Main ideas
p. 68 - link analysis → traffic analysis - powerful tool for mapping movement analysis
p. 69 - Techniques for defeating traffic analysis.
p. 70 - Leo's/Nexis "Netmap" program for drug interdiction, etc.
p. 71 - Stolen cellphones disrupt traffic analysis.
p. 71 - Head of Cellnet says all positional info stored for 2 years on cell phones.
p. 72 - Neural networks do not detect new fraud patterns.

CONNECTIONS 24(3): 66-78

Terrorists/Liberators: Researching and dealing with adversary social networks[1]

p. 73 - Dramatic growth in traffic analysis + movement to eliminate warrant requirements.
p. 74 - easily replaceable leadership of Terror Groups.
p. 76 - profile of ~~Dentel~~ Dutch criminal organizations & extension to Islamic Terrorists.
p. 77 Structural holes quickly filled w/ new players in waiting line.

Karl M. van Meter
LASMAS-CNRS, Paris

We first describe the recent evolution in the definition of the term "terrorism" following the 11 September 2001 attacks. We presented two specific types of "link analysis" methods used to analyze adversary networks. Ralph McGehee, of the CIA, developed the village survey method used in Thailand in the mid-1960s. We present in detail the evolution of "traffic analysis" (communication link analysis) from its description in World War II US Army manuals to CIA use in the late 1960s against Eastern diplomats in the US and against rebels in Latin American, to MI5 use since the 1970s against the IRA in Northern Ireland (and vice versa), and to modern extra-judicial use by police, intelligence and private parties for "non-intrusive" telephone surveillance. This presentation of traffic analysis includes publicly-available counter-measures that have been developed over time. In the last section, we present Peter Klerk's doctoral thesis on the analysis Dutch criminal networks and strategies against them, including targeting their weakness associated with queue analysis of key network position replacement.

CLARIFYING TERMS: "TERRORISTS" OR JUST ADVERSARIES

When MI5 and the IRA used the same methods of link analysis against each other to target individuals for assassination, it's difficult to call one use "anti-terrorist" and the other "terrorist." Even with the worldwide backing of the US government's "anti-terrorist" campaign against the individuals and organizations responsible for the 11 September 2001 attacks in New York City and Washington, the United Nations was unable to come up with a definition of "terrorism." The head of Reuters news service even went as far as explicitly discouraging the use of the term "terrorist" in Reuters press releases following the 11 September attacks. Indeed, the governments of South Africa, Angola and Zimbabwe — to only name a few — are run by individuals and parties that were widely described as "terrorists" until the regimes they were fighting against crumbled. A very thorough development of this question was recently provided by Seumas Milne (2001) who stated that: "The transformation from terrorist to respected statesman has become a cliche of the international politics of the past 50 years, now being replayed in Northern Ireland."

[1] We would like to thank the French "Association pour le Droit à l'Information" (ADI, Association for the Right to Information) for access to its documentation and libel use of material at its Web site in New York City <http://blythe.org/intelligence> or published in its fortnightly journal, *Intelligence*.

When the same methods are used by one large company against another, by one intelligence service against another, or by a democratic government against religious fanatics, it seems more appropriate to avoid terms such as "illegal" and "illicit" and to use the term "adversary"; thus the title of this article is "Researching and Dealing with Adversary Social Networks."

This is not to discourage attempts to arrive at a consensus concerning what is "terrorism" and developments since the 11 September attacks have indicated a direction of possible progress. Western Europe reportedly developed the first "modern" definition of terrorism in the 1980s as "violence to obtain political objectives." Thus, the Red Brigades in Italy and ETA in Spain were "terrorists." However, the United States could not condone such a definition which could seriously hinder its foreign policy, particularly in Israel and Palestine where the Israeli government applies an official assassination policy against Palestinian leaders.

Following the 11 September attacks, a consensus seems to be developing around the use of the term "terrorism" to describe "violence to obtain political objectives and involving attacks against citizens of foreign countries not directly involved in a conflict." This, of course, focuses the problem of clarification on the term "directly involved in a conflict," but it makes it clear that the 11 September attacks were "terrorism." However, it leaves open the question of whether or not killing civilians, in a theater of combat, without proof of support of rebels is also "terrorism."

Researching "adversaries," including political or commercial rivals, can take many forms. Even when limiting the field to empirical, data-based methods, there are still numerous possibilities even though this tends to eliminate almost all the "methods" employed by political, commercial and other organizations that are not intended for scientific research. By limiting the field even further to "structural" methods used in scientific research, there are still many candidates and this issue of *Connections* will be presenting several of them. Below, we present two: the village survey method developed by CIA officer, Ralph W. McGehee, and traffic analysis or communication link analysis whose first formalization we have found in a US Army World War II manual.

MCGEHEE's VILLAGE SURVEY METHOD

In September 1965, CIA officer and former Notre Dame football star, Ralph McGehee arrived in Bankok, Thailand, to fight Communist rebels (McGehee, 1983). He soon found out the CIA data on the rebels was not only unreliable but, in many cases, false. This reflects the same discovery concerning official data on adversaries that Klerks notes in his article in this issue of *Connections* concerning Dutch criminal networks. McGehee decided to "go into the field" and develop what he called the "village survey" method which is simply a form of the classic village monograph method in anthropology. McGehee and his district survey team would interview village members and note family and community relationships. Cross-checking was all that was needed in many cases to obtain confessions of Communist Party membership or even arms training.

