The Challenge of Combating Online Organised Crime – A Multi-Disciplinary Perspective

Organised criminal gangs are increasingly exploiting the Internet to steal money and information. **Anna Cevidalli** and **John Austen** explain how the forces of law need to organise themselves to make the most of their resources and skills.

Royal Holloway University of London

SearchSecurity.co.UK

THE RISE OF THE ONLINE ORGANISED CRIME GROUPS (OOCGS)

'There are 'new crimes, new tools' committed against computers and IT networks ... and there are 'old crimes, new tools' ... traditional crimes, supported by the use of the Internet and high technology ...'

Len Hynds, UK National Hi-Tech Crime Unit (February 2006)[1]

IN THE LAST FEW YEARS, Information Security reports such as the 2008 'Symantec Report on the Underground Economy XII'[2] and public statements from governments and law enforcers, such as the joint report sponsored by the US Dept of Homeland Security Science and Technology Directorate and the Anti-Phishing Working Group[3] in 2006, have highlighted the increase in organised criminal activity on the Internet.

The problem is estimated to affect businesses of all kinds, to the extent that the Verizon '2009 Data Breach Report'[4] stated that 91% of 'all compromised records' from a sample of 90 confirmed breaches 'were linked to organised crime groups'.

Such reports find that these technically-sophisticated professional groups are an industry of dedicated organised criminals who 'treat their malicious activities as a full-time job rather than a hobby'[5] and who pose a new type of threat to information on the Internet because they are financially-motivated, operate on an international scale, use a variety of tactics such as easy-to-use, powerful crimeware kits, exploit human frailties through social engineering and who mimic the strategies of successful legitimate corporate businesses.

Examples of innovative tactics which organised crime and other offenders have borrowed from the legitimate commercial sector include:

- Establishing 'rogue Internet Service Providers' to co-ordinate the distribution of illegal content such as malware and hard-core pornography
- Creating 'misleading applications', in particular the 'scareware' security applications, which may do the opposite of the stated purpose
- Creating 'instructional videos' as part of a criminal product package
- Applying 'Copyright Notices' to their malware (eg to Trojans)
- Including 'Terms and Conditions' statements with their products which include reporting non-compliance to legitimate anti-virus companies.[7]

As well as exploiting the new 'tools' of technology, organised crime groups also employ

tried and tested traditional organised crime methods such as money-laundering, fraud and extortion which have found new forms of expression within the online environment.

This evolution from informal to more strategic and aggressive large-scale tactics among online offenders led Keith Laslop of Prolexic Technologies (whose network protection company was targeted by the Distributed Denial of Service campaign that brought down The Blue Security Team in 2006) to remark: 'We used to call the Internet a sort of Wild West. Now it's more like Chicago in the 1920s with Al Capone.'[8]

THE RESPONSE FROM GOVERNMENTS AND LAW ENFORCEMENT

'It's about time law enforcement got as organised as organised crime.'

Rudy Giuliani (October 1984)[1]

Modern organised crime has been identified as one of the five key security threats to EU states,[2] with the 2009 'State of the Future'[3] report highlighting the 'enormity' of the threat of transnational organised crime by stating that: 'Its global income is estimated to be about $3 trillion, which is twice all the military budgets of the world combined.'

In response to these new threats, governments, law enforcement, Information Security (IS) and business professionals who are tasked with protecting valuable information assets in capitalist societies are recognising that they can no longer work in silos and must collaborate to manage the problem. They are making concerted efforts to work more closely at international level, for instance by introducing or updating relevant legislation or by producing national cybersecurity and organised crime strategies such as those published by the US and UK in 2009.[4]

Whereas in the past, intelligence and detection strategies focused on identifying individuals (for instance, organised crime leaders) and crime groups, official organisations are devising new, broader-ranging techniques, including reaching out to the private sector as never before. This approach acknowledges the value of multi-disciplinary collaboration, including the benefits of exchanging information and efficiency savings from sharing limited resources. Just as organised crime groups use blended attack strategies for maximum impact, so it is necessary for counter-measure strategies to also incorporate a range of defensive and detective methods, including

both technical and non-technical countermeasures, ideally identified by a multi-disciplinary team of professionals.

