THE NETMAP SYSTEM

EVALUATION OF A

TRIAL APPLICATION WITHIN

THE NATIONAL CRIME AUTHORITY

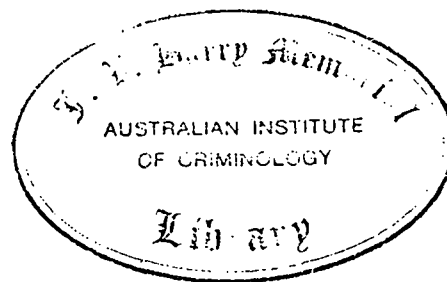**Prepared by the NCA Evaluation Team**

July 1988

THE NETMAP SYSTEM

EVALUATION OF A

TRIAL APPLICATION WITHIN

THE NATIONAL CRIME AUTHORITY

Prepared by the NCA Evaluation Team

July 1988

C O N T E N T S

ANNEX A   –   The Intelligence Process

ANNEX B   –   Glossary of Terms

ANNEX C   –   NETMAP Master Menu

ANNEX D   –   Event Link Types/Source Types used in NCA Trial

<u>A REPORT ON THE JOINT NCA/NETMAP TRIAL OF</u>
<u>CUSTOMISED NETMAP SOFTWARE</u>

<u>Prepared by the</u>
<u>NCA EVALUATION TEAM</u>

<u>INTRODUCTION</u>

1.   In late 1987, NETMAP International Pty Ltd applied to the
Australian Criminology Research Council for a small financial grant to
fund a joint trial with the National Crime Authority in Sydney, of NETMAP
software customised for specific applications in a law enforcement
intelligence environment. The funds were needed to defray programming
costs involved in the customisation and workstation hire charges as the
software runs on an APOLLO 4000 series workstation which was not
available within the NCA.

2.   The primary goal of the trial was to determine the viability of
the NETMAP software to assist law enforcement intelligence analysts in
their examination of criminal and/or suspected criminal organisations
through visual analysis technology (V.A.T.) with a view of gaining a
better understanding of current criminal relationships and to facilitate
efficient and effective methods of targetting. Subsequent possible goals
considered were, pattern analysis of movements of persons of interest eg.
by motor vehicle, as an air passenger etc., and possibly, money transfers.

3.   It was decided that viability would be tested by processing
three types of current data via manual data entry to the NETMAP System
(electronic transfer of data to be examined at a later stage) from three
separate and distinct sources:

    .   data from telephone intercept product;

    .   data from visual surveillance reports/running sheets; and

    .   data from all other sources such as informants, documents,
          transcripts of hearings etc.;

and to display that data to indicate the strength and frequency of
association between individuals. Telephone numbers, addresses, business
organisations and vehicles were to be recorded and displayed where
appropriate.

4.   The following objectives were then decided:

    .   to identify what advantages the customised NETMAP software
          might offer to persons involved in the analysis of events

associated with, or contacts between, known or
suspected criminals and their activities;

. to gauge the capabilities and advantages of the
customised NETMAP System for the above purposes
vis-a-vis manual and conventional ADP techniques,
(with particular regard to minimisation of the human
fallibility factors, utilisation of "what-if?" factors
and the simulation of alternative scenarios and
possible courses of operational action); and

. to establish whether the customised NETMAP System is
able to provide "measurable" assistance to criminal
investigations (and whether it is capable of doing
this in a timely and cost-effective manner).

5.   The trial was intended to run for some 12 weeks but this time
frame had to be extended due to the fact that the Authority's Telephone
Interception capability was not realised during the time of the trial and
an alternative area of potential use, received more concentrated
attention.

6.   The trial evaluation team consisted of:

. Mr Bryan Pannell, Director Intelligence, NCA
. Mr Howard Clarke, Senior Intelligence Analyst, NCA
. Mr Terry Brophy, Intelligence Analyst, NCA

and was conducted under the guidance of Dr John Galloway, Director NETMAP
with programming assistance from Mr Philip Magson also of NETMAP.

CONDUCT OF TRIAL

7.   The initial phase of the trial involved the documenting of user
(NCA) specifications by the NETMAP programmer in conjunction with NCA
intelligence staff, for three sub-application areas:

. a technical surveillance (TS) Analysis sub-system;

. a physical surveillance (PS) Analysis sub-system; and

. an "Other Information" (or general intelligence)
sub-system.

Having established the user requirements, NETMAP were quickly able to
design and format appropriate data entry and enquiry menus for the
sub-systems (these are described later in this report). The
"customisation" was a continuing process as prototype menus were
experimented with and the necessary enhancements and modifications
identified and made.

Rationale: Three Sub-Applications

8.   In complex or long running investigations it is recognised that
there is potential for considerable loss of valuable intelligence through
the non-integration or correlation of all connected events and persons
(particularly unidentified or partly-identified persons).

A technological solution to this problem has been needed for sometime and with this in mind, the team undertook to develop a system which would provide advanced collation (sorting) and analytical support to intelligence analysts in the processing of data derived from numerous sources. (The Intelligence Process followed by an analyst is outlined at ANNEX A)

9.   The NETMAP software has already demonstrated its effectiveness in various commercial application areas in facilitating analysis of relationship and communication patterns and in detecting networks and graphically displaying those networks and associated linkages. The indications observed by the team are that the applicability of this software in addressing the technological problem identified above are that it is likely to be both appropriate and successful.

10.   The team's primary aim was to develop enquiry menus which would permit an analyst to look at captured data (through a series of netmaps) in a variety of ways, and thus allow him/her to modify search parameters quickly and efficiently. The NETMAP system was found to lend itself to this type of customisation and appropriate data entry and enquiry menus were developed (and subsequently modified) without difficulty.