By returning later to the same villages, redoing another survey and cross-checking data with the previous survey, McGehee often obtained a complete description of the local or even district structure of the Communist Party and its various associated organizations. By surveying 30 Thai villages, he was able to extrapolate results to all of Thailand, and that's where things went wrong. He found more Communists in one province than the CIA officially recognized for all of Thailand. Using available information, the method indicated that if applied to Vietnam, the picture would have been catastrophic: "the surveys would have shown there that the communists could not be defeated" (*ibid*: p. 116). The CIA's response was to award McGehee its highest service medal and keep his results from being known by anyone outside a very small circle of CIA officials including William E. Colby, then CIA Far East division chief and McGehee's more-or-less direct superior, before becoming head of the CIA during the Vietnam "police action."

WORLD WAR II AND EARLY HISTORY OF TRAFFIC ANALYSIS

During World War II, "traffic analysis" was defined as "that branch of cryptology which concerns the study of the external characteristics of signal communications and related materials for the purpose of obtaining information about the organization and operation of a communication system" and presented in a US Army technical manual (1948). Although traffic analysis probably existed in other forms since the use of electronic battlefield communication systems, this is the first mention of the term and the first formal presentation we have found. It is a "filing card" technology system, meaning that its data analysis methods — mostly manual cross-checking — were no different from those McGehee was using in Thailand in the late 1960s before computers were widely available.

One should note in the above definition the use of the term "external characteristics," clearly implying that the structure of communications, and not their content, is the object of study. In its most precise and limited definition, traffic analysis, or "metering," consists of a form of network analysis of many telephone calls (or other forms of contact or communication) to determine who calls whom, in what order, for how long, and at what time. Such analysis does not involve listening in on conversations and is therefore not legally "wiretapping" under most nations' laws. Indeed, since privacy law does not even mention the existence of traffic analysis (or pen registers) in most countries, it can be done by law enforcement agencies, intelligence services, private companies or anyone else who can obtain the necessary "metering" information. Properly done, with good data, and with unaware adversaries not employing counter-measures, traffic analysis can determine "ring leaders," "gate keepers," "messengers," "outliers," and other types of network members and their roles.

POST-WAR "CIVILIAN" USE OF TRAFFIC ANALYSIS

As the Cold War settled in and US military policy in Latin America evolved from sending in the US Marines to CIA-developed "counter-insurgency," traffic analysis reportedly found new life in tracking Eastern diplomats — and potential spies — in Washington, DC, and New York City, NY. In such developments, the British are either not far behind or even working directly with the US, which seems to be the case for traffic analysis. The first detailed publicly-available information we have been able of find on the non-wartime use of traffic analysis was its use in Northern Ireland against the Provisional IRA as part of a system called Movement Analysis developed by the British MI5 internal security service, also known as the Security Service but preferring the acronym "MI5" (Military Intelligence 5) to that of "SS." This information surfaced in January 1989, in London, when MI5 asked the Speaker Office of the House of Commons to withdraw the name of Hal G. T. P. Doyne Ditmas from a question by Labour MP, Chris Mullin. The reason was that MI5 feared Irish subversives would discover that Mr. Ditmas "made a significant contribution to the efforts of British intelligence in Ireland," according to the Dublin newspaper, *The Phoenix*, on 13 January, by developing and applying movements analysis against the IRA both in Northern Ireland and in Great Britain.

Then attributed to Terry Guernsey, the head of the Royal Canadian Mounted Police, or "Mounties" (Canada's internal security service), movement analysis reportedly consists of a data collection system and a statistical analysis system to determine who holds what position and what are their functions. Reportedly used initially in North America against Eastern block diplomats, Mr. Ditmas supposedly adopted it for MI5's work on Eastern block diplomats in London. As a MI5 KY Branch officer in the late 1960s, Mr. Ditmas worked with Barry Russell-Jones of MI5 on the program. Mr. Russell-Jones then became head of MI5 FX Branch in the mid-1970s and head of MI5 S Branch (computer service) in 1979 before retiring in the early 1980s. He then set up Russell-Brooks Associates with MI6 officer, Anthony Brooks, according to press reports.

In movement analysis, data is systematically collected on times, durations, days of the week, places and individuals visited, type of visits, car licence plates, trajectories by car, foot, or public transportation. First, by simple cross-tabulation, and then by more sophisticated statistical methods such a automatic

classification analysis, typological analysis, and factor analysis, specific "types" of behavior can be precisely defined, along with the "outliers" who do not fit easily into the specified types. These types and outliers can then be examined in detail to see if they represent profiles characteristic of adversary activity. Secondly, structural analysis to determine the relationship between the different individuals analyzed can be done using the various network analysis statistical methods such as traffic analysis. These determine who are the leaders of groups, the "gate keepers" between different groups, the peripheral members, and the central members.

When MI5 decided to computerize its operations in Northern Ireland in the mid-1970s, it took several years but, when completed, it was Mr. Ditmas who installed the movements analysis system that covered all Catholic ghetto areas where the IRA operates. Called "Operation Vengeful," it used British soldiers both for routine information collection and for "census" calls on virtually every Catholic household. This aspect closely resembles McGehee's village survey work, but in a "domestic" and much more hostile environment. In October 1990, Mr. Ditmas was named to the newly-created post of Chief Inspector of Transport Security, according to *The Guardian* (31 October 1990). He was officially described as a former under-secretary at the Ministry of Defence and his career "spans periods at the Foreign Office as well as the Cabinet and Northern Ireland Offices." In his new job, he was to be responsible for security at sea and air ports and, of particular importance, the Channel Tunnel. In January 1994, Mr. Ditmas made the news by finding four international airlines operating in Great Britain which failed a security review, including Virgin Atlantic, a member of a consortium which later bid to take over and operate the British portion of the Channel Tunnel railway in January 1995. On 18 November 1996, a major fire broke out in the Channel Tunnel and closed it for some time, but Mr. Ditmas had apparently already moved on.

