# Integrating Data Sources and Network Analysis Tools to Support the Fight Against Organized Crime

Luigi Ferrara[1], Christian Mårtenson[1], Pontus Svenson[1], Per Svensson[1,*],
Justo Hidalgo[2], Anastasio Molano[2], and Anders L. Madsen[3]

[1] Dept. of Decision Support Systems, Swedish Defence Research Agency,
SE 164 90 Stockholm, Sweden
[2] denodo technologies Europe c/ Alejandro Rodriguez, 32 Madrid 28039, Spain
[3] HUGIN Expert A/S, Gasværksvej 5, DK 9000 Aalborg, Denmark
{luigi.ferrara,christian.martenson,pontus.svenson,
per.svensson}@foi.se, {jhidalgo,amolano}@denodo.com,
anders@hugin.com

**Abstract.** We discuss how methods from social network analysis could be combined with methodologies from database mediator technology and information fusion in order to give police and other civil security decision-makers the ability to achieve predictive situation awareness. Techniques based on these ideas have been demonstrated in the EU PASR project HiTS/ISAC.

## 1 Introduction

The serious criminal threats facing society today require new methods for modelling and analysis. In fact, civil security decision makers, analysts and field operators fighting organized crime and terrorism across the European Union all need front-line integrated information collection and management technologies to support their cooperative work. Their adversaries are no longer organized in hierarchical structures, but instead consist of individuals and groups that are loosely organized in "dark networks" [1]. They stage attacks or set bombs against unprotected civilians, or seek to influence crowds of legitimate demonstrators so that critical riot situations occur.

In order to construct data analysis and other decision support systems that take account of these new factors, new and powerful methods and techniques from several technological domains need to be brought together and integrated.

### 1.1 Cross-Border and Cross-Agency Interoperability

To achieve the necessary cross-border and cross-agency interoperability, models and methods for secure sharing of information will have to be based on integrity and ownership across the information-sharing network, including dynamically modifiable role-based access rights, technology for dealing with heterogeneous data schemas and protocols, a service-oriented system architecture based on data services for sharing information, and new analysis tools to support operations during stationary as well as mobile activities.

[*] To whom correspondence should be addressed.

C.C. Yang et al. (Eds.): ISI 2008 Workshops, LNCS 5075, pp. 171–182, 2008.

### 1.2 Intelligence Analysis Based on Information Fusion

Fundamentally uncertain intelligence information has to be interpreted, integrated, analysed, and evaluated to provide situational awareness based on information fusion, in particular situational assessment and threat assessment methods. Relevant intelligence information originates from many sources, some of which are well-established infrastructure sources, others may be secret human intelligence information sources, some are open or public sources like mass media or the Internet [2], yet others are sensors and other physical devices of many kinds [3]. Potentially relevant data from such sources need to be stored in databases for later proactive reanalysis.

### 1.3 The EU PASR Project HiTS/ISAC

In the recently completed HiTS/ISAC project (EC SEC5-PR-113700) [32], financed by the EU Preparatory Action for Security Research (PASR) programme[1], environments and tools have been created for collaboratively solving a large class of social network interaction problems in law enforcement intelligence analysis.

The HiTS/ISAC problem-solving environment for interoperability and situation awareness has been demonstrated and assessed using realistic scenarios set up in cooperation with law enforcement authorities from several EU member states. The project was concluded by demonstrating a complete problem-solving environment to the project’s end-user representatives using a fictitious organized-crime scenario. In that application the project showed how authorities may interoperate with information security over the network and illustrated how law enforcement authorities may cooperatively develop and share mission-critical information across national borders.

This paper deals with intelligence analysis aspects of the HiTS/ISAC demonstration system.