TS Sub-system

11.   Typically, under conventional arrangements, analysis of this type of product is concentrated on a call-by-call basis utilising the hard-copy transcript of conversations with pattern analysis and event correlation being conducted utilising an analyst's mental recall and supporting information retrieval systems.

12.   In the early stages of the trial, efforts concentrated on historic telephone traffic data which was entered onto the system via keyboard. This was found to be a simple, relatively small and comparatively problem-free process (for this particular sub-application) because the data flow was manageable and there was a limited amount of data generated on a day-to-day basis. The result of this limited exercise was encouraging in that clear traffic patterns were evident on the netmaps produced. Furthermore, the netmaps compared favourably (both from the points of accuracy and clarity) with hard-copy TS traffic charts which had been produced previously within the Branch and also, had the advantage of being readily updated electronically whereas the other charts/diagrams had to be physically re-drawn every time a new batch of data was added and as the overall traffic pattern changed.

13.   As the overall trial progressed it became apparent that slippage in the proclamation date for legislative amendment to the Telephone Interception Act would impact substantially on the evaluation of this sub-system. The NCA would be delayed in commencing it's own telephone intercept operations (and complimentary surveillance operations) until at least July 1988. Consequently there was a need to change trial priorities and therefore NETMAP was asked to concentrate customisation work on the third sub-system, 'Other Information'. Initially, this sub-application was intended only to be a supplement to the TS and PS sub-systems. However, before describing development on this front, further explanation is warranted on the TS sub-system development.

TS Data Input Menu

14.   Recognising that particular types of information would become available concerning telephone calls to/from targetted telephone services and that analysis of telephone traffic patterns would be facilitated by examination of the data according to various "mixes" or combination of data categories, the data entry format with associated information categories, was developed as described below.

15.   In a telephone interception operation, the following information which is relevant for intelligence analysis purposes, will normally be recorded: date of call, time of call, direction of call, details of target telephone service (and subscriber), whether local/STD/ISD, whether English or foreign language spoken (or both), and conversation details. Sometimes the identities of callers will be known (sometimes it will have to be established by other means). The number being called from the targetted telephone service (outward call) will normally be recorded but not the source of inward calls, though sometimes the caller may divulge this detail in conversation or it may be established through analysis. Other information can be derived or reliably interpreted from the foregoing raw data, ie. category call (type), length of call, identities of call participants etc. Call categories maybe based upon a call "type" allocated to each telephone conversation, eg. drug-related, business, family/social, "suspect" (exact nature unclear but probably involves illegal/criminal activity or planning or conspiracy). It was also recognised that a single telephone call may involve more than one topic, eg. a social conversation and a "suspect" conversation with another individual.

16.   With these factors in mind, data entry categories were identified and are described as follows.

(a)	**Date:**	the date on which the telephone call occurred.
(b)	**Time:**	the time of the telephone call.
(c)	**Call Flag:**	this is to signify whether there was only a single conversation involving two parties (coded "0"), or there was a second conversation on the same call involving a third party (coded "1") or a third conversation on the same call involving a fourth party (coded "2") etc.
(d)	**Transcript Reference:**	this is to be a reference to the hard-copy (transcript) reference document, to which the particular line of data entry is sourced.
(e)	**Incoming/ Outgoing:**	indicates whether the telephone call was "incoming" or "outgoing" with respect to the targetted service.
(f)	**Target Name:**	the identity of the person speaking on the targetted telephone service (unique numeric identity codes are used in lieu of names – for the purposes of the NETMAP system

processing data; on-screen, the name and the identity code both appear on the netmap).

(g) **Other Party:** the identity of the person who has contacted, or has been contacted from the targetted telephone service and who was the other party to the conversation (again represented by identity code).

(h) **Telephone:** the telephone number of this "other party"; with an outward call from the targetted service this will be automatically recorded, however, for inward calls this will not be known unless divulged during conversation or established through research/analysis (eg. known to be the same telephone service occurring on a previous documented occasion where the telephone number was established).

(i) **Length Of Call:** as the times of commencement and termination of calls is recorded, then call length can be easily established and may prove valuable for pattern analysis purposes.

(j) **Local/STD/ ISD:** merely records whether the recorded call was of a local/STD/ISD nature.

(k) **Language:** records whether recorded conversations were conducted in English or a foreign language (the system can be set up to record varieties of foreign language, eg. Mandarin Chinese, Italian, etc.)

(l) **Category Of Call:** based on conversation subject matter, the primary content of the conversation is assessed in accordance with specific categories eg., drug-related(d), corruption(co), criminal-other(cr), suspect(su), business(b), family(f), social(so), not known (n), other(o), unanswered(u), absent party(a).

17.   The processing of data from TS transcript involves an intelligence analyst examining each call and recording a one-line assessment/summary of that call in accordance with the foregoing required information items. The exception to the one-line-per-call entry will be the multi-conversation call where the analyst will record a one-line entry for each conversation recorded within the single telephone call (refer the "Call Flag" item explanation). All but the last item (category of call) could be considered factual as against interpreted data. The following depicted Telephone Intercept Analysis data entry screen is the means by which a trained typist/WPO enters the coded date into the NETMAP system. Refer Illustration 1.)

TELEPHONE INTERCEPT ANALYSIS

Target #

Date	Time	Call Flag	Transcript Reference	Incoming/ Outgoing	Target Name	Other Party	Telephone	Length of Call		Local/STD /ISD	Language	Category Of Call
		0		incoming ¦				0	0	local_cal ¦	english	drug_rel

EXIT

Illustration 1

TS Analysis Enquiry Menu

18. Given the range of data provided to the NETMAP system via the TS data entry facility, an extensive range of enquiries (including multiple-part enquiries) can be addressed to the netmap data. In principle, the data presented on a netmap developed from TS data focuses on telephone traffic links between individuals or between telephone numbers, and on actual or perceived groups of individuals reflected in the data. In examining netmaps of such data, patterns will emerge causing questions to be prompted, the answers to which might suggest the relative significance or importance of particular individuals in criminal groups or in the overall scenario. The implications of such knowledge (intelligence) for investigative targetting, are obvious.