Is there an untapped potential for IS and business professionals to contribute to the multi-disciplinary approach to combating organised crime by applying strategic management methods and their professional knowledge and expertise?

This new approach was demonstrated by the UK Serious Organised Crime Agency (SOCA) in October 2009 at the RSA Conference in London,[5] which announced that, as well as employing 'follow the money' strategies by tracking the electronic exchanges of funds between different criminal groups, they would be seeking to identify weaknesses in criminal business models and attempting to locate their covert data stores.

Such declarations raise intriguing questions for information security (IS) and business professionals. If, as has been stated, there is a close correlation between online organised crime and business, what types of insight can business professionals bring to the table? Is there an untapped potential for IS and business professionals to contribute to the multi-disciplinary approach to combating organised crime by applying strategic management methods and their professional knowledge and expertise? If so, how can they apply such techniques to their own business and where can they find appropriate resources to assist them with this task?

THE DIFFERENT FLAVOURS OF 'ORGANISED CRIME'

'Organised crime is both more and less than the average person understands it to be. It is more pervasive, more dangerous and more diverse ...'

J O Finckenauer, 'The Mafia and Organized Crime' (2007)[1]

As Kaspersky[2] has pointed out, organised crime must be understood before it is addressed. This task is not as straightforward as it might seem. Although some sources, including official reports and statements, have a tendency to use the

MATRIX TABLE A (EXAMPLE)

MORPHOLOGICAL ANALYSIS OF A THEORETICAL ONLINE ORGANISED CRIME GROUP

STEP 2 – CREATE A MORPHOLOGICAL MATRIX

Elements of Problem						
Criminal Organisational Structures	Collaboration	Fluid, changeable roles, membership and structure	Hierarchical Structure	Network Structure	Commercial/ Business-Like Structure	Specialised Division of Labour
Criminal Organisational Business Model	Subscription Business Model	Collective Business Model	Online Auction Business Model	'Other' Business Model Type		
Criminal Organisation Attack Vectors	Phishing	Distributed Denial of Service (eg botnets)	'Drive By Downloads'	Insider Corruption	Fraud	Spyware
Potential Targets (Sites)	Site Type A – Headquarters	Site Type B – Vancouver Office	Site Type C – Nairobi Office	Site Type D – London Office	Site Type E – Melbourne Office	Site Type E - Home-working sites
Potential Targets (Data)	Personal Data (all types)	Research and Development Data	Intellectual Property	Financial Data	IT-Related Data (eg Network Infrastructure Maps)	Physical Site Maps and Blueprints
Potential Targets (Stakeholders)	Staff (Management)	Staff (Operational)	Third Parties	Existing/ Potential Customers	Shareholders	Other Stakeholders
Potential Targets (Physical/ IT)	Network Infrastructure	Physical Storage Systems (eg Paper files)	Databases	Websites	External Storage Devices (eg PDAs, USB drives)	Physical Assets (eg Keys, Safes, Staff Passes)

MATRIX TABLE B (EXAMPLE)

MORPHOLOGICAL ANALYSIS OF A THEORETICAL ONLINE ORGANISED CRIME GROUP
ANALYSIS OF A THEORETICAL ONLINE ORGANISED CRIME GROUP
STEP 3 – DEVELOP POSSIBLE EXPLANATIONS OR OUTCOMES

Elements of Problem						
Criminal Organisational Structures	Collaboration	Fluid, changeable roles, membership and structure	Hierarchical Structure	Network Structure	Commercial/ Business-Like Structure	Specialised Division of Labour
Criminal Organisational Business Model	Subscription Business Model	Collective Business Model	Online Auction Business Model	'Other' Business Model Type		
Criminal Organisation Attack Vectors	Phishing	Distributed Denial of Service (eg botnets)	Ransomware	Insider Corruption	Fraud	Spyware
Potential Targets (Sites)	Site Type A – Headquarters	Site Type B – Vancouver Office	Site Type C – Nairobi Office	Site Type D – London Office	Site Type E – Melbourne Office	Site Type E - Home-working sites
Potential Targets (Data)	Personal Data (all types)	Research and Development Data	Intellectual Property	Financial Data	IT-Related Data (eg Network Infrastructure Maps)	Physical Site Maps and Blueprints
Potential Targets (Stakeholders)	Staff (Management)	Staff (Operational)	Third Parties	Existing/ Potential Customers	Shareholders	Other Stakeholders
Potential Targets (Physical/ IT)	Network Infrastructure	Physical Storage Systems (eg Paper files)	Databases	Websites	External Storage Devices (eg PDAs, USB drives)	Physical Assets (eg Keys, Safes, Staff Passes)