### 1.4 Structure of the Paper

A data analysis environment and toolset capable of dealing with social network analysis (Ch.2; [4]) and visualization tasks involving partly uncertain data was created by the project. Requirements on such environments are discussed in Ch. 3. The analysis system was built by combining several open-source network algorithm and visualization software packages [4][5] with a COTS (commercial-off-the-shelf) system for Bayesian belief network (BBN) modelling, embodying modern concepts and methods for management of uncertain information (Ch. 4.3; [6][7]). In addition, the use of COTS software implementing emerging database mediator technology (Ch. 4.1; [8]) made it possible to connect in a non-intrusive way, organizationally and geographically distributed and heterogeneous data sources into a single, homogeneous and secure virtual system. An architectural overview of this system is given in Ch. 4.2, below. Ch. 5 concludes the paper.

[1] Now superseded by the 7th Framework Programme for European Research 2007-13, which for the first time includes a Security section.

## 2 Methods for Coping with the Threats to European Security

It can be argued whether the notion of “organized crime” is appropriate for today’s loosely connected networks of criminals. The new threats to European security typically come from terrorism and other large-scale criminal activities, carried out by individuals and groups that are loosely organized in “dark networks” [1]. Such networks are advantageous from a criminal’s point of view since they reduce the risk of detection during planning and preparation phases. A further difficulty for law enforcement agencies is that not all actors are known in advance – the network may involve individuals without criminal records or known connections to extremist organizations.

The papers [1][9] provide examples of social network analysis in anti-terrorism applications and indicate both usefulness and some limitations of social network analysis as a basis for quantitative methods for situation awareness and decision-making in law enforcement applications. The paper [1] discusses the organizational structure of certain drug trafficking, terrorism, and arms-trafficking networks, showing how some of them have adapted to increased pressure from states and international organizations by decentralizing into smaller units linked only by function, information, and immediate need. Another interesting application of social network analysis to terrorist networks is given by [10]. In that paper, the author discusses methods for estimating the vulnerabilities of terrorist networks.

In serious-crime analysis applications, networks of relations between people, in some cases very large ones, will thus have to be set up: who knows whom, who has family relations with whom, as well as who met whom where and when, or who phoned whom when, and so on. Figuring out nested business connections across the known set of individuals or organizations is a closely related issue.

### 2.1 Social Network Analysis

Social network analysis (SNA) [11], is a family of methods that support statistical investigation of the patterns of communication within groups. Social scientists use these networks to analyse, *e.g.*, families, organizations, corporations, or Internet communities. The basis of the methodology is the assumption that the way that members of a group communicate with members of another group reveals important information about interesting properties of the group.

#### 2.1.1 Structural Analysis

The emphasis in social network studies is on relations between individuals and/or groups of actors. It is sometimes referred to as *structural analysis*. In order to study the structural properties of a group, it is necessary to model it mathematically. This is most naturally done by constructing a *graph* or *network* representing the relationships within the group. Each member of the group is mapped to a node in the graph, and edges between nodes are introduced if the corresponding members communicate. Most edges link exactly two nodes; graphs where multi-edge relations are allowed are called *hypergraphs*. A hypergraph can always be embedded in an ordinary graph by introducing an extra node for each relation that involves more than two nodes.

For example, several studies, such as [12], of the citation and collaboration networks of scientists have been carried out. In these, the network of interest is the one where there is a link between all individuals who have co-authored a paper. In order to avoid having to handle hypergraphs, additional nodes are introduced for each paper, and binary relations between papers and their authors are introduced. If we are studying collaboration networks, this leads to a *bipartite* graph, where there are two different kinds of nodes, and no edge links two nodes of the same type.

An analogous example from the law enforcement domain of interest here might be that we need to model individuals who have met. In a bipartite graph of people and meetings, we can represent information about which particular meeting two specific persons attended.

### 2.1.2 Weights and Measures

In addition to including several nodes, edges can also be extended to include a weight or probability. This is used to model, for example, the maximum amount of information that can flow between two nodes, or to indicate the certainty with which we know that the edge is actually present in the network.