19. Whilst data maybe entered separately for each TS project (i.e. each TS operation) netmaps can be viewed on the basis of individual TS cases or all TS operations collectively (thus permitting examination of investigation or traffic pattern overlaps). A description of the menu utilised for these purposes and associated menu items follows but the reader should refer to Illustration 2. At the conclusion of the following description, comment is made on the "parameters" menu which also impacts on the way NETMAP data ia displayed on-screen. Both "link" menu and "parameters" menu (PARAM) are accessed through the NETMAP "applications" menu. (See ANNEX C)

NOTE: A Glossary of Terms is located at ANNEX B.

DE	ALL NODES	No Link	0			
	OFF					
	OFF					

PHONE MENU 1

CATEGORY	LANGUAGE	TYPE OF CALL
Categories	☑ All Language Spoken ..	☑ All Type of Call. .
g Related	☐ English	☐ Local
ruption	☐ Foreign	☐ STD
er Criminal	☐ Both	☐ ISD
ness		

All CONVERSATIONS | AT LEAST | 0 | 0 | ONLY | AT LEAST | 0

al/Family Matters
Known/Other
ted Party Absent/Unanswered

| if | Number of calls | AT LEAST | 1 | ONLY | Number of calls | AT LEAST | 1 |

| | ON | | QUIT | | Width base 0 Width Divisor 0 | Link Width : Nothing (Width = 1) Link Colour : Green |

Illustration 2

(a) Link Menu

(1) The user is first offered a choice of link/node combinations to be viewed. The options, accessed through the "INCLUDE" menu item, are controlled by a 'switch' (ALL LINKS; LINKS BETWEEN; LINKS TO/FROM) allowing the user to choose one of those selections. Another 'switch' allows the user to choose in conjunction with the foregoing choice either HIGHLIGHTED NODES or SPECIFIC ID CODE/S). The resultant range of choices are:

    — all links to/from all nodes;

    — links to/from a specified node (i.d. code nominated by user);

    — links to/from two specified nodes;

    — links between two specified nodes;

    — links to/from "highlighted" nodes;

    — links between "highlighted" nodes; and

    — links between specified node and "highlighted" nodes.

(2)   The user can then choose to ignore date/time
         considerations or choose to examine the data
         according to various date/time parameters
         (eg. all telephone calls after 010188, or all
         calls from 1400 hours to 2000 hours on any
         day, or all calls between 010188 and 150188;
         (refer DATE and TIME fields).

(3)   As was indicated in the TS data entry menu,
         telephone calls have been categorised
         according to conversation content and the
         enquiry sub-menu provided under CATEGORY
         allows the user to examine the data according
         to call category eg. look at drug-related
         conversations only, or drug-related plus
         other criminal type communications (any other
         combination) or all categories; the resultant
         netmap will represent the different types of
         conversations between parties by colour-coded
         links. (CATEGORY field refers - see
         Illustration 2.)

(4)   Conversation links can be examined further
         according to the language spoken, eg. examine
         links through conversations only in a foreign
         language, or English only, or both.
         (LANGUAGE field refer' - see Illustration 2.)

(5)   Links established by calls can be
         differentiated for analysis purposes
         depending on whether the user is interested
         in local calls, or STD calls, or ISD calls;
         but if preferred, these choices can be
         ignored and all calls can be included in the
         netmap. (TYPE OF CALL field refers - see
         Illustration 2.)

(6)   The field ALL CONVERSATIONS/CALLS provides a
         switch whereby the user can choose to examine
         telephone traffic on a call or conversation
         basis (the distinction being highlighted in
         the explanation of the TI data entry menu
         refer paragraph 16 (1))

(7)   The NUMBER OF CALLS field allows the user to
         have the netmap display only those telephone
         traffic links which satisfy the selected
         criteria, i.e. a minimum number of calls eg.
         say at least three (otherwise no display), or
         a maximum number of calls say more than five
         (or disregard) or on exact number of calls.

(8)   LINK WIDTH/COLOUR options allow the user to
         vary the colour or width of link displays (or
         both), eg. multiple calls will show as a
         multiple link band, and selected call types

		SURVEILLANCE ANALYSIS			
Date	. Time	Document Reference	1st Entity ID	2nd Entity ID	Type of Event
					arrive_at

EXIT

Illustration 3

(a) **Date:** date on which surveillance observation occurred.

(b) **Time:** time at which surveillance observation occurred.

(c) **1st Entity Id:** to record the identity code for the first entity featured in the occurrence (the entity being either a person, a vehicle, or a location).

(d) **2nd Entity Id:** to record the identity code for the second entity featured in the observed occurrence (which involved the first entity).

(e) **Type of Event:** to record the event linking the two entities, eg. person/vehicle arrives at location, person drives vehicle, person/vehicle departs from location, etc; a standard set of most commonly-occurring "events" were established for use with the surveillance menu.

(f) **Exit:** allows the user to exit from data entry mode.

Physical Surveillance Enquiry Menu

22.   This menu was not developed due to time and human resource availability.

'Other Information' Data Entry

23.   A third type of data entry format was developed to cater for information from all other sources (ie. exclusive of TS and PS). The primary purpose of having such a third level of information processing was to provide for correlation between event and date-specific information derived from TS and PS activity and that derived from all other means (eg. seized documentation, informant information, other investigations and enquiries, relevant material on agency files, etc). The effect of this third dimension of information collation and analysis will be a more complete 'picture' than would otherwise be the case.