generic term 'organised crime' in the abstract without defining any specific scope or context, it is, in reality, an emotive, confusing and controversial subject which means different things to different people. For instance, although they are often classed together, the structures of the Russian mafiya vary from those of the Italian Mafia groups which, in turn, are differentiated from their American counterparts.

Critics observe that 'organised crime' is a 'slippery',[3] imprecise notion which is very susceptible to subjective interpretation, with Klaus von Lampe citing over 100 different government and other sources that provide 'organised crime' definitions.[4]

DISPELLING THE MYTHS

IS and business professionals involved in media handling and awareness-raising need to take care when expressing statements about organised crime, in order to avoid sending mixed messages, reinforcing distorted crime group and ethnic stereotypes, infringing intellectual property rights (for instance, those of films or television) or creating an impression that they are trivialising, exaggerating or sensationalising their subject.

Even so, despite the potential pitfalls of citing dramatic examples, such items are useful for quickly getting a message across and recent evidence demonstrates that they can be effective if properly managed. 'Signal events' (that is, events perceived to be of particular significance and impact) such as the ShadowCrew arrests and the 'Conficker' outbreaks captured the public imagination and, in their '2009 e-Crime Survey',[1] KPMG reported that 42% of respondents had cited knowledge of high-profile incidents in other organisations as the main driver for increased security investment in the previous year.

THE CHALLENGE OF SYNTHESISING DIVERGENT VIEWS

The perspectives in the previous sections provide a flavour of the wide diversity of mindsets and approaches which can legitimately be applied to the complexity of organised crime. All of them have validity within their specific contexts. An appreciation of these different perceptions is an important cultural consideration for all organisations which have an investment in crime prevention and detection, both in terms of stakeholder engagement (for instance, with their own staff, their colleagues from other disciplines

or the public) and also to obtain a fuller appreciation of all the factors which may underpin organised criminal activity.

A pressing challenge facing law enforcement and the public/private sector is how to understand and synthesise the most significant findings from the various disciplines, in order to create a new, relevant and comprehensive holistic frame of reference for organised crime.

DEFINING THE REALITIES

Whilst recognising that distinctions between terrestrial and technology-oriented organised crime may disappear in the future (given the prevalence of technology), we can define the current, transitional state of 'organised crime' within[4] broad categories:[1]

Organised Crime – A generic term that may apply to all types of organised crime activity, whether terrestrial or technology-oriented

Online Organised Crime – Potential or actual criminal activity that primarily targets the Internet environment

Terrestrial Organised Crime – Potential or actual criminal activity that primarily targets the physical environment, as opposed to the technology-oriented environment

Technology-Oriented Organised Crime – Potential or actual criminal activity that primarily targets any aspect of the Information and Communications Technology (ICT) environment, including the Internet.

STRATEGIC ANALYSIS AND OOCGS

In circumstances which may involve online organised crime activity and which require further investigation, IS/ business professionals need access to simple-to-use, generic tools which can help them quickly identify the key elements of the situation, from which position they can undertake more in-depth risk analysis procedures as necessary. In particular, they require tried and tested tools which they can utilise immediately without 'reinventing the wheel'.

There are a number of business approaches and techniques which have been identified for use in law enforcement and which can easily be extended for use within multi-disciplinary environments. Most notably, Gottschalk[1], Ratcliffe[2] and Albanese[3] demonstrate how established strategic analysis techniques such as maturity models, trend analysis, risk analysis, morphological analysis (MA), process mapping and

SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis are relevant to the organised crime environment. All of these tools will already be familiar to business professionals and, although they may have been devised for terrestrial situations, can be applied equally to known factors within online legitimate and illegal business scenarios.

An important point, observed by Emigh and Ramzan,[4] is that, because OOCGs are mainly motivated by profit, successful countermeasures do not have to be watertight, merely sufficiently effective to make the attack unprofitable.