There are several important measures that can be used to characterize a network. Perhaps the simplest is to count the number of edges that different nodes have. This can be seen as a measure of the popularity of a node, and is one of the methods that are used by web search sites such as Google to rank search results [13]. Relying on the number of edges alone is not always sufficient, however. Better measures are obtained by looking at the amount of information that flows through a node. Such measures are called centrality measures. The two most important centrality measures are the *betweenness centrality* and *max-flow centrality*. The high computational complexity of the max-flow centrality problem [11][14] makes it necessary to also consider approximations to it.

Sociologists are often interested in actors that control the interaction between different groups. Such nodes are called “liaisons”, “bridges”, or “gatekeepers”, and they can also be found by calculating the centrality measures.

### 2.1.3 Statistical Analysis of Very Large Networks

Recently, many physicists and computer scientists have become interested in network analysis. This has led to an increased emphasis on studying the statistical properties of very large networks, such as the internet, biological food webs, and even infrastructure networks (see [15] for an overview). This influx of people to the field has also led to several new approximate algorithms with which important properties may be computed [14][16][17].

### 2.1.4 The Need for Management of Uncertainty

Intelligence representation languages and systems need the ability to express and reason with incomplete and uncertain information. Representation, management, and categorization of uncertainty in order to enable a machine to reason about potential relations are complex tasks. These are scientifically studied in the field of information fusion [27] which provides methods for reasoning about information arising from several different uncertain sources (see, *e.g.*, [20]).

*Bayesian belief networks* (BBN) [6] is one such uncertainty modelling and information fusion methodology used to represent and exploit uncertain causal relations between several variables. The BBN methodology has several potential areas of application within the intelligence domain, for instance for detecting threatening behaviours by insiders [21], for probabilistic assessment of terrorist threats [7], and for anti-terrorism risk management.

## 3 Requirements on Law Enforcement Problem-Solving Environments

The HiTS/ISAC project strives to contribute to a deeper awareness and understanding of modern methodological opportunities among European law enforcement authorities. These include on-demand, real-time problem solving based on scientifically sound methods of often large-scale data analysis. Organizationally, one needs to move away from "closed-room" approaches into collaborative working styles. Not only is trans-national collaboration needed between authorities in different security-related areas, such as police, coast guard, and customs services, but in order to enable effective use of modern analytical techniques and problem-solving methods there is a clear need also for cross-professional collaboration and involvement of mathematically trained analysts. A paper discussing the need for such changes in organizational culture, written from the perspective of a senior analyst is [18]. Another interesting study in the law enforcement investigative analysis area is [19].

Confidentiality, integrity and availability of information and communication systems need to be well protected [3]. Data from many different sources as well as aggregated or otherwise partially processed information, which could be sensitive and classified, must be protected from unauthorized access and modification. Although preventive countermeasures are most important, detection of misuse and intrusion must be available to deal with various types of attacks such as insider attacks and identity theft.

### 3.1 The HiTS/ISAC Interoperability Platform

Although database interoperability is only one of several interoperability issues that need to be addressed in a civil security intelligence system for routine operations, it is one of high technical complexity and critical importance.

A modern approach for integration of heterogeneous data sources is to make use of mediators between data sources and those consumer applications and software tools which tap these sources [22]. Mediator systems enable automatic translation between the concepts and conventions, *schemas*, of different distributed data sources, *i.e.*, names and other characteristics of their data items as well as the semantic relationships between them, offering a virtual data layer that can be queried by consumer applications using database-like query languages (*e.g.* SQL and/or XQuery).

The HiTS/ISAC project provides prototypical mechanisms for information sharing with retained integrity and confidentiality to support role-based cooperation.

Depending on the situation the users will have easy but secure access to information and services tailored to their respective needs.

In the HiTS/ISAC demonstration system no single unifying software technology is used. Instead, different technologies are contributed by different partners, making the challenge of maintaining interoperability greater than in a homogeneous single-vendor system, but at the same time providing greater benefits due to the pooled capabilities. COTS software (Denodo Virtual Data Port and HUGIN), sometimes modified open-source software (JUNG, Prefuse, PROXIMITY, Monet), and in-house middleware developments are all part of the final system.