24.   This data entry menu is a more detailed version of the PS Menu and this is necessary in order to give the range of information source types, the accuracy of information itself and the reliability of the associated sources. The information entered into the NETMAP system via this menu will reflect the variety of information sources and reliability/validity weighting given to information sources and the information itself.

25.   The data entry menu items (refer Illustration 4) are:

(a) **Date:**   date on which event/relationship occurred.

(b) **Time:**   time at which event occurred (if known).

(c) **Document   relevant file/folio or running sheet
     Reference:**   reference.

(d) **Source Type:**   this provides for the entry of a
                          two-character source code representing the
                          range of commonly-occurring source types,
                          eg. address book(ad), bank
                          records/statements(ba), informant source
                          (if), passport information(ps), etc.

(e) **Source   records the source reliability grading
     Reliability:**   using the Admiralty System (a-f values) as
                          used widely in law enforcement circles in
                          Australia and overseas.

				OTHER INFORMATION DATA ENTRY				
Date	Time	Document Reference	Source Type	Source Reliability	1st Entity ID	2nd Entity IC	Type of Event	Link Confirmed /Suspected
27	1200	12-3	do	a	0001	4327	qp	confirmed

Illustration 4

(f) 1st Entity Id: records the identity code for the first entity (node) featured in the event/relationship.

(g) 2nd Entity Id: records the identity code for the second entity node) featured in the event/relationship.

(h) **Type of Event:**   used to record the nature of the event or relationship linking the two entities; an extensive list of event link types was compiled, eg. accomplice(ac), common address(ad), solicitor(sl), travel companion(tr), etc. (this extensive listing was also summarised down to eight link categories which are used for enquiry/search purposes – see 'Other Information' Enquiry Menu description).

(i) **Link Confirmed/ Suspected**   this provides for the user to record whether the event/relationship link is confirmed, suspected or of an otherwise unconfirmed nature (recording this detail allows the user to enquire on the basis of confirmed information only if he/she desires).

Other Information Enquiry Menu

26.   This menu permits the system user to examine netmaps compiled from all other information sources (i.e., exclusive of TS and PS sources) and provides for examination of data according to a range of concerns and preferences as to source type, source reliability, confirmed/non-confirmed information, etc. A netmap can be presented to the user on the basis, for example, of confirmed information, or exclusive of informant information. Comparisons can be made between netmaps (and the pre-defined and emergent groups displayed therein), utilising all sources/information types (irrespective of quality) and netmaps produced from a narrow information field, eg. confirmed information/first-rate sources. Differences in the 'pictures' so presented can be noted mentally and can prompt the analyst to ask questions that hither to may not have been obvious or even considered. The answers to these questions may have critical implications for investigative planning or targetting, eg. a key group or individual may only be central in the perceived scenario on the strength of 'doubtful' information. The new knowledge may lead to a setting aside of previous perceptions or the instigation of more keenly focussed information-gathering activities to clarify the doubtful facet or situation.

27.   A description of the link menu utilised in examining this 'other information' follows (refer Illustration 5).

(a) <u>Link Menu</u>

    (1) The choice of link/node combinations to be examined is identical with that provided for TS analysis (refer sub-paragraph 19(a)(1)). The particular enquiry options are standard for both TS, PS and Other Information enquiries.

    (2) As with TS, the system user can choose to examine data according to various date/time parameters. The enquiry options are identical to those utilised for TS (refer sub-paragraph 19(a)(2)).

    (3) The specific selections to be utilised for enquiry purposes follow in the subsequent block on the screen, titled 'Other Information' Menu and comprising:

        –   Link Type Category/Link Type

        –   Source Type

        –   Source Reliability

        –   Confirmed/Non-Confirmed

    Each of these sub-menus contains multiple choice boxes from which a selection may be made by 'clicking' (mouse) over the appropriate box, with the system placing a tick (✓) alongside the selection. The various choices can be ignored in each sub-menu by selecting 'All Links/Types' (and this can be made the default or automatic selection by the system, if preferred).

    (4) The link Type Category/Link type sub-menus feature a switch allowing the user to work from either of these sub-menus, depending on whether one wishes to work from very specific link types or from broader (summary) categories. The Link Type Categories feature the broad range of linkages which may be evident between persons, persons/institutions, persons/locations, eg. criminal activity link, financial link, family link, etc. The Link Types cater for very specific (descriptive) linkages which, when viewed on-screen, provide the user with a clearer understanding of the nature of associations between entities featured in the netmap, eg. a co-offender link, an accomplice link, a business partner or travel companion link. The use of these link types helps reduce the ambiguity of the broader link categories when analysing specific netmaps. The specific link types utilised can be made to conform with the linkage types utilised on the client agency's mainframe system (this was the case at NCA). A full list of the Link Type Categories and Link Types utilised in the NCA trial is attached at ANNEX D.

(5) Using this facility the user may choose to see a netmap showing those persons linked by particular types of relationships, eg. drug involvement links, or particular combinations of relationships, eg. drug involvement links plus travel links. Alternately, these can be ignored by selecting "All Link Types". Using the link colour facility a variety of link types can be viewed simultaneously, being distinguishable to the user through the different link colourings.

(6) A range of standard information source types was noted and by selecting the source types of interest, or combinations of source types, the data attributed only to these selected information source types will be viewed. As with Link Types/Categories, a netmap of criminal groups, of individual persons can be viewed from the perspective of information source allowing the user to judge the strength/weakness of the information collection effort, information deficiencies, possible over-reliance on informant information in certain quarters, etc. This perspective can be viewed by choosing to have the various source types differentiated by link color.

(7) Source reliability is a factor of great importance to law enforcement officers and the use of that particular sub-menu will be obvious to persons familiar with information evaluation practices. As each item of information entered onto the system will carry an "a" - "f" reliability grading, the user is able to examine data according to source reliability, ie. examine data only from usually/or completely reliable sources. In addition, using the same rationale described at sub-paragraph 27(a)(5), a netmap can be examined from a source reliability perspective, using the link colouring facility.

