysis is more thoroughly used when a theoretical & practical approach is used.

There are various software programs that can be used to assist the investigator within there role of crime mapping, data mining and geographical profiling.

A department from within law enforcement will be directed by its crime analysis unit. The standard procedures require routine reports from the crime analysis unit. There must be a defined target area, time frame, trend or pattern before a report is filed to the operations unit. The operation's commander develops an appropriate plan of action when they receive a report if it is deemed appropriate.

Crime analysis and field operations can successfully achieve objectives & be effective, provided there is good communication & cooperation. Crime analysis is considered the keystone on a new approach for delivering police services (MJ, Palmiotto CSU Readings 1988).

MJ, Palmiotto CSU Readings (1988, p.88) stated 'by using the crime analysis model Sergeant Marvin Evans of the Newport News, Virginia Police Department tracked twenty-eight homicides in an eighteen month period that ended in July 1985.'

It was established that only a few cases were victims and murderers strangers. Fifty percent of all murders in Newport News involved family members and in half of those cases police had previously responded to complaints of domestic violence. Evans made domestic violence his target.

After these findings police were required to make arrests when they had witnessed domestic violence or when they had perceived evidence of assault or when drug or alcohol use was evident.

Crime analysis and investigative practices has shown here, that a proactive strategic approach had developed as a result of the investigation and analysis of intelligence that promoted the acts of murder in Newport News.

A finding of the Newport News of problem oriented policing was that the crime analysis model appeared to be effective when applied to the problems of police work – petty theft, vandalism and such. Crime analysis focuses on groups of events rather than isolated incidents. The crime locations are identified then the use of patrol and investigative time can be more effectively used through crime analysis.

There are various processes involved in the analysis of information for crime investigations with profiling and crime mapping being two of the most popular and successful techniques (MJ, Palmiotto CSU Readings 1988).

Profiling

Profiling involves evaluation of the criminal act itself and comprehensive evaluation of the specifics of the crime scene(s). A comprehensive analysis of the victim evaluation of the preliminary police reports and evaluation of the medical examiners autopsy protocol also development of the profile with critical offender characteristics and investigative suggestions predicated on construction of the profile.

Criminal profiling is used by the investigator to narrow down the scope of an investigation. Criminal profiling can assist to identify the offender. Criminal profiling is a tool that can be utilised by a skilled investigator in crime solving. There are also databases of information relating to profiles that may hold the crime offenders identity profile.

Law enforcement agencies submit specific criminal case information to the staff from the analysis unit. Information from the analysis is used to determine if a similar pattern of characteristics exists among individual cases.

Within the database systems, similar patterns are made by analysing victimology and physical evidence also suspect description and suspect behavior exhibited before during and after the crime.

The crime incident or crime scene report must be accurate, specific and consistent in order for crime analysis activities to obtain a level of usefulness. Crime pattern analysis can be a very useful tool for investigators.

