Operating Principles for Network Analyses

West Midlands Police
Data Analytics Lab

Operating principles for the use of the output of various network analyses provided by the Data Analytics Lab

Version 0.4.1

08/06/2021

Contents

1. Purpose

The purpose of these operating principles is to provide clear guidance on the use of any output from various network analyses and dashboards provided by the Data Analytics Lab (DAL) West Midlands Police (WMP).

1.1 Intended remit

The DAL sits within the Intelligence Department and was tasked to provide a series of network analyses to enhance the department's understanding of criminal networks involved in Serious Organised Crime (SOC); Child Sexual Exploitation (CSE) and County Lines (CL).

These principles are intended to provide an overarching framework for the use of all these network analyses and any similar future network analyses.

1.2 Data sources

The network analyses developed by the DAL use data taken from the WMP data system CONNECT (from April 2021) and corresponding legacy systems which include:

- crime records
- custody records
- intelligence records (only those graded as 'reliable' are included– see Appendix 2)

In addition, the analyses use data from:

- Prison Intelligence Notification System (PINS)[1]
- COMPACT (missing persons records)

Please see the relevant technical reports for details about how these data sets are used.

Of note, the Management of Police Information (MOPI) Code of Practice (2005)[2] in relation to the review, retention and disposal of policing information and records is applied to all these data sets. Records assigned as Group 1 (certain public protection matters) are retained until the subject's 100th birthday; Group 2 records (other sexual, violent or serious offences) are reviewed every 10 years and Group 3 records (all other offences) are deleted after a six-year clear period. As the network analyses will be refreshed on a regular basis, those subjects whose names do not reappear will be deleted through routine MOPI processes.

1.3 Oversight of data analytics projects

All the network analyses covered by these principles have had a Data Protection Impact Assessment (DPIA) approved by Information Management and have been approved by Legal Services.

Each project is accompanied by a technical report describing the methodology and an evaluation of the accuracy of the output. As part of this process the output has been tested and verified by colleagues within the Intelligence Department using 'traditional' methods.

[1] Prisoner Intelligence Notification System (PINS) is software used by almost every police service in the UK. It collects prison and police data from a variety of key sources and automatically cross-references and links historic and current prisoner records on a daily basis. It notifies law enforcement agencies of forthcoming prison releases to assist offender managers as offenders re-enter the community.

[2] College of Policing Authorised Professional Practice – Information Management https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/

In addition, each project has been considered by the independent Data Ethics Committee using the ALGO-CARE[3] framework to assess any ethical issues that might arise and their advice has been actioned. All the papers and minutes are publicly available.[4]

2. Network Analyses Output

The output of the various network analyses is a series of linked dashboards[5] which visualise nominals who appear in WMP data sets and who can be shown to be linked to others in a network involved in criminality, whether that is serious organised crime, child sexual exploitation or county lines. Some nominals may appear in networks connected to more than one type of criminality. Nominals may be offenders or victims, or both within a network.

The dashboards provide a visual representation of:

- the associations between nominals and the strength of these associations
- the changes over time to understand which individuals are gaining influence within a network; or which networks are collectively causing increasing harm[6]
- which nominals within a network are key to its operation and therefore of greatest interest in terms of dismantling the network
- the geographical locations which are of relevance to these networks

It is anticipated that the visualisations in the dashboards will evolve over time based on feedback from end users.

2.1 Access

The raw output of the network analyses is held within the DDI cloud environment which can be accessed by the DAL team.

Access to the dashboards is limited to officers and police staff in the Intelligence Department and senior officers responsible for tackling the threat. The Intelligence Academy will facilitate the development of knowledge within the department of the methodologies used and of their limitations.

Access to the dashboards for anyone outside of this group will need to be authorised by the Director of Intelligence.

2.2 Dissemination

The criminal network dashboards are an intelligence tool for use by intelligence professionals to support the force's decision making processes. Decisions to target an intervention at a group or an individual will not be made as a direct consequence of the output of the dashboards. These are tools designed to enhance the core business of intelligence professionals.

Whilst the techniques used to produce the network analyses are relatively new to policing; the data underpinning the model is standard law enforcement data routinely used by intelligence

[3] The ALGO-CARE framework assesses projects from a number of perspectives: Advisory; Lawful; Granularity; Ownership; Challenge; Accuracy; Responsible; Explainable.

[4] Office of the Police and Crime Commissioner for the West Midlands host the Data Ethics Committee. All papers and minutes published here https://www.westmidlands-pcc.gov.uk/ethics-committee/

[5] The dashboards are in Business Insights, designed and built by WMP using Qlik software.

[6] Both the Cambridge Crime Harm Index [Sherman, L.W. How to Count Crime: the Cambridge Harm Index Consensus. *Cambridge Journal of Evidence Based Policing* (2020). https://doi.org/10.1007/s41887-020-00043-2] and the Office for National Statistics (ONS) Severity Scores [https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeseverityscoreexperimentalstatistics] are used within the analyses.

professionals. Therefore, the dissemination of any intelligence products developed from the dashboards will be subject to routine processing and handling procedures according to the College of Policing (CoP) Authorised Professional Practice (APP).[7]

All members of the Intelligence Department complete appropriate training to understand their legal obligations in relation to the handling of data, intelligence and police information.