EMPLOYING MORPHOLOGICAL ANALYSIS (MA) WITHIN A MULTI-DISCIPLINARY CONTEXT

Originally designed for use within the field of astrophysics, Morphological Analysis (MA)[1] is a useful simple tool for helping multi-disciplinary anti-organised-crime teams to quickly identify the key issues in a situation and to effectively share and update their skills and experience. It divides the problem into different elements and displays them in the form of a matrix that visually represents the[4] steps of the analytical process.

The MA method is 'tried and tested' over several years and has been proven to work within a variety of different contexts, including scientific and corporate environments.

Within the field of criminal intelligence, it has been proposed as a tool to develop strategic thinking about organised crime.

One of the key benefits of MA is that its processes ensure that all input is managed and that both input and decisions are clearly trackable to their source. Another key aspect is that, because its purpose is to provide a holistic interpretation of a situation, MA requires multi-disciplinary input to be truly effective.

MA is intended to be used during the early stages of exploratory analysis. For instance, it can be used during the early identification (triage) stage of an Incident Management process when time is of the essence or in any situation where there are a wide range of possible scenarios which need to be reduced to those which are most feasible.

As well as its potential for use within any environment, external data can easily be incorporated and the results from the exercise can be used as a baseline or other foundation for subsequent work using other complementary methods, including commercial risk and impact assessment tools.

In brief, the 4 steps of the MA process are:

1. Break down the problem (identify the broad elements and categorise them)

The first step of the process is for the multi-disciplinary team to identify the problem to be addressed and to capture its potential elements, for instance by asking the question: "In what ways might an online organised crime activity pose a threat to our organisation's vulnerable assets?"

2. Create a morphological matrix

The output from Step 1 forms the basis of a matrix table (see Matrix Table A).

The categories within the matrix can be composed from any set of issues affecting the problem. Items within the categories are listed horizontally.

3. Develop possible explanations or outcomes

This stage identifies attributes in the situation which may not have been previously apparent and which may require further analysis. It explicitly requires that the participants exercise professional judgment, without any 'specialist' bias, in order to extract the most significant possibilities from within the matrix, with these items being further assessed against additional factors, such as feasibility.

One important by-product of this and the subsequent stage is that the team members will be informing and updating each other about significant aspects of the situation during their focussed discussions.

Once the matrix is complete, it is read downwards and across to create sets of associations (see Matrix Table B for the possible links between one set of the attributes). The features in adjacent rows do not need to relate to the group above. If the associations are not inherently consistent, contradictory or may not be relevant to the situation, then they are discarded.

For instance, the associations in Matrix Table B might suggest the following scenario:

> *A threat to personal data in corporate databases/ arising from spyware/ installed via senior management remote access accounts/ by a specialist sub-division of an online organised crime group/ who obtain their tools via a criminal online auction site.*

Substituting any single item (for instance, replacing 'Site Type E – Homeworking Sites' with 'Site Type A – Headquarters' or replacing 'Spyware' with 'Distributed Denial of Service' attacks) creates a new and different scenario.

By the end of this stage, a list of scenarios has been identified through brief and simple methods of systematic analysis and elimination which, between them, capture the key issues which, according to professional consensus, need to be prioritised.

4. Grade the explanations (eg from most feasible to least feasible).

The last step of the process assesses the findings from Step 3 against potentially-relevant criteria such as whether the scenarios are 'possible, practical and feasible' or whether there are known precedents for the scenarios within that particular industry. At this stage, the team also reintroduces pertinent issues arising from their specialist fields.

The scenario example might be assessed as follows:

Scenario	Possible? (Y/N)	Practical? (Y/N)	Feasible? (Y/N)
A threat to personal data in corporate databases/ arising from spyware/ installed via senior management remote access accounts/by a specialist sub-division of an online organised crime group/ who obtain their tools via a criminal online auction site	Yes	Yes	Yes

The scenarios with the highest number of 'Yeses' are retained for further analysis, with the other scenarios being discarded (although, in some instances, they may be useful in highlighting issues outside the scope of the exercise which can be addressed elsewhere).