Crime Mapping

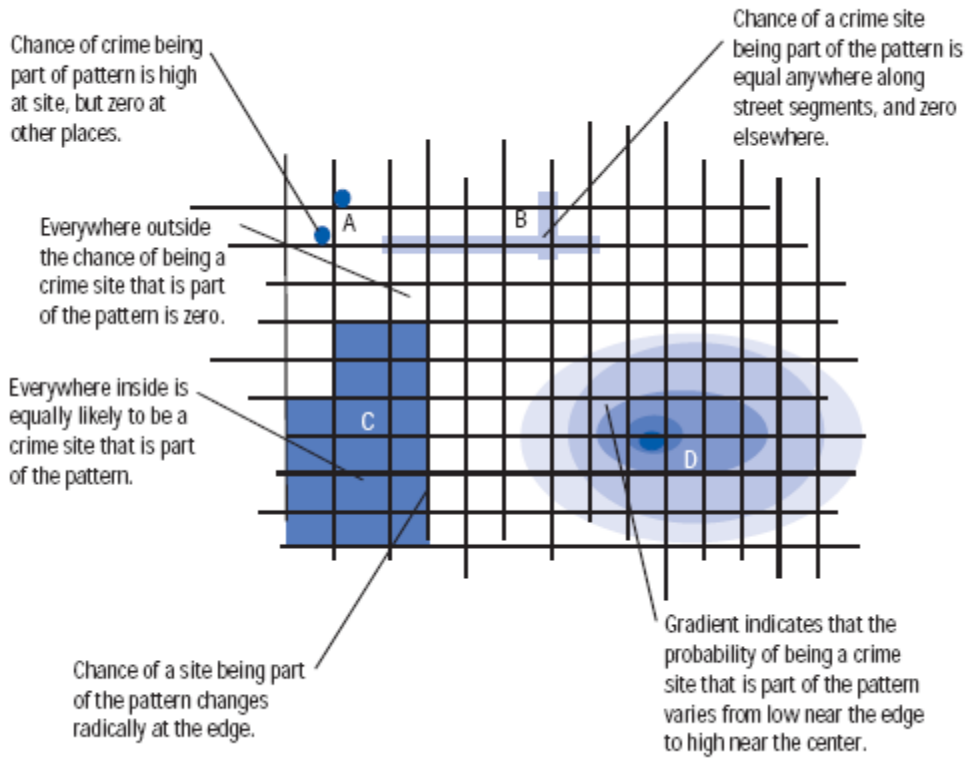
US Department of Justice (2005 p.11 states ‘crime maps convey powerful messages to their readers most of whom are not knowledgeable about the technicalities of crime mapping.’ These messages are conveyed in symbols, dots and shaded street segment also shaded area and areas covered by gradient.

The dots draw attention to specific places and suggest that places without dots can be ignored. A point conveys the message that the crime hotspot is located at the exact location and should be the focus of police efforts.

US Department of Justice (2005, p.11 states ‘the shaded street segment suggests that the chances of crime are roughly equal along the entire segment and police efforts should focus along this line, but not along other lines. A shaded area such as used in a chloropleth map, also suggests equivalent risks of crime throughout the area with a dramatic reduction in risk at the border. It suggests that police activity throughout the area is appropriate.

An area covered by a gradient such as that depicted in isoline maps, implies that a centre of high – crime activity exists and that criminal activity tapers off gradually from that center. It directs police attention to the centre and its surroundings.’

Exhibit 3. Messages in crime maps



Source: US Department of Justice, Office of Justice Programs

Each way of connecting hot spots is connected with useful theories, each of which suggests different types of police action. Recognition of these links in mapping practice will lead to better use of crime maps.

Crime analysts can examine crime related data to visualise and understand crime hot spots. Statistics has shown how simple-to-apply tests can reveal an understanding of what is to be expected in a crime hot spot map even before the map has been created.

There are various types of software used for creating time maps. Some software programs are readily available for free download from the internet. Arcview chloropleth mapping and Arcview spatial analyst are useful programs for visualising crime hotspots and clusters.

There is also a program called CrimStat that uses a graphical interface for database management operation as well as for the implementation of a number of statistical procedures that can be linked to a Geographical Information Systems (GIS) program. The procedures vary from descriptive centrographic applications to more sophisticated nearest neighbor and spatial autocorrelation statistics (US Department of Justice 2005).

The spatial statistics program package provided with CrimStat is divided into four categories. Spatial distribution, distance statistics, crime hotspot analysis routines and interpolation statistics.

GeoDa is similar to CrimeStat; GeoDa is a Windows based application that is practically a reinvention of the original SpaceStat package and its Arcview extension. GeoDa can analyse objects characterised by their location in space. GeoDa is a specialised program especially useful in examining crime related location and determining crime hotspots (US Department of Justice 2005).