Both the training package and landing page of the dashboard will remind users;

- that the analyses are designed to augment rather than replace the user's decision making in the identification of cases and allocation of resources;
- that they should consider the potential for error when making their decision and ensure this is fed back to the DAL so that any errors and their causes can be investigated and rectified. Where information has been passed to other colleagues or partner agencies, they should be alerted as soon as possible;
- that they should confirm the reliability of any intelligence from the source system before taking action - a reference to the original source is included on the dashboard. Only intelligence acquired from a 'reliable' source is included in the analyses (see Appendix 2). Therefore, the resulting intelligence products can make recommendations with a reasonable degree of certainty. Intelligence assessments use the nationally agreed terminology of the 'Probability Yardstick' to ensure probability is conveyed in a consistent language.[8] (See Appendix 3).
- of the need to monitor the use of the tool for bias and ensure any concerns that this may be the case are fed back to the DAL so that the cause can be investigated and rectified;
- of the need to retain material relating to an investigation, including the technical paper describing the analyses, in order to fulfil their obligations under the Criminal Procedure and Investigations Act (CPIA) 1996. The ability to audit and review an output from the dashboard at a point in time is currently in development. This will assist with CPIA disclosure requirements;
- of the need to consider handling codes and relevant legislation before sharing information;
- relevant dashboards should be referenced within intelligence products in order to maintain transparency about the use of data science techniques

These principles will be developed as feedback is received from end user testing and as we develop the training package with the Intelligence Academy. Example guidance can be found in *Appendix 1*.

[7] College of Policing Authorised Professional Practice: https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/#handling-codes-and-conditions

[8] College of Policing Authorised Professional Practice - Intelligence Managemetn. https://www.app.college.police.uk/app-content/intelligence-management/analysis/delivering-effective-analysis/#communicating-probability

2.3 Tasking processes

Intelligence products feed into existing tasking processes and as such any interventions will be as a result of human decision making processes supported by information from the dashboards which has been assessed by intelligence professionals:

Examples of how the output will be used	
Operational	The networks will be updated on a weekly basis to take account of new crimes, intelligence reports, arrests, prison releases or missing person episodes and to determine where any new links are made. The SOCEx intelligence team will use the updated output to assess where there are new opportunities to develop our knowledge of criminal networks and use this to develop intelligence products for further dissemination to relevant teams as prioritised by the SOCEx tasking meetings.
Tactical	The output will be used by the SOCEx and Tactical intelligence teams to identify which networks or nominals are becoming more active over time and any changes in the levels of harm they are causing to individuals or communities. Intelligence products using the dashboards will support Force Tasking meetings where resource allocation decisions are made.
Strategic	A strategic understanding of the criminal networks operating with the West Midlands, their extent and levels of harm they cause enables WMP to focus resources in the longer term and to make informed decisions with regional and national partners such as the ROCU, NCA, Local Authorities and the Home Office.

Through these tasking processes, the resulting decisions will be disseminated as required to internal departments such as local policing and investigations.

In addition, these decisions (note: not the dashboards) will be shared as appropriate with partner agencies outside of WMP, with whom lawful sharing is permitted and required. These include Regional Organised Crime Unit (ROCU), National Crime Agency (NCA), Home Office, Central Motorway Policing Group (CMPG), Local Authorities, Violence Reduction Unit (VRU), Children's Trust, Youth Offending Teams (YOTs) and housing teams. These partners routinely receive intelligence products from WMP to enable partnership work across the 4P approach to tackling organised crime (prepare, prevent, pursue and protect).

There may be occasions where partners such as ROCU or CMPG will submit a list of nominals of interest to be compared to the WMP criminal networks. They will receive confirmation of whether the nominal exists in the WMP networks and their harm score. This information will feed into their own intelligence processes.

Appendix 1: Example of dashboard guidance

Below is an example of the guidance and reminder of the caveats to be considered by users of the dashboard. This is taken from the NDAS Modern Slavery dashboard prototype in March 2021:

1.1 When operating the tool, users are reminded that it is designed to augment rather than replace the user's decision making in the identification of cases and allocation of resources. The potential for error should be considered at all times.

1.2 Users are reminded of the need to monitor the use of the tool for bias. Particular caution should be taken to avoid taking action on links identified solely by protected characteristics of nominals.

*****

2.1 Products produced by this analysis will contain 'Sensitive Material' as defined in the Criminal Procedure and Investigations Act 1996 for the disclosure of unused material to the defence and is therefore subject to the concept of Public Interest Immunity. No products produced by this analysis should be disclosed to the defence without prior consultation with Force Intelligence. It will be recorded as 'Sensitive Unused Material' on disclosure form MG6d.

The information contained in this report is supplied in confidence and should only be shared in circumstances where there is a legal basis for doing so, e.g. GDPR, s.115 Crime and Disorder Act 1998.