At this point, additional methodologies can be introduced to further ascertain the likelihood of particular threats, for instance undertaking further risk and impact analysis using threat and vulnerability assessment manual or software tools, with the final objective being to provide recommendations for further action. ■

ABOUT THE AUTHORS

Anna Cevidalli became interested in information security in the late 1990s when she got involved in installing patches and anti-virus software. Following completion of her MSc with RHUL, she has started work as a security consultant in the field of information assurance, working for a company that works on Government contracts.

John Austen John Austen is the Course Director for the Royal Holloway Diploma in Information Security. He was head of the Computer Crime Unit, New Scotland Yard, until September 1996. He was a career detective for 30 years, investigating the first major UK computer crime in 1976 and founding the Computer Crime Unit in 1984 - the first of its type in the world.

REFERENCES

The Rise of the Online Organised Crime Groups (OOCGs)

1. Information-age.com: Online version of 'Interview: Len Hynds, National Hi-Tech Crime Unit' (February 2006):

http://www.information-age.com/articles/289406/interview-len-hynds-national-hitech-crime-unit.thtml

2. The 2008 'Symantec Report on the Underground Economy XII:

http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

3. Joint Report between the US Department of Homeland Security, SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, sponsored by the US Dept of Homeland Security Science and Technology Directorate: Page 5, 'The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond' (October 2006)

http://www.antiphishing.org/reports/APWG_CrimewareReportpdf

4. Verizon: Page 2, '2009 Data Breach Investigation Report'

http://www.verizonbusiness.com/products/security/risk/databreach/

5. Jakobsson and Z Ramzan: Page 1, 'Crimeware – Understanding New Attacks and Defences' (Addison Wesley) (2008)

6. Anna Cevidalli: Page 52, 'Leveraging the Multi-Disciplinary Approach to Countering Organised Crime – An Evaluation for Information Security and Business Professionals'

(MSc Thesis, Royal Holloway, University of London) (September 2009)

7. Examples of innovative tactics:

'Rogue ISPs' (the 'Pricewert' case)

CNet.com: 'Federal Trade Commission shuts down rogue ISP' (June 2009)

http://search.myway.com/search/GGmain.jhtml?PG=SEASUSH&SEC=ABMANY&psa=_UkGfRVGZZwhc1yUG6Lgzw&ptnrS=DK&st=kwd&searchfor=federal+commission+shuts+down+rogue+ISP

ComputerWeekly.com: 'Cybercrooks Develop own Search Engines to Burgle Users' (May 2009)

http://www.computerweekly.com/Articles/2009/05/07/235935/cybercrooks-develop-own-search-engines-to-burgle-users.htm

'Misleading Applications'

The following 'Symantec' report includes a list of 'Top 10' Misleading Applications (at December 2008):

Symantec White Paper: Pages 17-18, 'Web-based Attacks – February 2009'

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

'Instructional Videos'

ComputerWorlduk.com: 'Behind the Scenes of an Online Fraudster's Arrest' (April 2009)

http://www.computerworlduk.com/management/security/cybercrime/in-depth/index.cfm?articleid=2224

'Copyright Notices'

The Register.co.uk: 'VXers Slap Copyright Notices on Malware' (April 2008)

http://www.theregister.co.uk/2008/04/28/malware_copyright_notice/

'Terms and Conditions'

Fraudwar.Blogspot.com: 'Internet Gangstas Don't Appreciate Software Piracy, Either!' (May 2008)

http://fraudwar.blogspot.com/2008/05/internet-gangstas-dont-appreciate.html

8. Quoted in Wired: 'Attack of the Bots' (November 2006)

http://www.wired.com/wired/archive/14.11/botnet.html?pg=4&topic=botnet&topic_set=