(8) Discriminating users of the NETMAP system may, at times, only be interested in viewing criminal networks established from confirmed data. The Confirmed/Un-Confirmed sub-menu allows this 'screening' process to occur. The "All Links" choice can be selected if the user only wishes to get a general overview of the situation, irrespective of the un-confirmed nature of some of the data.

(9) The "Number of Links" field allows the user to examine only those relationships satisfying the selected criteria, eg. where three or more links/link events exist between entities. Similarly a range of link occurrences may be selected, excluding isolated link events.

(10) Link Width/Colour options are identical to those on the TS Enquiry menu and the comments at paragraph 19.(a)(8) apply also here.

(11) The OK/QUIT options are also identical to those available on the TS Eqnuiry menu (refer sub-paragraph 19(a)(9)).

INCLUDE	ALL NODES	in Code		u	AND	the Code		u
DATE	OFF		:	:	AND		:	:	
TIME	OFF		no. pm		TO			nn nn	

'OTHER INFORMATION' MENU 1

LINK TYPE CATEGORY	SOURCE TYPE	SOURCE RELIABILITY	CONFIRMED/SUSPECTED
☐ All Link Type Categories	☐ All Source Type	☐ All Links	
☐ Criminal Activity Involvement	☐ (AD) Adress Book		☐ All Links
☐ Business Dealing/Association	☐ (BA) Bank Records/Statements	☐ A - Completely Reliable	
☐ Financial Link	☐ (DO) Document Source	☐ B - Usually Reliable	☐ Confirmed
☐ Documentation Link	☐ (IF) Informant Source	☐ C - Fairly Reliable	
	☐ (OB) Observation Sheet		
☐ Travel Link	☐ (PS) Passport Information	☐ D - Not Usually Reliable	☐ Suspect
☐ Some Contact(meet/phone/letter)	☐ (PM) Passenger Card Information		
	☐ (PO) Other Police Records	☐ E - Unreliable	
☐ Family/Social	☐ (PU) Other Public Records		☐ Unknown
☐ Other Link	☐ (RS) Running Sheet (NCA)	☐ F - Reliability Unknown	
	☐ (TE) Teledex		

| Drawlink if | Number of Observations | AT LEAST | 1 | ONLY | Number of Observations | AT LEAST | 1 |

| Select Menu | OK | QUIT | Width used u | Link Width : Nothing (Width = 1) |
| | | | Width Division u | Link Colour : Multi-colours |

Illustration 5

RESULTS AND CONCLUSIONS

28.   The foregoing explanations though brief, illustrate the rationale used and the concepts visualised by the Trial team in customising the existing NETMAP software to specific law enforcement intelligence applications. Obviously, much more could be said about the individual experiments and "in-part" trials conducted by the team which were both intriguing and exciting from a developmental view point.

29.   Considering that the trial had to be conducted within the confines of largely historical data, and competing operational priorities in relation to analyst man-hours available for the trial purposes; plus the fact that operational TS data was not available because the T.I. Act had not (and still has not) been proclaimed, the outcome was very encouraging and in the team's view, vindicated their earlier vision of producing the original intelligence officer's "crystal ball".

30.   The Trial Team's view is that the NETMAP software, appropriately customised, is indeed a prototype "crystal ball". However like all new equipment and the user skills that go with it, this system needs practise on the part of the user in order to become expert in all facets of interpretation and in its practical uses to render the "crystal ball" clear and not opaque or even cloudy.

31.   In relation to the specific objectives of the trial the following comments are appropriate:

    a.   The advantages of the NETMAP software to an intelligence analyst are:

        (1)   The in-built discipline of the system ensures that all data entered is properly evaluated and categorised thus enabling the user to see all data displayed in its pre-determined value ie, there is no place for "garbage" input and therefore the data base is clean even though some of the data might be unconfirmed. This factor is obvious to the user.

        (2)   The options provided to the user via the various menus cause the user to think far more extensively than he perhaps might if not using this software. eg. the NETMAP pictures are "worth more than a thousand words" in that they can display data and the user can manipulate it, to show specific emerging patterns. Thus the analyst can view all relevant data from different perspectives very easily and quickly. This is the beginning of visual analysis technology (VAT).

(3) When the analyst identifys the most suitable netmap for his oral briefing or written assessment, he can produce a "hard-copy" netmap for these purposes very quickly (in minutes as compared with hours or days to manually prepare a link diagram). As more up to date data is entered or unconfirmed data is confirmed, the netmap picture can be adjusted electronically and new netmaps produced to reflect the current situation which then can be compared with the previous netmap. Such changes, which are very obvious to the analyst, also cause questions to arise and answers to be found resulting in more new knowledge for the analyst to add to his comprehension and understanding of the situation; thus he is in a better position to more accurately brief and advise his operational commander/decision maker.

(4) The above matters considered, the analysis of events associated with, or contacts between, known or suspected criminals and their activities is greatly enhanced using the customised NETMAP software. Depending on the skill, initiative and inquisitiveness of the user, the advantages of this system over manual and indeed other electronic systems are considered by the team to be significant. Visual Analysis Technology is a quantum leap forward for intelligence analysts.

b. The capabilities and advantages of the customised NETMAP system are too numerous to describe comprehensively and also briefly; however, given high quality data entry/capture either manually or electronically, the human fallibility factor in relation to the production of netmap-v-link diagrams and other forms of event flow charts etc., is considered to be minimised to the greatest extent possible. In relation to the utilisation of "what-if" factors and the simulation of alternative scenarios etc., these exercises can be conducted with accuracy and speed.

c. Due to the nature of the data entered during the trial ie. (it was mainly historical), it is not possible to say that the third objective was adequately met; however, on one occasion data relative to more than 10 link diagrams produced by hand over a period of seven days, was entered manually to the netmap system in 4-5 hours and then displayed on screen and printed in hard copy form immediately. In performing this exercise, inconsistencies in the hand drawn diagrams were picked-up immediately. The trial team concluded therefore that netmapping is both a timely and cost effective way for analysts to support criminal investigations.