The backbone communication network in the HiTS/ISAC demonstration system is based on services that are available today as standard products from the project partner TeliaSonera. The system satisfies the security levels required by the Swedish police, while meeting their demands for identification, tapping and integration protection, confidentiality and security. High-capacity, secure Internet solutions based on virtual private networks (VPN) and encryption techniques, as well as telephony services fixed or mobile, are examples of products on which the solution has been based.

The workstations are standardized and may be continuously updated and monitored, this way ensuring that the right software and the right versions are always used. This is of particular importance for the software used to manage the security of the system.

## 4 Secure Collaborative Analysis Environment (NetSCW)

The purpose of the secure collaborative problem solving environment NetSCW is to provide a common data analysis environment managing issues of interoperability, availability and reusability of data, as well as analysis processes and results. In this environment (fig. 1), subject matter experts, data analysts, database and ICT security administrators, *etc.*, can meet to share their resources and expertise, as well as collaborate in real time. The NetSCW environment uses a Service-Oriented Architecture (SOA). The SOA concept envisions an interconnected network of producers and consumers of information and supports the development of a uniform framework for description and utilization of distributed components.

The top layer comprises various data analysis-related tools, *e.g.*, tools for analysing social network data by a single analyst or collaboratively by a group of analysts.

### 4.1 Denodo Virtual DataPort Data Mediation Platform

The Denodo Virtual DataPort (VDP) [8][28], a state-of-the-art data mediator system, provides a solution for accessing, querying and integrating information from any kind of digital source, from structured repositories such as databases, Web Services, and applications, *via* semi-structured sources such as dynamic Web content and delimited files, to unstructured repositories (documents, emails, forums, *etc.*). The system is able to provide a single view of the heterogeneous data stores of participating law enforcement authorities, while allowing them to remain autonomous and unchanged.

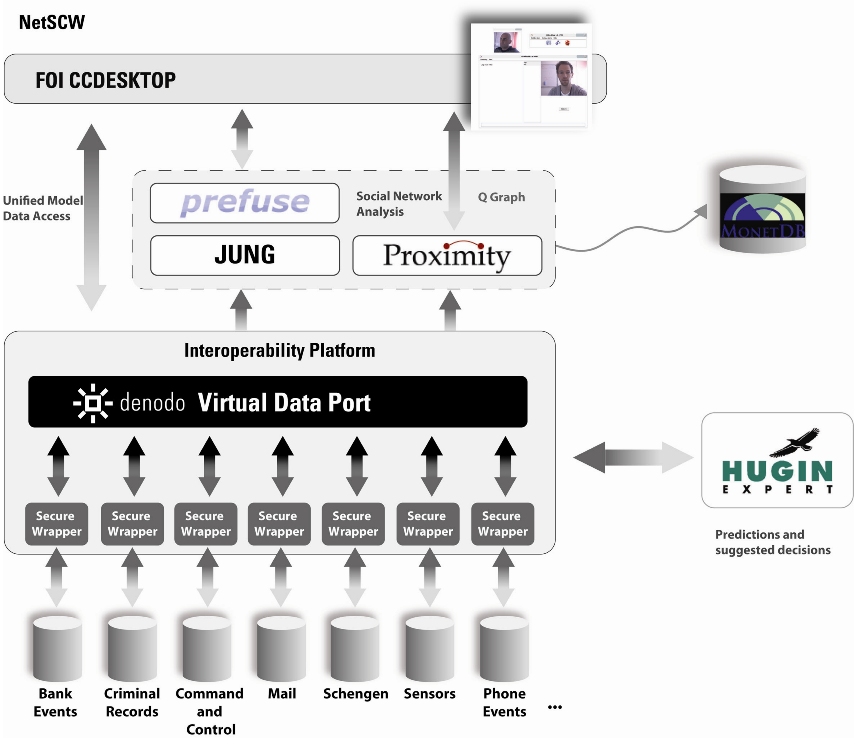

**Fig. 1.** Architecture of the HiTS/ISAC collaborative problem solving environment

The Denodo VDP platform combines data mediation with an advanced web automation technology that allows the exploitation of information in complex hidden web data sources. With this functionality it is possible to integrate data from such complex web sites that are being used nowadays for organized-crime related activities.