Conclusion

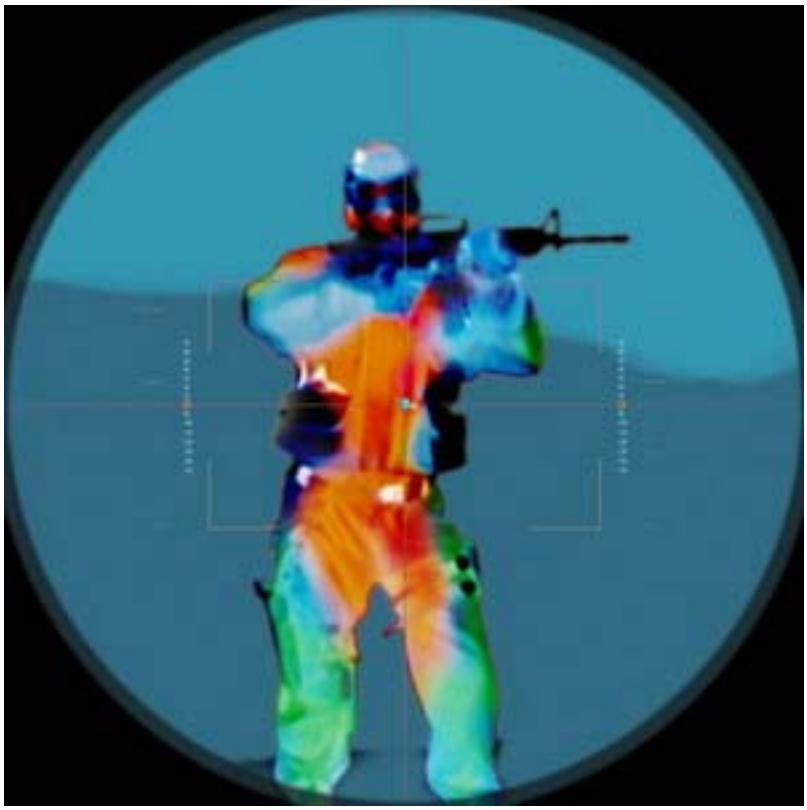
Cybercrime and terrorism in history hasn't been treated with great care through investigative practices through periods that the world's countries have suffered disastrous events of terrorism. Cybercrime has also been occurring rapidly with the ever changing e-commerce transactions from the internet.

Preparedness and prevention are found to be the key points when utilising modern tools to analyse and investigate cybercrime and terrorism applying a strategic approach to achieve positive outcomes.

Good communication and cooperation in field operations within crime analysis is considered to be the keystone on a new approach for delivering police services.

Criminal profiling and crime mapping with the use of modern software programs is assisting investigators to analyse the criminal environment critically. Crime pattern analysis is one of the most useful tools for investigators to achieve positive outcomes with terrorism and cybercrime.

In using modern techniques and technology, criminal profiling and crime mapping with the strategic approach, strong intelligence capabilities used to combat international terrorism and cybercrime will limit the opportunities for those who commit crimes.



Bibliography

Australian Government 2004, *Protecting Australia against Terrorism: Australia's National Counter - Terrorism Policy and Arrangements*, Commonwealth of Australia.

Branca, P 1998, *Geographic Profiling: A new tool in serial crime investigation*, Intelligence Digest August.

Bratingham, PJ & Brantingham, PL (eds.) 1981, *Environmental criminology*, Waveland Press, Prospect Heights, Ill.

Carozza, D 2006, *Fraud Magazine, Journal of the Association of Certified Fraud Examiners*, January/February 2006 Volume 20, no.1 ACFE.

Chalmers, AF 1982, *What is This Thing Called Science?* University of Queensland Press, St. Lucia.

Day, K 1998 *Investigation & Policy Issue*, Australian Federal Police, Canberra ACT Australia.

Goldstein, H 1990, *Problem Oriented Policing*, McGraw-Hill, New York.

Gordon, A 2006, *Agent: Essential Reading for Collectors, Investigators, Process Servers & Repossession Agents*, February/March 06 Volume 39 issue 7 IMA.

Gudjonsson, GH 1992, *Interviewing: Basic Principles & Theories in the Psychology of Interrogations Confessions & Testimony*, Wiley, Chichester.