32.   This report, in some respects, is "thin" insofar as the details of the many experiments undertaken by the team analysts during the trial. However, the evaluation team is of the view that the NETMAP software has many definite advantages over other systems (both manual and electronic) known to the team and that its potential to improve an analyst's capability to produce timely and accurate reports, charts etc., particularly in relation to law enforcement intelligence, is quite high.

THE INTELLIGENCE PROCESS

The word "intelligence" can be defined in numerous ways but to those people who claim to be members of the law enforcement intelligence community, its definition is, in simple terms, a comprehensive sum of knowledge of persons engaged in, or at least associated with, criminal activities. Such knowledge includes the full personal particulars of these persons, where they live, who their associates are, what their methods of operation are, their particular skills, their criminal history, and an understanding of what their strengths and weaknesses are and to what type of investigation they might be vulnerable.

The accumulation of this knowledge is often a long and laborious task that requires patience, diligence, determination and perseverance on the part of the Intelligence Analyst as he follows the long established "intelligence process", step by step. He must first study all of the collected data relative to the suspect or criminal or criminal activity of particular interest and interpret its meaning or significance. In the process of completing his study of the data or his assessment of the situation, he will identify 'gaps' in his information data-base and in order to be sure that his assessment is balanced, he will need to eliminate most of those gaps as quickly as possible. In any "intelligence" environment, timeliness is most important because new knowledge is of little use after the event it relates to - 'fore' knowledge is a far more valuable commodity than 'after' knowledge.

The collection of new information to fill these data-base "gaps" is, in itself, a task which requires attention to a number of details and involves continual checking to ensure that the information being collected is what was asked for and that it arrives in time to be put to use.

As new information arrives at the Intelligence Office (some in response to specific requests for information to eliminate knowledge deficiencies and some unsolicited, from all manner of sources) it all has to be evaluated for its relevance and pertinence to the various subjects of interest and also for its accuracy. Sources of information have to be considered as to their reliability and consistency for providing accurate information. Officers performing this evaluation obviously require a broad and also sound general knowledge of many and various subjects of interest in the first instance and secondly, need to have the skills and technical capability to test the new information rigorously before accepting it for unqualified inclusion in their data base. Even so, on many occasions, new information will have to be added to the data-base with the qualification that it is as yet unconfirmed.

Part of the evaluation process involves comparing the new information with what is already held and then deducing the reliability of the source and its probable level of accuracy. At times this

comparing will enable the officer to enhance the original information by adding relevant and accurate snippets from other areas of the data-base. All of this activity helps to "flesh-out"the data-base and steadily eliminate potential information deficiencies in future assessments.

The next step in the overall process that the Intelligence analyst must follow is to collate the various items of new information with like items in the data-base and also with his particular study or assessment, where the new information is most relevant. On many occasions there will be a need to cross-reference the new information to other items of information in other subject areas of the general data-base as well as to the particular matter of immediate interest. Modern technology can assist greatly with these latter requirements and "links" can be noted very easily using computers.

Having reached this stage of the Intelligence Process, the analyst is finally in a position to perform his primary function - to analyse all of the information, new and old, in his possession. The new information hopefully, will fit into the previously identified gaps in his knowledge like the completion of a mental jigsaw puzzle. Often though, the clarity of the mental picture perceived by the analyst will be less than desirable and he will need to hypothesise as to the true situation. Often the picture will be clouded by misleading or vague or unconfirmed information; or partly eclipsed by competing subjects of interest; or extraneous matters such as those of an administrative nature - all of which inhibit the analyst's ability to focus his mind on the total spectrum of available data relevant to a single subject of intelligence interest. The consequence in such situations is that often, small but nevertheless important aspects can be overlooked or that their relative importance or significance is reduced to the extent that they are ignored. "Indicators" of what is happening or about to happen, are most important to an analyst.

The final part of the Intelligence Process involves the analyst in preparing a report which will represent a comprehensive understanding of the meaning or significance of the subject of interest, in time for the operational planner and decision maker to consider the analyst's assessment, finalise his plan of action and execute it.

The analyst's report/assessment will usually be in writing supported by graphs, charts, photographs and the like but on many occasions it will be presented orally, in person. When this occurs, graphic aids will be used to support and illustrate key aspects of the assessment.

To follow this "process" successfully requires high standards of self-discipline; it also requires enormous attention to detail and a high level of intellectual honesty on the part of the analyst who, at all times, is subject to the human frailties associated with stress, competing priorities and demands and other numerous distractions.

Intelligence analysts in the law enforcement community are no different to intelligence analysts in other disciplines – their desirable personal attributes and skills are similar across the board. One area or analytical endeavour though, while not totally peculiar to law enforcement operations, is demanding of particular attention on the part of intelligence analysts. It is known as targeting; that is, the selection of targets (persons) to be investigated. In current times, it is imperative that the most cost effective methods be used and the deployment of the least number of human resources and costly capital equipment be achieved, while maintaining the actual aim of neutralising a particular criminal activity and the successful prosecution of the associated offenders.

Identifying and prioritising potential targets for investigation is just another facet of the law enforcement intelligence analyst's duties; but this task, perhaps more than some other analytical tasks, requires particular attention to detail in the collation of data, linking, and the recording of the date and time of events. The task lends itself to the production of flow charts and organisational diagrams which assist the analyst to understand how various persons and groups of interest, relate to each other; and the likely levels of influence one might have on another. It is a time consuming activity which places additional demands on the personal skills of the analyst by requiring him to organise his data pictorially; to draw neat diagrams; and to print clearly. He needs to be able to scale the diagrams so they can be used either in face to face presentations or to support a written report. In other words as well as having good intellectual, analytical, conceptual and communication skills, the analyst needs to be an experienced draughtsman.