Denodo VDP provides a three-level data integration architecture, at the bottom the *data source connectivity* layer that allows integration of data views coming from different data sources (*i.e.,* employing different protocols and data formats) and isolating the complexity for accessing the information to the rest of the platform; the intermediate *transformation and enrichment* layer follows an extended relational model, able to handle both tabular and hierarchical information, and allows the combination and correlation of information by means of data views built with relational operations, such as joins, unions or selections; finally information is delivered to the consumer application through *standard interfaces* such as JDBC/ODBC, SOA/Web Services and Java APIs.

### 4.2 The NetSCW Collaborative Core (NetSCW/CC)

Computer Supported Collaborative Work (CSCW) [23] is an interdisciplinary research and application domain which has evolved since the mid-1980's, with contributions from social anthropology, psychology, and computer sciences. The research focus of CSCW is Groupware, i.e., applications designed to help people involved in a common task to achieve their goals.

### 4.2.1 NetSCW/CCDesktop

In the HiTS/ISAC project, CCDesktop, a Java-based application, has been developed by FOI as the CSCW component of NetSCW. The CCDesktop design aspires to implement much of the desired CSCW functionality and bring it into an analytical problem solving environment. CCDesktop supplies basic functionality through a common communication interface which adds collaborative and group awareness features to existing analysis tools. In addition, CCDesktop provides a secure multimedia communication infrastructure which provides users with video, voice and text messaging facilities. The current version of CCDesktop offers the following tools: participant panel, chat board with video and voice functionality (via RTP, the Real-time Transport Protocol [31]), *simultaneous shared access* to tools for Social Network Analysis [4], as well as to middleware [5] adapting Denodo VDP output to the input requirements of the PROXIMITY graphical query language-based SNA processing tool.

A close integration of JUNG, prefuse, PROXIMITY, and the required data connection to Denodo VDP was developed by two M Sc thesis projects at FOI [4][5]. Functions for adding, merging, grouping by attribute, and removing nodes and edges did not exist in the version of JUNG that was used for the implementation, and were added. Key design requirements of these projects were:

**Data collected from several different databases.** A common schema is needed to reduce the analysts' mental effort.

**Queries as filtering method.** Working with large-scale social networks will require various filtering techniques to select appropriate subsets and reduce the volume of data.

**Objects first mapped to relational data, then into graphs.** Social networks consist of objects that are represented as nodes and edges, not as standard relational database tabular data.

**Sets of subgraphs are combined based on given predicates.** By comparing with the original graph the frequently large number of subgraphs generated by PROXIMITY/QGraph can often be greatly reduced. Using the CCDesktop system, the user may decide on a conceptual level which of these subgraphs should be merged.

**Graphs easily exported.** Graphs need to be readable by other programs, so they are stored either in JUNG internal format or in GraphML external format, or both.

**Combining *prefuse* with JUNG.** This has involved resolving several issues related to the two systems' different graph storage structures, user interaction conventions, and display functionality.

### 4.2.2 PROXIMITY

Social Network Analysis is a required capability of the HiTS/ISAC project. SNA can become computationally intense and the integrated database of HiTS/ISAC may potentially become quite large. Therefore, there is a need to be able to filter data and to find interesting subgraphs, *e.g.* when one wants to find all networks connecting two criminals by either phone calls or email. The SNA query system PROXIMITY [24] provides a network filtering functionality, extended to allow integration with the other components of the HiTS/ISAC analysis system. This functionality is controlled *via* QGraph, a visual language that returns graph fragments with highly variable structure.