TRAFFIC ANALYSIS "BITES BACK" AND PUBLIC COUNTER-MEASURES

Mr. Ditmas may still have been working with traffic analysis in Northern Ireland when MI5 discovered not only that the IRA knew about the method, but had actually developed its own version and used its against British intelligence. Reportedly IRA traffic analysis discovered that all Royal Ulster Constabulary (RUC) agents and informants were paid the same day every month and would line up at a certain number of automatic teller machines to draw out their cash, thus permitting the IRA to identify a major part of MI5's secret anti-IRA assets.

The next time traffic analysis entered the public domain, it was because of a 19 July 1992 theft of confidential documents in a Scottish police station. The publication of this information in the newspapers, *Sun* and *Scotland on Sunday*, revealed that the police had carried out widespread traffic analysis of telephones used by 78 persons and organizations. The publication also resulted in the arrest and detention of two journalists that fall. These reports clearly referred to the use of traffic analysis or "metering." It seems like poetic justice that some of those who were "metered" — journalists — were those that exposed the method ... and were put in jail for their contribution to public knowledge.

In early 1994, the first publicly-available "counter-measure," that we have found, was described in press reports. To defeat traffic analysis, a caller needs to protect, at a minimum, both his or her identity and the duration of the telephone call. This impedes establishing a link between the caller and a targeted number under surveillance or being eavesdropped. If it is the caller who is under surveillance or being eavesdropped, this "first-generation" system, the "Stopper," does not work. But the minimum requirements of anonymous caller identity and indeterminate call duration were reportedly met by Stopper which was a secure switching scheme provided by a Washington and Beverly Hills-based privacy lawyer, William Dwyer II. It also kept a caller's unlisted number secure from caller ID systems. By telephoning first to 1-900-stopper (786-7737) at what was then a $1.95 per minute rate, the caller received a dial tone to make a touch-tone call anywhere in Northern America. For $3.95 per minute and an initial call to 1-900 call 888 (225-5888), it was possible to telephone anywhere in the world without revealing your number. Other security features included multiple outgoing calls, which

prevented identifying a call by the time of day and its duration, and the possibility of using Cylink voice encryptors between the caller and Stopper, but such options interest intelligence agents much more than the general public. Nonetheless, US and Canadian officials declared the system legal. It closely resembles current widely-used "Kall Back" systems.

Traditionally, a new director of the Belgian Sûreté d'Etat internal security service gives a press conference concerning the service's priorities. It's a sort of initiation ceremony and the late 1994 appointment of Bart Van Lijsebeth as Sûreté chief was no exception to this rule. A new priority for Mr. Van Lijsebeth was the Belgian extreme right and local religious sects. This axis was probably determined largely by that year's political events including investigations of the Sûreté's shady ties with the neo-Nazi Westland New Post and with the Brabant massacres. Van Lijsebeth also stated he would like to have more personnel and legalize telephone eavesdropping. Because "wiretaps" were still illegal, the Sûreté was reportedly getting around the problem by telephone traffic analysis, "a form of network analysis to find 'gate-keepers' and 'core' persons by analyzing who calls whom at what time and for how long. Since this information does not constitute 'tapping', the Sûreté can resort to it without oversight" (ADI, 1994: 32).

RECENT DEVELOPMENTS IN TRAFFIC ANALYSIS

With such information available in the public domain, it couldn't have been long before the then proud and powerful software industry put traffic analysis tools on the market to replace file-card cross-tabulations and the user-unfriendly "homegrown" programs that were being used by law enforcement agencies, intelligence services, private companies and assorted "adversaries." In spring 1996, Alta Analytics, of Columbus, Ohio, well-known for graphical data analysis, announced a "product development and joint marketing agreement" with a major on-line data service, Lexis-Nexis, concerning a link analysis "data mining" program, Netmap. An ADI (1996: 2) review of the program noted that "information specialists probably didn't notice that Netmap's 'credentials' include being 'widely used in intelligence and law enforcement'. Link analysis is part of a larger category of scientific tools called network analysis and can be applied to all forms of relationships: financial, organizational, command, hierarchical 'pecking orders', telephone conversations, emotional support, counselling and advice."

Up until then, the type of network or link analysis programs available to the general public (outside the social network scientific community) had been mostly "graphical," meaning new and more beautiful ways of presenting data in full color to decision-makers. What Alta had done with Netmap was to adapt certain scientific tools for intelligence work, and for public data mining. The US Defense Intelligence Agency (DIA) Office of National Drug Control Policy had "plugged" Netmap into its new Emerald drug interdiction coordination computer network, and other intelligence services could clearly profit from Netmap applications, according to Alta Analytics, which also recommended Netmap for assisting "in the intelligence production cycle to detect and expose financial crimes and money laundering activities."