GLOSSARY OF TERMS

Attribute: An item of personal detail or a characteristic of an individual node (usually a person, or a telephone number).

Call Category: This is used in the Telephone Intercept (TI) sub-system, and indicates the type of conversation (subject matter) that has occurred; a standard set of call categories (refer Illustration 2) was developed to represent the common types of conversations encountered and of interest for analysis purposes.

Call Flag: This term, used in the TI sub-system, indicates which of multiple conversations in a single telephone call is being referred to, eg. 0 = single conversation call, 1 = second conversation, etc.

Emergent Group: A group of nodes (usually people, but may include vehicles, addresses, telephone numbers) who together share more linkage with each other than they do with nodes outside the group. This netmap chart is the _informal_ organising of nodes (entities) to depict trends in group activities Each group is relatively cohesive because of the characteristic that most linkage is shared. The concept of emergent group is probably more meaningful in a relationship sense when people nodes are being considered, although when a non-person node (eg. vehicle, telephone number) features in a group, the question must be asked, "why is this node here?" and "who is the person behind/associated with this node?"

Those groups are "emergent" out of the linkage data, in that they are based on any pre-defined criteria such as family (whether actual/crime family), investigation connection, etc. or any other node attributes. A pattern recognition routine examines the links in the relevant network and classifies nodes into one of four categories, ie. isolates, attached isolates, liaisons, group members.

Entity: This is something that has a real existence, or identity (most frequently a person, but can be an address, a vehicle, a telephone number). It is an alternative name for a node.

Event: This is an occurence which is of relevance for investigation and/or analysis purposes and which provides a link between two or more nodes/entities, eg. links person-person, person-vehicle, person-address, telephone service-telephone service, etc.

Group Members: The members of an emergent group together share more linkages with each other than they do with others. The netmap program uses the following criteria:

a. there are three or more nodes in a group; and

b. each nodes has two or more links within the group; and

c. each node has at least half of it's links to others within the group.

I.D. Code: Each node (entity) is identified within the system by a unique computer generated identity (i.d.) code. Netmapping operations are conducted using this code rather than the entity name, even though that name is displayed on-screen; data entry and enquiries conducted in relation to specific entities both require use of this i.d. code.

Isolates: This is a category of node (entity), recognisable in "emergent group" mode, which has no links to other nodes in a particular network. Using a "what if?" question, involving a different definition of the linkages, the user may find that certain nodes do not remain as isolates. Isolates may be either attached isolates (minimal or indirect links to a network) or detached isolates (thoroughly detached, with no links to the network).

Link: A relationship existing between two entities, either by virtue of fact (eg. family, employee/employer relationship) or as determined by events (eg. meeting, payment, telephone contact).

Liaison: These are nodes (entities) which provide a linking function between various emergent groups but which are not themselves members of those groups.

Netmap: A diagram which displays networks, showing the links between group of nodes and within each of the groups. The system has two styles - pre-defined and emergent groups.

Network: Fundamentally, this is a set of nodes (entities) and links - where the key entities are people and links are the relationships or specified dealings between them. In the Intelligence Application of the Netmap system, the networks recorded will primarily be social and criminal networks.

Node: This is a basic unit or component of the system, an entity, which is capable of being linked to other nodes via relationship or event (eg. persons, vehicles, locations, etc).

Pre-defined Groups: These are groups or categories of nodes, so established through the sharing of common attributes or values (eg. type of node, name, family, etc). This netmap is the more _formal_ organisation of nodes (entities).

Source Reliability: The reliability grading allocated to the information source responsible for each item of information (based on the Admiralty "a-f" system used by most law enforcement agencies in Australia and other western nations).

Source Type: The type of information source from which data has been obtained for netmap processing; a list of such source types and corresponding abbreviations was developed during the NCA evaluation trial for use with the Intelligence Application.

NETMAP MASTER MENU

This menu is presented to the user following selection of the appropriate project area on which it is intended to work. It is an enquiry menu not a date entry menu (which are elsewhere described).
The master menu comprises those basic selection options essential to accessing any specific enquiry function and either viewing consequential graphics in a number of ways or plotting the image.

These menu selections are as follows:

EXIT: terminates the NETMAP enquiry session and takes the user back to the NETMAP logo and the preliminary NETMAP applications menu.

FIT: rescales the viewing area to allow the complete NETMAP to be viewed; it is utilised to restore a rescaled (eg. "window" segment displayed) NETMAP diagram to its normal dimensions; size.

ZOOM/PAN: dynamically zooms/pans over the netmap, allowing the user to view the netmap from different perspectives; left mouse button: zooms in – brings the netmap closer middle mouse button: zooms out – moves the netmap further away right mouse button : pans – moves netmap left/right/up/down.

WINDOW: defines a viewing window, allowing the user to select a portion of the netmap to be examined more closely; the netmap will be automatically rescaled so as to display the defined window segment using the full screen.

PARAMS: allows modification of display/processing parameters; selecting this command causes a Parameters menu to appear and selections can be made from offered menu options by pressing the mouse when the cursor is positioned over the preferred parameter choice.

DEFINE LINKS: this is not intended for user/analyst use; it is the equivalent to getting under the bonnet of a vehicle to do "hands-on" maintenance work.

LINK MENU: displays the link selection menu, which provides the user with a choice of linkage types/definitions for viewing the netmap data.