The Response from Governments and Law Enforcement

1. Time.com – Page 8, 'The Sicilian Connection' (October 1984)

http://www.time.com/time/magazine/article/0,9171,923697-8,00.html

2. EU: 'A Secure Europe in a Better World – European Security Strategy' (December 2003):

http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

3. World Federation of UN Associations, The Millennium Project '2009 State of the Future' Executive Summary, Page 2:

http://www.millennium-project.org/millennium/issues.html

4. Key UK and US reports include:

UK Cabinet Office: 'Extending our Reach: A Comprehensive Approach to tackling Serious Organised Crime' (July 2009)

http://www.homeoffice.gov.uk/crime-victims/reducing-crime/organised-crime/

SOCA: 'The United Kingdom Threat Assessment of Organised Crime 2009/10'. See in particular 'Annex A – Harm Framework of Organised Crime':

http://www.soca.gov.uk/about-soca/library

UK Cabinet Office: 'Cyber Security Strategy 2009' (June 2009)

http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

UK Cabinet Office: 'Security in an Interdependent World' (June 2009) and 'Security for the Next Generation' (June 2009)

http://www.cabinetoffice.gov.uk/reports/national_security.aspx

US Government: 'Cyberspace Policy Review' (May 2009)

http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

5. ITPRO: 'RSA 2009: SOCA attacks heart of organised cyber crime':

http://www.itpro.co.uk/616603/rsa-2009-soca-attacks-heart-of-organised-cyber-crime

The Different Flavours of Organised Crime

1. J O Finckenauer: Page 1, Ch 1, 'The Mafia and Organized Crime' ('Beginner's Guide' Series, Oneworld Publications) (2007)
2. E Kaspersky, KasperskyUSA.com: 'The Cybercrime Ecosystem' White Paper (September 2008)

http://www.kasperskyusa.com/partners/pdf/The_Cybercrime_Ecosystem.pdf

3. G P Gilligan, Page 2, 'Business, Risk and Organised Crime' (Journal of Financial Crime, Volume 14, No 2) (2007)
4. K von Lampe: 'Definitions of Organised Crime' section, 'Organised Crime Research' website:

http://www.organized-crime.de/OCDEF1.htm

Dispelling the Myths

1. KPMG: Page 30, '2009 e-crime survey':

http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009_AKJ_KPMG(1).pdf

Defining the Realities

1. Alternatively, it could be argued that there is a single category, 'Organised Crime', from which all sub-categories (in this instance, Definitions 2, 3 and 4) will evolve.

2. 'United Nations Convention On Transnational Organised Crime' (2000)

http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

3. CERT®: Page 11, 'Spotlight on: Malicious Insiders with Ties to the Internet Underground Community' (March 2009):

http://www.cert.org/insider_threat/

4. Cyber-Ark: Page 2, '2009 Trust, Security and Passwords Survey Research Brief' (June 2009)

http://www.cyber-ark.com/landing-pages/downloads/snooping-survey-2009.asp

5. See V3.co.uk, online interview with Eugene Kaspersky: 'Credit Crunch forcing software engineers into crime' (December 2008)

http://www.v3.co.uk/vnunet/news/2232084/credit-crunch-force-software

Strategic Analysis and OOCGs

1. P Gottschalk: 'Criminal Entrepreneurship' (Nova Science Publishers, Inc, New York) (2008)

2. J H Ratcliffe (Ed): 'Strategic Thinking in Criminal Intelligence' (The Federation Press) (2004, 2007)

3. J S Albanese: 'Risk Assessment in Organised Crime: Developing a Market and Product-Based Model to Determine Threat Levels' (Pages 273 – 272, Journal of Contemporary Criminal Justice, Volume 24, Number 3) (August 2008)

http://jayalbanese.com/organized_crime

4. A Emigh and Z Ramzan: Page 28 ('Crimeware - Understanding New Attacks and Defences'

(M Jakobsson and Z Ramzan (Eds), Addison Wesley) (2008)

Employing Morphological Analysis (MA) Within A Multi-Disciplinary Context

1. The MA methodology approach described here originates from:

C E Heldon's chapter: 'Exploratory Analysis Tools', Pages 112-14, within J H Ratcliffe (Ed), 'Strategic Thinking in Criminal Intelligence' (The Federation Press) (2004, 2007)

The origins of the MA methodology are explained in T Ritchey's paper: 'General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling', adapted from: 'Fritz Zwicky, Morphologie and Policy Analysis, presented at the 16th EURO Conference on Operational Analysis, Brussels (2003-2009):

http:/www.swemorph.com/ma.html

MA includes the option to incorporate larger data sets which can be analysed semi-automatically to create inference models using the 'MA/Casper: Computer Aided Scenario and Problem Evaluation Routine' software program (See Page 9 in Ritchey's paper).