Schematically, the program laid out analytical "units" (persons, bank accounts, companies) on the perimeter of a circle and traced lines between the "units" representing a "link" or tie. The darker or thicker the line, the greater the tie (more financial transactions, more telephone calls). This particular graphic technique had already been around in network analysis since the late 1970s and early 1980s, and was used as a starting point of cognitive mapping techniques developed in France at the Ecole des Mines de Paris by Jean-Pierre Courtial (van Meter and Turner, 1992; van Meter and Turner, 1997). Where network analysis and cognitive mapping usually go from this basis into multivariate analysis — and therefore lose the general public and most intelligence professionals — Netmap makes it simpler by sticking to univariate (single variable) analysis and successively "cleans up" the circle diagram (although Netmap does have certain multivariate capabilities). Thus, a circle of 4,003

telephone calls between 1,103 numbers was reduced to 45 "units" (telephone numbers) with more than 20 calls, then to three numbers with 40 or more calls.

If sequence of calls is introduced, then Netmap can help map out the "command hierarchy" of telephone calls (which is not necessarily pyramidal as the general public is usually led to believe) and furnish valuable information on whom to "wiretap" or arrest. This is exactly what the US Army was doing in World War II on bristol cards when it was doing traffic analysis: identifying the adversaries "command hierarchy"... before bombing it. More recently uses of traffic analysis results have often not led to more subtle outcomes. In classic intelligence and law enforcement work, traffic analysis can usually be done without a warrant since conversations are "counted," not "listened to." When several Netmap-like circles (one for telephone calls, one for "work together," one for "leisure time together") are overlaid, one on top of another, or analyzed at the same time (multivariate analysis), the often complex structure of an adversary's network becomes much more clear. What is done with this information is, of course, something else, as we will see below.

HIGH-TECH FOR THE BAD GUYS AND THE GOOD GUYS

But just as the cops were catching up with the crooks — technologically speaking — the crooks "pulled a fast one" with still newer technology that easily defeated Netmap and similar traffic analysis methods: cell phones. As portable or mobile telephones became widely available, they also because widely stolen. Crime bosses would buy a half dozen at a cheap price, use one after another for a few days — it depends on how dangerous your "business" is — and then "recycle" them by either putting them back on the black market or running over them with their car. Dropping them out of a car window on a busy freeway is also considered "cool" ... and probably bothers the police technicians who are trying to follow the location of the cell phone.

In Great Britain, cell phone technology also brought new developments for the "good guys" when, in 1997, it was reported that under the British Interception of Communications Act 1985, the British police were not obliged to seek a warrant to eavesdrop on private conversations made by the then 4 million users of mobile telephones. This interpretation of the eavesdropping law was a direct result of advances in signal technology. The mobile telephone is made up of two items: a base unit, which is part and property of the public telephone network; and a handset, which is regarded as a stand-alone private system using radio waves to transmit instead of a land line. British legislation, as then drafted, allowed the police or other government agents to use signal intelligence equipment to intercept conversations "broadcasted" by private systems without having to seek legal permission to do so. This interpretation was underlined at the time by a Law Lords ruling in the case of a drug dealer, convicted on signal intercepts, which confirmed that "the interception by the police of telephone conversations on a cordless telephone is not subject to the Interception of Communications Act 1985 and evidence at a criminal trial of such conversations is not rendered inadmissible" (ADI, 1997: 4). So who needs traffic analysis when you can listen directly to the conversation and, moreover, record the physical location of the callers? A question for future research is whether or not British crooks went back to land lines when this information became available.

Although not directly related to traffic analysis, although very closely associated, is cell phone location information which we have not found to be covered by privacy legislation in any country. On the contrary, again in Great Britain, its use by authorities has been clearly stated. Mobile telephone location information can be used to trace a caller's physical presence years afterward by employing technology reportedly used for the first time in 1997 in a British murder trial and in a British Winchester football match-fixing trial. In the former case, the police used computer records to track the accused's journey from work to the murder scene and back again, even though no calls were made or received. William Ostrom, of Cellnet, one of Britain's four largest mobile phone providers, stated that the stored data was used for billing purposes, but it was also used to check for "unusual use" and possible theft of a telephone. He claimed: "We can tell where any one of our mobile phones was, as long as it was switched

on, for any time and date in the past two years. It's exactly the same for all four mobile networks in Britain, which deal with nearly seven million users. [...] We are helping the police with three cases at the moment" (*ibid.*) Vodafone admitted that similar data is stored, but another British mobile phone provider, Orange, refused to comment. Orange now belongs to France Telecom but it is possible that British cops have kept Orange's old location information. Another future research project would be to find out what happened to privacy data, and particularly cell phone location information, following takeovers by telecommunication companies from different countries.

When activated, mobile telephones, even when not receiving or sending a call, emit a signal so that base units know where it is and which apparatus it is so that a call to or from it can be quickly routed. This signal serves as a miniature tracking system unknown to the user and reveals the whereabouts of the apparatus at any given time. The electronic signal data, pinpointing the device's location, are stored in service provider computers for several months and, in Great Britain, up to two years. "Smart" mobile phone users often think they have "outsmarted" the system by simply turning off their unit, but most, if not all, units can be turned on remotely with the appropriate high-tech equipment at the disposal of official intelligence services. The only "foolproof" counter-measure is to take the battery out of the mobile unit or put the unit in a "tempested" farad cage, if you have one. Members of the general public usually not. not true. not true. They are called metal boxes, elevators, basements. etc. Leave cell phone at home.