**PRE-DEFINED/
   EMERGENT:**   this switch controls the node grouping style used for the netmap and the two options are alternatives the user must choose between in viewing the netmap. Pre-Defined – nodes are grouped according to pre-defined values (eg. node type, family group, etc.); the attribute value upon which the grouping is based is as previously selected on the Parameters menu. Emergent – node groupings are automatically determined based on the currently defined linkage types (ie. the NETMAP system determines the groupings); basically, a "group" in this mode, is a set of nodes which share more links with each other than they have with other nodes outside their group.

REDRAW: re-displays the netmap after a change in parameter settings (using current parameter valves); a "redraw" is necessary to effect new node groupings, colourings.

HIGHLIGHT: by means of colour highlighting, this enables nodes to be selected/deselected for special attention; highlighted nodes can be excluded from netmapping operations (by virtue of the Parameters menu) and they can also be isolated for examination in relation to their to/from linkages (via the Link menu).

PROFILE: this allows the details of a node to be examined; it contains node attribute details (eg. node type, number of linkages, etc.) as well as textual information about

the node (eg. person profile, vehicle description/registration, etc.); it contains a free text field for the latter purposes and textual date can be down-loaded to it from other mainframe or PC files.

PLOT: produces a hard-copy of the netmap on a HP compatible plotter connected to a serial part on the Apollo workstation; it is the equivalent to a PRINT command on a conventional computer and utilising a colour plotter, coloured A3 reproductions of on-screen netmaps can be produced.

QUEUE: controls plotting of netmaps; decides the manner in which plots are processed, including queuing them and recording chart titles and explanatory notes to be reproduced on the hard-copy netmap.

NOTES: this is an on-screen "note-pad" facility, which permit free-text recording of relevant information about the project or netmap concerned.

HELP: this provides guidance on how to obtain "help" with
NETMAP system functions; it advises that individual
"help" items can be found by depressing the mouse right
button when the cursor is on any menu selection.

EVENT LINK TYPES/SOURCE TYPES

USED IN NCA TRIAL

Event Link Types

gr :	Group Together	le :	Leter/Telex sent to
ac :	Accomplice	qm :	Manager of
an :	Antagonist/enemy	fa :	Family Relationship
bu :	Business dealing	me :	Meeting
nc :	Client	mo :	Money Paid/Transfer
co :	Co-Offender	qt :	Business Partner
cc :	Co-Conspirator	po :	Pornography Involvement
ad :	Common Address	qr :	Power of Attorney
te :	Common Telephone No.	pr :	Proprietor
cr :	Criminal Involvement	qp :	Prostitution Involvement
do :	Documentation	re :	Public Officer
dr :	Drug Involvement	sl :	Solicitor
em :	Employee	so :	Some Link (non specific)
ep :	Employer	te :	Telephone Contact
fn :	Personel Friend	tr :	Travel Companion
ga :	Gambling Involvement	tt :	Travel To
ll :	Landlord	tf :	Travel From
		vi :	Violence Involvement
		wi :	Witness

Source Types

ad :	Address Book
ba :	Bank Records/Statements
do :	Document Source
if :	Informant Source
ob :	Observation Sheet
ps :	Passport Information
px :	Passenger Card Information
po :	Other Police Records
pu :	Other Public Records
rs :	Running Sheet (NCA)
te :	Teledex

CRIMINOLOGY RESEARCH COUNCIL

FINAL REPORT

GRANT NO. 22

Dr. John J. Galloway
Netmap International Pty Ltd
Sydney

APPLICATION OF THE NETMAP SYSTEM
TO INTELLIGENCE USE

Approved: 10th October, 1987
          & 4th August, 1988

Amount: $23,556

28th September

The aim of this project was to test the applicability and examine the relevance of the Netmap System to intelligence use, specifically to certain uses that the National Crime Authority sought to explore. (The system was originally designed for, and has been extensively applied to, ▬ purposes of diagnosing the linkages of how an organisation works in order to strengthen its operations. An assumption behind this project was that the same underlying principles might be re-directed toward the purposes of weakening an organisation's operations).

The original uses desired by the Authority - to do with the Netmapping of telephone interception data - could not be examined in this project. The reason related to innumerable delays in proclamation of the relevant legislation. This necessitated the project being refocused toward another type of application - because of the availability of data - and to be extended from three months to four months duration. The extra time led to a cost over-run of $1096 beyond the original budget. An additional grant covering this amount was gratefully made available by the Council bringing the total costs of the project to $23,556.

The original aims of the project I believe have been achieved, viz. testing the applicability and examining the relevance of the Netmap System to intelligence use. It is a pity that the original specific application could not be examined because telephone intercept data would seem to be almost "tailor made". Nonetheless, the various "other information" types of data, derived largely from historical documents and therefore not so "urgent", did provide a reasonable fit with the project objectives allowing use of the Netmap System to be explored.

The above comments indicate that the project was quite data dependent. Other different sorts of "intelligence" data - whether retrieved on-line from other computer systems or available as keyed-in data - were obviously not included within the bounds of this trial, e.g. visual and interactive analysis of telephone toll data, money and asset flows, suspected fraudulent relationships, criminal case accumulated relationships and sequencing, and various "live" investigations.

The National Crime Authority established an internal team to evaluate the project. They have kindly made available multiple copies of their report which are attached. I concur with the contents of the report. I believe that it provides a sound and comprehensive evaluation of the project.

Finally, I would like to thank the two main organisations which have made this project possible. The National Crime Authority at all times has been supportive and helpful. Especially, I would like to mention the Evaluation Team comprising Mr. B. Pannell, Director of Intelligence, Mr. H. Clarke, Senior Intelligence Analyst and Mr. T. Brophy, Intelligence Analyst. I also wish to express my gratitude to the staff of the Criminology Research Council for the interest that they showed and their assistance, and to the Council members for generously making the grant available.

John J. Galloway (PhD)

28th September, 1988