PROXIMITY helps human analysts discover new knowledge by analyzing complex data sets containing network-structured information, using specially developed algorithms that help manage, explore, sample, and visualize data.

PROXIMITY is a Java-based open-source software system. It uses the Monet DB, an open-source "vertical" database [25] optimized for analytical queries.

### 4.2.3 Prefuse

*prefuse* is a Java-based open-source software toolkit [26] for building interactive information visualization applications.

*prefuse* supports a rich set of features for data modelling, visualization, and interaction. It provides optimized data structures for tables, graphs, and trees, a host of layout and visual encoding techniques, and support for animation, dynamic queries, integrated search, and database connectivity. *prefuse* is a Java-based open-source software system. It has no SNA capabilities of its own but can be integrated, as demonstrated by the HiTS/ISAC project, with the JUNG framework for immediate access to SNA functionality.

### 4.2.4 JUNG

JUNG, the Java Universal Network/Graph Framework, [29] is an open-source software library that provides a common and extendible language for modelling, analysis, and visualization of data that can be represented as a graph or network. The JUNG library provides a variety of graph algorithms, network visualization tools, and support for dynamic graphs. It also provides a mechanism for annotating graphs, entities, and relations with metadata. This facilitates the creation of analytic tools that can examine the relations between entities in complex data sets as well as metadata attached to each entity and relation.

## 4.3 HUGIN

The HUGIN [6][30] software tools for Bayesian belief networks implement advanced algorithms for knowledge discovery and probabilistic reasoning. These tools consist of the HUGIN Decision Engine and the HUGIN Graphical User Interface, well-suited for developing model-based decision support systems based on Bayesian belief networks (BBNs). A BBN is an intuitive graphical knowledge representation supporting belief update in the light of observations. It consists of an acyclic, directed graph representing causal dependence relations between a set of variables representing entities of the problem domain and a set of conditional probability distributions encoding the strength of the dependence relation.

The HUGIN Decision Engine is the inference engine that takes care of the representation of models, the mathematical calculations performed as part of probabilistic inference, etc., while the HUGIN Graphical User Interface provides a graphical user interface to the functionality of the HUGIN Decision Engine.

In HiTS/ISAC a BBN model for identifying suspicious activity has been developed by knowledge engineers and domain experts in corporation. The BBN model is to be used by analysts in their everyday intelligence work as a tool to perform information fusion and analysis.

A Bayesian model for ranking suspicious bank transactions is shown in Figure 2. The model is evaluated for all transactions, resulting in a ranked list of transactions. One bank transaction, weakly suspected *a priori*, has a high rank in this list and a relatively high degree of *a posteriori* suspiciousness.

The databases used here are a border transaction database and a bank transaction database, which are assumed to reside in different countries and belong to different organizations. The BBN is fed with data from a view constructed in Denodo VDP.

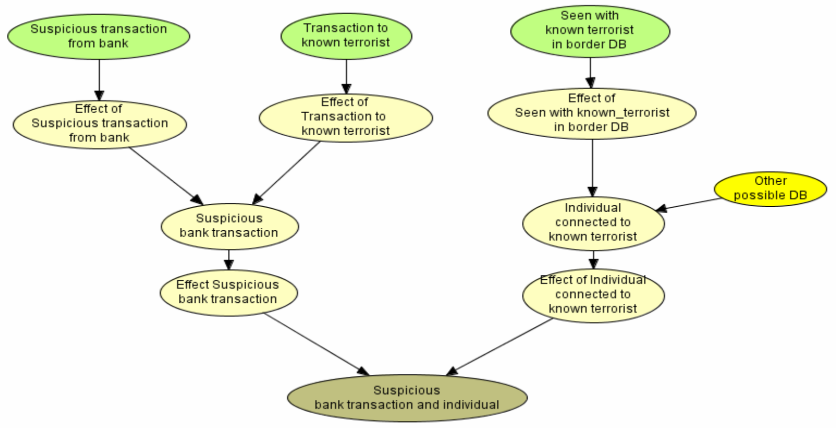
Suspicious transaction from bank
Transaction to known terrorist
Seen with known terrorist in border DB
Effect of Suspicious transaction from bank
Effect of Transaction to known terrorist
Effect of Seen with known_terrorist in border DB
Other possible DB
Suspicious bank transaction
Individual connected to known terrorist
Effect Suspicious bank transaction
Effect of Individual connected to known terrorist
Suspicious bank transaction and individual