TRAFFIC ANALYSIS MAKES THE BIG TIME

In March 1998, traffic analysis -- and all forms of social network analysis — "made the big time" in official surveillance and eavesdropping when the American Association of Artificial Intelligence (AAAI) launched its "Call for Papers" for its fall symposium on Artificial Intelligence and Link Analysis in Orlando, Florida, on 23-25 October 1998. The AAAI recognized — as we have mentioned above — that "computer-based link or network analysis is increasingly used in law enforcement investigations, fraud detection, telecommunications network analysis, pharmaceuticals research, epidemiology, and many other specialized applications. Much of the current software for link analysis is little more than a graphical display tool, but many advanced applications of link analysis involve thousands of objects and links as well as a rich array of possible data models which are nearly impossible to construct manually." In short, formal network analysis was necessary, and, as the symposium organizers stressed, "the focus of the symposium is new technologies, not capabilities and applications embodied in current software." Little wonder that the organizers included William Mills, of the CIA Office of Research and Development (R&D), and Raphael Wong, of the US Treasury Department FinCEN financial "cops" specialized in money laundering pattern recognition (ADI, 1998a: 2).

At the same time, in addition to law enforcement and intelligence, network analysis made its entry on the Internet when UCLA sociology graduate student, Marc Smith, used his program, Netscan, to analyze USENET topic groups for patterns of interaction such as how many posts were made to a newsgroup during a given time period, how many different people made those posts, and how many of those posts were cross-posted to other newsgroups; more-or-less traffic analysis applied to USENET activity. Netscan produced simple bar graphs and numbers and could help generate hypotheses about the social dynamics in the newsgroups and what kinds of experiences each group offers its participants. Although Netscan did not actually do multivariate network analysis, it could easily function as the "front-end" of more advanced systems, and Smith intended to develop that aspect.

It also appears that network analysis and associated pattern recognition methods defeated one of the "new pretenders" at the time: neural network analysis. According to an early 1998 study by InfoGlide Corporation, of Austin, Texas, "neural nets are essentially obsolete for fraud detection" when compared to pattern recognition, although this result may be dependent on the specific methods tested (ADI, 1998a: 2). Usually, neural networks are "trained" by multivariate pattern recognition and network analysis methods before functioning independently. If the objects of analysis suddenly

undergo a significant change, such as a new form of fraud, the neural net must be "retrained" by the multivariate methods before it can function again correctly. Since some criminals are not stupid, they often come up with new types of fraud that initially avoid detection by existing systems. Thus, back to traffic analysis.

In early 1998, two of Ireland's top universities, Trinity College, Dublin, and Queen's University, Belfast (QUB), obtained European Commission funding to establish a "transfer technology node" to promote the application of supercomputer technology into commercial and industrial projects such as data mining in the financial sector and simulation of network designs for the telecommunications industry. The ADI disingenuously commented: "Previous major computer programs in Ireland included MI5 'traffic analysis' of IRA suspects' movements and telephone calls, and IRA analysis of automatic teller withdrawals to identify RUC [Royal Ulster Constabulary] agents and informants. The current project appears to be the EU contribution to 'peaceful' use of computer technology" (ADI, 1998b: 5).

THE NEW KGB, PRIVACY INTERNATIONAL, THE FBI & NEW YORK GET INVOLVED

In late July 1998, the Russian FSB internal security service (the successor of the Soviet KGB "domestic" chief directorate) announced that under its Project "Sorm" (System of Operative Intelligence Actions or System for Ensuring Investigative Activity, depending on translations), it planned to monitor the Internet in Russia, in real time, for every email message and Web page sent or received. All Internet services providers (IPS) in Russia would have to install an eavesdropping device on their servers and to build a high-speed data link to the FSB's Internet control room. The US firm, Cisco, probably found a market for its "Private Doorbell" surveillance-friendly encryption system, and, according to the Swedish publication, *Svenska Dagbladet*, the FSB had developed three levels of control: full, statistical traffic analysis (listing all outgoing and incoming telephone conversations), and control of a communication area through network analysis monitoring by a station covering the area. The importance of the project could be judged by the man in charge: FSB deputy director, Aleksandr Bespalov (ADI, 1998c: 29).

In fall 1998, the British group, Privacy International, awarded its annual Big Brother "Name and Shame" privacy invader titles. The product winner that year was WatCall software, produced by Harlequin Ltd., for telephone record "traffic analysis" "which avoids the legal requirements needed for phone tapping."

In May 1999, the administration of President Bill Clinton, through the International Law Enforcement Telecommunications Seminar (ILETS), an umbrella organization set up by the FBI in 1992 which includes security and law enforcement agencies from 20 Western countries, was pressuring EU members to force European ISPs to provide "interception interfaces" for all future digital communications to allow police and spies to monitor an individual's web activity, check newsgroup membership and intercept email. Caspar Bowden, director of the London-based Foundation for Information Policy Research (FIPR), stated at the time that the data-taps probably infringe on the European Convention on Human Rights (ECHR). Mr. Bowden claimed that even if Internet users encrypt their email, sophisticated analysis programs — such as communications traffic analysis — can reveal a great deal to the trained professional about an individual's usage and his or her network of personal contacts. Thus, traffic analysis could be used even to counter encryption-based public privacy in communications. This seems to be one of the uses of traffic analysis by the worldwide Echelon electronic communications eavesdropping system directed by the US National Security Agency (NSA) and the cornerstone of the secret UKUSA security agreement (ADI, 1999: 3).