Irvin, BV Garson, GD 2003, *Crime Mapping: New Tools for Law Enforcement*, FBI Law Enforcement Bulletin www.findarticles.com/p/articles/mi_m2194/is_1_75/ai_n16114610/print, cited 13/05/2006.

Jeffery, CR 1971, *Crime prevention through environmental design*, Sage Publications, Beverly Hills.

Jiggins, S 2000, *E-crime: a global challenge for law enforcement*, Australian Federal Police.

Kinsey, R, Lea, J & Young, J 1986, *Losing the Fight against Crime*, Basil Blackwell, Oxford.

Krone, T 2005, *Hacking Motives*, High Tech Crime Brief, Australian Institute of Criminology, Canberra ACT Australia.

Krone, T 2005, *Hacking Offences*, High Tech Crime Brief, Australian Institute of Criminology, Canberra ACT Australia.

Krone, T 2005, *Phishing*, High Tech Crime Brief, Australian Institute of Criminology, ACT Australia.

Krone, T 2005, *Hacking Techniques* High Tech Crime Brief, Australian Institute of Criminology, Canberra ACT Australia.

McGrath, MG, MD 2000, *Criminal Profiling: Is There a Role for the Forensic Psychiatrist?*

Microsoft 2005, *Microsoft Partners with Australian Law Enforcement Agencies to Combat Cybercrime*, Australia.

Newman, O 1972, *Defensible space, Macmillan*, New York.

Palmiotto, MJ (ed.) 1988, *Crime Pattern Analysis: An investigative tool, in Critical issues in criminal investigation,* 2nd edn, Anderson Publishing, Cincinnati, Ohio.

Poultney, B 2005, JST426 *Crime Analysis & Investigation*, Faculty of Arts Readings, Charles Sturt University, Albury-Bathurst-Wagga Wagga, New South Wales Australia, pp. 86-88.

Poultney, B 2005, JST426 *Crime Analysis & Investigation*, Faculty of Arts Study Guide, Charles Sturt University, Albury-Bathurst-Wagga Wagga, New South Wales Australia.

Poultney, B 2005, JST426 *Crime Analysis & Investigation,* Faculty of Arts Subject Outline 200640, Charles Sturt University, Albury-Bathurst-Wagga Wagga, New South Wales Australia.

Powell, C 2002, *War on Terrorism: Patterns of Global Terrorism*, Platypus Magazine number 76 September.

Ratcliffe, JH 2003, *Intelligence- Policing: Trends & Issues in crime and criminal justice*, Australian Institute of Criminology.

Ramsland, K 2005, *Geographical Profiling*, Crime Library, www.crimelibrary.com/criminal_mind/profiling/geographic/1.html, cited 13/05/2006.

Smith, RG, Woolanin, N & Worthington, G 2003, *e- Crime Solutions & Crime Displacement*, Trends & Issues, Australian Institute of Criminology, Canberra ACT Australia, p.2.

Smith, RG 2004, *Impediments to the Successful Investigation of Transnational High Crime,* Trends & Issues, Australian Institute of Criminology ACT Australia.

Smith, RG 2003, *Investigating Cybercrime: Barriers & Solutions,* Australian Institute of Criminology, Canberra ACT Australia.

Williamson, G McFadden, M & Cameron - Stephen, S 2002, *Preventing fraud and corruption in government: Fraud Investigation, A knowledge-driven approach*, Platypus Magazine number 76 September.

US Department of Justice 2005, *Mapping Crime: Understanding Hot Spots,* Office of Justice Programs National Institute of Justice www.ojp.usdoj.gov/nij, cited 16/05/2006 p.11.

US Department of Justice 1998, *Terrorism in the United States* Federal Bureau of Investigation, pp. 6-10.

Xu, J Hsinchun, C 2003, *Criminal Network Analysis and Visualisation: A Data Mining Perspective*, University of Arizona, Tuscon, AZ.