2.2 All users are reminded to consider the reliability and current relevance of any intelligence prior to taking action.

2.3 The dashboard refers to intelligence with both Handling code: P (lawful sharing permitted) and C (conditions applied). Users are reminded of the need to check any handling conditions before dissemination.

2.4 Users are reminded of their obligations under the CPIA 1996 (s.23(1)) Codes of Practice to retain any material that is relevant to a criminal investigation.

Appendix 2: Management of Intelligence

Intelligence reports are graded according to the national '3x5x2' process undertaken by trained Intelligence Officers:

- The person submitting the intelligence assesses the reliability of the source of the information as 'reliable', 'untested' or 'not reliable'. Reliable information could be CCTV images; untested could be an anonymous report via Crimestoppers.
- The intelligence is also assessed based on how it came to be known; or can be corroborated by other sources; whether it is 'known directly to the source', 'known indirectly to the source but corroborated', 'known indirectly to the source', 'not known' or 'suspected to be false'.
- The third element deals with who should have access to the intelligence and how it should be handled or 'exploited'.

The 3x5x2 system replaced the 5x5x5 grading system in 2017. The table below shows the grades from the two systems which are perceived to be 'credible' and therefore used in the network analyses:

	Old		New	
Included	**Source**	**Information**	**Source**	**Information**
Yes	A - Always reliable	1 - Known to be true without reservation	1 - Reliable	A - Known directly
Yes	B - Mostly reliable	2 - Known personally to the source but not to the officer	1 - Reliable	C - Known indirectly
Yes	C - Sometimes reliable	3 - Not known personally to source but corroborated	1 - Reliable	B - Known indirectly but corroborated
No	D - Unreliable	4 - Cannot be judged	3 - Not reliable	D - Not known
No	E - Untested	5 - Suspected to be false	2 - Untested	E - Suspected to be false

IMS new and old intelligence grading system

The table below shows the current 3x5x2 intelligence grading system, including the handling codes. More information can be found on the College of Policing Authorised Professional Practice for the Management of Intelligence[9], from which the table is adapted:

Acquisition and Exploitation of Intelligence *Gradings shown in grey are **not** used in these analyses*		
ACQUISITION		**EXPLOITATION**
Source	**Intelligence**	**Handling**
1 – Reliable	**A** – Known directly	**P** – Lawful sharing permitted
	B – Known indirectly but corroborated	
2 – Untested	**C** – Known indirectly	
		C – Lawful sharing permitted with conditions
3 – Not reliable	**D** – Not known	
	E – Suspected to be false	

[9] https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/#lawful-sharing-permitted-with-conditions-c

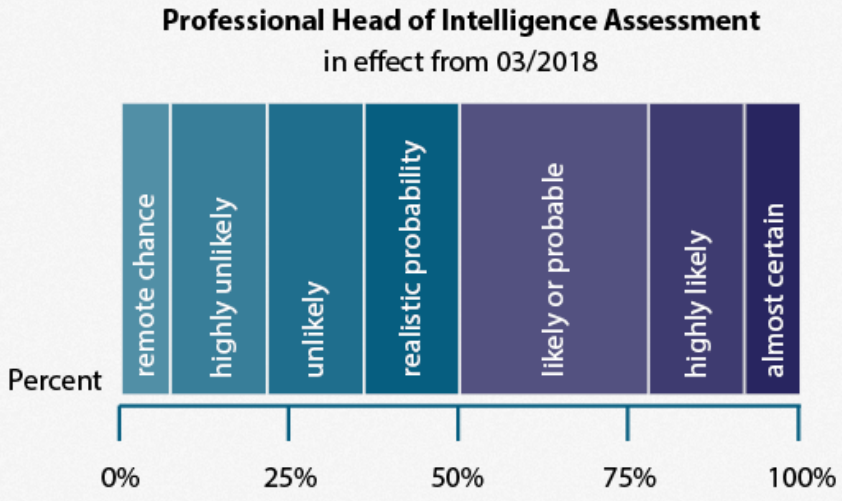
Appendix 3: The Probability Yardstick

The Probability Yardstick is the agreed standard for conveying probability in intelligence analysis in the UK. It was developed by Defence Intelligence and latterly adopted by the Professional Head of Intelligence Analysis (PHIA) got use across the government intelligence community. The scale comprises accepted intelligence terminology at a national level.

PHIA Probability Yardstick

Probability range	Judgement terms	Fraction range
≤ ≈5%	Remote chance	≤ ≈ 1/20
≈10% - ≈20%	Highly unlikely	≈1/10 - ≈1/5
≈25% - ≈35%	Unlikely	≈1/4 - ≈1/3
≈40% - <50%	Realistic possibility	≈4/10 - <1/2
≈55% - ≈75%	Likely or Probably	≈4/7 - ≈3/4
≈80% - ≈90%	Highly likely	≈4/5 - ≈9/10
≥ ≈95%	Almost certain	≥ ≈19/20
= approximately equal to	≥ is greater than or equal to	≤ is less than or

PHIA probability yardstick diagram



See CoP APP Intelligence Management for more information

https://www.app.college.police.uk/app-content/intelligence-management/analysis/delivering-effective-analysis/#communicating-probability