On 6 July 1999, in a unanimous opinion, the New York Court of Appeals marked a significant shift in wiretapping jurisprudence and gave traffic analysis by law enforcement a real "shot in the arm" by deciding that police may install pen registers — devices that monitor numbers dialed from a telephone line — without obtaining a warrant based on probable cause. "Reasonable suspicion" is now sufficient

for pen register surveillance to be initiated. At least, pen register surveillance is now mentioned in law and can be discussed in court. Few countries are even that far down the road to protecting privacy. Indeed, we made a request to Privacy International concerning information on the legality of traffic analysis and pen registers in Western countries. Privacy International, which keeps tabs on privacy legislation in most developed countries, gave us a polite reply that our question would make a good but difficult project for future research.

HIERARCHICAL THINKING AND KLERK's THESIS ON DUTCH CRIMINAL NETWORKS

Following the 11 September attacks, one would have thought that the concept of pyramidal hierarchical command structures for illicit adversary social networks, particularly for those of Islamic extremists, would have lived out its overextended life. Indeed, both the media and officials, including the Pentagon, have recently called on the social network analysis community for possible contributions in understanding — and fighting or dismantling — such networks. But official thinking has not changed that quickly. Tamara Makarenko, *Jane's Intelligence Review*'s special advisor on transnational crime and lecturer in criminology at Glamorgan University, Great Britain, proved this point in the November 2001 issue of that review. In his article, "Transnational Crime and Its Evolving Links to Terrorism and Instability," he writes in his section on "Structure" that: "Unlike the hierarchically structured criminal and terrorist groups of the past, transnational criminal groups increasingly appear non-hierarchical in their organisation. Furthermore, they are commonly decentralised and fluid, thus suggesting that the leadership positions are easily replaceable — thereby ensuring that the group continues to fulfil its aims and motivations well into the future" (Makarenko, 2001). Although we thoroughly agree, and develop further below, the idea concerning easily replaceable leadership positions, we equally thoroughly disagree with the idea that "criminal and terrorist groups of the past" were "hierarchically structured": it was official thinking about those groups or networks which was hierarchically structured, and in a very rigid manner.

We can think of no better demonstration of this fact than the doctoral dissertation of Dutch researcher and writer, Peter P. H. M. Klerks, "Big in Hash - Theory and Practice of Organized Crime" (Klerks, 2000), which is available in book form in Dutch. His work was based on an original and unique opportunity for a researcher to work directly on criminal intelligence material and have direct access to the specialists involved in the cases under study, thus producing, with the aid of social network analysis and grounded theory from sociology, some rather original perceptions of organized crime and the best — most efficient — ways to fight it (ADI, 2000: 1).

As Klerks explains in his article in this issue of *Connections*, government files on operational investigations regarding organized crime usually remain inaccessible to academic researchers and the general public for reasons of security. When reviewing organized crime literature, it soon becomes clear that the number of cases where an academic researcher has been allowed full access to police files is limited indeed. The Netherlands was no exception. Until the early 1990s there had been almost no attempts in academic circles to gain access, mainly because only a handful of researchers were active in studying contemporary organized crime. Therefore, when a Dutch police commissioner in 1993 needed scholarly assistance to think up new strategies for tackling organized crime problems in his region, there were very few original thinkers he could turn to. Still, he didn't have much trouble raising interest among police researchers once it became clear that full access would be given to all the relevant files and to police staffers who had been involved in a major and problematic investigation that had ran for more than two years.

Once funding was secured through the Justice Ministry for a researcher to work four days a week for two years, the research project entitled, "Underground Organizations in a Comparative Perspective," started in December 1993. While the formal empirical research ended with the production of a final report in November 1995, research was extended for the three following years to become a doctoral dissertation. This required extensive collection and analysis of relevant literature on organized crime,

policing methods, intelligence methodology and the sociology of secrecy, and some formalization of new research instruments developed in the course of the project.

The research project initially began with five central questions. I. What are the definitions of organized crime employed in academic research and by investigative agencies, and what are their usability and empirical foundation? II. Does a sociological-anthropological approach to criminal organizations offer new possibilities for knowledge in researching organized crime? III. What are the tactics and strategies employed by criminal organizations to ensure the continuity and expansion of their operations in reaction to (possible) government intervention? IV. How does the government create its initiatives against these criminal organizations? Which methods, tactics and means are developed and put into action? Which relationships are maintained: (a) within the police organization; (b) with other involved branches of government (public prosecutor, investigative magistrate); (c) with similar operational teams? What are the effects of such operational government actions in relation to those organizations? V. What new ways can be found to better control organized crime? With certain limitations, one can substitute the term "clandestine organization" for "criminal organization" and apply these question to the present post-11 September situation.

FULL ACADEMIC ACCESS TO CRIMINAL INTELLIGENCE DATA

During the final year of the "Underground Organizations" project, the Dutch parliament ordered another massive research project on organized crime in the wake of the so-called "IRT Affair" during which massive amounts of Latin American cocaine, under supposedly secret "police-controlled deliveries," flooded the Dutch market. In the research project, the "Research Group Fijnaut," consisting of four leading Dutch criminologists, was given almost full access to police files nationwide. It was then decided that the "Underground Organizations" project would not devote much time to research questions I. and IV. Moreover, governmental activities in the case study — mainly police investigative efforts — were to be treated only in a summary fashion since it had become clear that it would be impossible to write the full story without compromising methods and individuals. Therefore, the final report and the doctoral dissertation concentrated on developing new insights on the usefulness of what would be a more sociological network-oriented doctrine of organized crime, on the ways in which criminal organizations evade and counter government action, and on innovative strategies and tactics to control organized crime.

Working in the tradition of Glaser and Strauss's grounded theory approach, data were collected, coded and systematized from hundreds of open publications and stacks of operational dossiers, a process which gradually produced a framework for further classification and analysis that has become a separate instrument in itself (the "analytical scheme for criminal organizations"). The original empirical material consisted of the nearly-complete dossiers of the investigative "Ferrari-team" (a fictional pseudonym), some twenty to forty investigators who had been operational for about two years in the early 1990s. More than 200 document files filled some twelve meters of bookshelfs. This paper archive, plus a personal computer, contained about 20,000 logged telephone conversations, 1,700 checked car license plates, thousands of records on individuals, plus several other logs and reports.

In addition, seventeen functionaries were formally interviewed for their insights on the behavior of lawbreakers and law enforcers. While some of the interviews produced unusual results, they also brought up a specific methodological and ethical problem: the interpretation of information obtained in the course of a research project on confidential matters cannot be fully shared with other researchers. This prevents an open discussion of certain essential aspects of the organized crime phenomenon, which, in turn, posed limits on the control capability crucial to any academic work.

After extensively discussing the history of organized crime doctrines in the United States and their current relevance, Klerk's thesis presents "social network" concepts. The history of organized crime in The Netherlands is then briefly described from a policy point of view, while one specific case, the

criminal network organized in the 1980s by the late cannabis wholesaler, Klaas Bruinsma, is analyzed in detail. Subsequently, a panoramic sketch of the main criminological viewpoints in Holland regarding organized crime is followed by a detailed critique of the definition of organized crime presented by the "Research Group Fijnaut" which was dominant in Dutch academic and policy circles at the time. The threat of criminal networks is then analyzed according to financial-economic strength, potential for violence, resistance to dismantling and sociopolitical influence. Using the analytical framework mentioned earlier, first, insights from the literature on issues such as recruitment, leadership, covert logistics, clandestine security, intelligence-gathering, and the culture of trading and hedonism are discussed extensively, followed by a detailed description of the criminal "Verhagen group" (again a fictional pseudonym), its participants, their activities, the social, criminal and market environments, their world view and lifestyle.

THE VERHAGEN CRIMINAL NETWORK

The criminal Verhagen network, named after the person considered to be the nominal boss, consisted basically of informal sub-networks, each clustered around one of a clique of five entrepreneurs who all brought their own contacts and clandestine abilities to a series of criminal projects. Nearly all important individuals were male Dutch nationals between the ages of thirty and fifty and of white (Caucasian) ethnic origin. Some were well-entrenched in the traditional urban underworld, others originated from the milieu of travelers who live in semi-permanent camping sites all over the country. One individual had good contacts among "adventurous" sailors willing and able to arrange worldwide cannabis transport by sea, while another had access to semi-clandestine financial service providers who could launder and stash profits: millions of guilders, British pounds, Deutsch marks, dollars and other currencies that became so bulky they were sometimes kept in garbage bags.

The criminal network was characterized by a near-absence of formal business structures. The threat of violence was a clear factor in the group's success: quite a few one-time partners, lured into participating in a criminal project, were left either stripped of their assets or in a foreign prison, but few dared to protest for fear of reprisal. Ultimately, however, the sometimes impulsive urge to resort to violence in resolving conflicts brought the main players long prison sentences: when they physically attacked a competitor, beating him virtually to a pulp, threatening his family with firearms and stealing most of his expensive furniture, they left him no choice but to report the incidents to the police. Building on these severe and documented offenses, the public prosecutor could charge the perpetrators with much more serious crimes than simply cannabis transport.

The efforts made by the group to keep its activities and communications a secret were also exploited in some detail, leading to the conclusion that while they had access to some surprisingly-detailed information on police activities, the general level of security awareness, methods and techniques employed was somewhat amateurish. Apart from the operational side relating to criminal activities, much attention is given to the social and subcultural aspects, motivations and life philosophy of the main characters.

USING SOCIAL NETWORK ANALYSIS AND QUEUE ANALYSIS RESULTS

In analyzing what exactly makes these criminal networks so resilient in the face of governmental interventions, the only logical explanation seems to be that it is the network structure itself which allows for informal, flexible and opportunistic operations on a project basis with a few resourceful characters mobilizing a great number of interested parties who all contribute and take a share of the profits. According to French intelligence analysis of the Islamic extremist networks in Algeria, the average "service life" of a local war lord is approximately six months. But the Islamic networks have been "stable" — meaning capable of continuing their campaign of massacring the civilian population — for almost ten years. Little formal queue analysis is needed to see that most war lords have a "waiting

line" behind them for their key network position and when it isn't the Algerian armed forces that "retire" a war lord, it is often those in the "waiting line." With a short "service life" but a substantial "waiting line," key network positions remain filled and the network can function.

Although mutual trust is vital in such clandestine environments without written rules, the Dutch study indicated that while Verhagen's reputation was far from reliable and solid, he was still an effective "boss" and had no problem finding business partners eager to invest in his projects. He was known as a mover and shaker, and the greed of smaller or more ignorant players apparently was such that any reluctance was quickly set aside in the face of what seemed to be a profitable deal. It may have also been a means for smaller players to put themselves on the "waiting list" just in case Verhagen was "replaced." Others on the "waiting list" probably included trusted partners Verhagen used as cut-outs to approach vital contacts such as ship captains and investors to gain their cooperation.

This mechanism, combined with a large and eager market for cannabis products in Holland, guarantees that "structural holes" in the network caused by conflicts or arrests can quickly be filled by new players from the "waiting line." Only certain vital positions requiring special knowledge or capabilities, such as technical skills or access to major foreign suppliers in the countries of origin, are harder to fill. Not surprisingly, these vital "broker" positions are held by silent, permanent players who cater to the service needs of multiple criminal groups, rather than the presumed "big bosses" of the drug networks, and would really be the most interesting targets for law enforcement from the point of view of intelligence and disruption.

In the case of Islamic extremists, French intelligence has found that specialists in counterfeit identity documents, trusted couriers, paymasters, and explosives technicians are key positions. French criminal intelligence has reportedly even engaged in some "network sampling" by detaining for questioning certain key individuals such as a document forger just to see which type of counterfeit document disappears from the underground market. Indeed, "selective detention" has been seen as an effective way to disrupt network functioning and, at the same time, to verify the network position of a detained specialist. By detaining one specialists after another, a network can be kept from functioning for some time. Moreover, the "waiting line" behind these specialists to fill key network positions is often very short and replacement rates are usually rather low.

OPENING CLOSED INTELLIGENCE COMMUNITIES FOR NETWORK ANALSIS

One can easily imagine that these ideas and Klerk's critique of law enforcement's mid-1990s conventional wisdom focusing on stable, pyramidal criminal hierarchies that demanded long-term secretive investigations ("to aim for the top" or "to get the boss") have not been easily accepted. Nonetheless, unprecedented access to sensitive data and intensive cooperation with investigators became a day-to-day reality for many Dutch organized crime researchers in the late 1990s. In that sense, the project portrayed in Klerk's thesis has become a pioneering effort in Dutch criminology and law enforcement. The new concepts it introduced, such as flexible and opportunist networked crime, best countered by equally flexible and pragmatic police teams instructed to create opportunities and make maximum use of intelligence to disrupt the continuity of criminal operations ("close-up investigating"), raised quite a few eyebrows in 1995, only to be included in the Justice Ministry's current organized crime doctrine within three years (ADI, 2000: 1).

What remains to be seen is whether or not the Dutch example will be seriously considered elsewhere in the Western world and whether or not the secretive and closed intelligence communities of those nations will be able to adopt and modify these ideas for use in their current urgent work against Islamic extremists. Unfortunately, this requires, as Klerks has shown, a serious and sustained official effort to open a closed community to academics who have almost always been considered and treated as "outsiders" and deprived of the cooperation necessary for a successful effort. Hopefully, this issue of *Connections* will push things in the right direction.

REFERENCES

ADI[2]. 1994. Belgium - Declared and Real Priorities of the Sûreté d'Etat. *Intelligence*, 254(12), December 1994.

ADI. 1996. Link Analysis Data Mining with Alta's Netmap. *Intelligence*, 287(13), May 1996.

ADI. 1997. Mobile Phone Technology Makes It To The Courts. *Intelligence*, 58(21), April 1997.

ADI. 1998a. Network Analysis 'Makes the Big Time' in Intelligence. *Intelligence*, 327(30), March 1998.

ADI. 1998b. Computers - EU Project Crosses the Irish Border. *Intelligence*, 328(20), April 1998.

ADI. 1998c. Russia - Internet & Economic Security under New FSB Chief. *Intelligence*, 334(7), September 1998.

ADI . 1999. More NSA Technology Information. *Intelligence*, 108(13), December 1999.

ADI . 2000. Intelligent Study of Dutch Organized Crime Leads the Way. *Intelligence*, 118(5), June 2000.

Klerks, P.P.H.M. 2000. *Groot in de hasj: Theorie en praktijk van de georganiseerde criminaliteit* ("Big in Hash - Theory and Practice of Organized Crime"). Politie Studies No. 26. Alphen aan den Rijn, NL: Samson Publishers.

Makarenko, T. 2001. Transnational Crime and Its Evolving Links to Terrorism and Instability *Jane's Intelligence Review*, November 2001.

McGehee, R.W. 1983. *Deadly Deceits: My 25 Years in the CIA* . New York: Sheridan Square Publications.

Milne, S. 2001. Terror and tyranny: What powerful states call terrorism may be an inevitable response to injustice. *The Guardian* (London), 25 October.

US Department of the Army (1948), Fundamentals of Traffic Analysis (Radio-Telegraph) *Department of the Army Technical Manual TM 32-250* and *Department of the Air Force Manual AFM 100-80*, reprinted with glossary and index by Aegean Park Press, Laguna Hills CA (C-66).

van Meter, K.M. and W.A. Turner. 1992. A Cognitive Map of Sociological AIDS Research. In M. Pollak, Ed., *AIDS: A Problem for Sociological Research*, thematic issue of *Current Sociology*, 40(3): 123-134.

van Meter, K.M. and W.A. Turner. 1997. Representation and Confrontation of Three Types of Longitudinal Network Data from the Same Data Base on Sociological AIDS Research. *Bulletin de Méthodologie Sociologique*, 56: 32-49.

[2] French "Association pour le Droit ... l'Information" (ADI, Association for the Right to Information).