**Fig. 2.** Bayesian belief network used in the demonstration. Input nodes and output node are marked with extra ellipses.

For each bank transaction, the view feeds the network with information such as the degree of suspiciousness of the transaction and the names of its sender and its receiver. By comparing these names to those on the list of known terrorists, the input node "Transaction to known terrorist" is set. A view is also constructed that contains all the border transactions of the persons mentioned in any of the bank transactions. If the border database contains a border crossing of a known terrorist that occurs near-simultaneously with a crossing of a person involved in a suspect bank transaction, the input node "Seen with known terrorist in border DB" is set to reflect the time difference between the person and the known terrorist crossing the border.

## 5 Summary and Conclusions

HiTS/ISAC is a pre-study of interoperability and situation awareness for civil security in Europe [32]. The project has demonstrated secure network analysis environments and tools with respect to immediate applicability and user-oriented functionality.

The HiTS/ISAC project dealt with operational, methodological, and developmental issues in a demonstration scenario application. Its focus was on scientifically sound analysis and secure management of distributed and usually uncertain information about events and relationships in organized crime and terrorist networks. The project has demonstrated how legacy databases of several authorities in different countries can be effectively integrated into a distributed problem-solving environment to provide a common user view of the combined relevant information assets of the participating authorities. Analysts working at different sites were able to work collaboratively on the same data without saving, transferring and loading files into their analysis software.

We believe that the experience gained and the lessons learned from this project can be important for determining what analysis capabilities are needed in European police intelligence work. Key technological enablers for successful use of such methodology are distributed, mediated access to large amounts of legacy data and support for real-time collaboration among analysts. Further studies are needed regarding how the operational processes used by criminal intelligence investigators and analysts need to be changed to take full advantage of the possibilities offered by new technology such as that described in this paper. In addition, a set of hard and sometimes highly controversial juridical issues need to be addressed and agreed upon. Such issues are, however, outside the scope of the HiTS/ISAC project and this paper.

## Acknowledgements

The authors wish to thank their HiTS/ISAC consortium partners, in particular Saab AB, TeliaSonera, EADS, and TietoEnator Alise, for sharing their expertise in the public safety area, as well as in the design, integration, and application of the various kinds of software components discussed above.

## References

1. Raab, J., Milward, H.B.: Dark networks as problems. J. Public Administration Research and Theory 13(4), 413–439 (2003)
2. Chang, K.C.-C., He, B., Li, C., Patel, M., Zhang, Z.: Structured Databases on the Web: Observations and Implications. SIGMOD Record 33(3), 61–70 (2004)
3. Popp, R., Poindexter, J.: Countering terrorism through information and privacy protection technologies. IEEE Security & Privacy, 18–27 (November/December 2006)
4. Sköld, M.: Social Network Visualization. M Sc thesis report, KTH School of Computer Science and Communication, Stockholm, Sweden (2008)
5. Asadi, H.C.: Design and Implementation of a Middleware for Data Analysis of Social Networks. M Sc thesis report, KTH School of Computer Science and Communication, Stockholm, Sweden (2007)
6. Kjaerulff, U.B., Madsen, A.L.: Bayesian Networks and Influence Diagrams. A Guide to Construction and Analysis. Springer, New York (2008)
7. Koelle, D., Pfautz, J., Farry, M., Cox, Z., Catto, G., Campolongo, J.: Applications of Bayesian Belief Networks in Social Network Analysis. In: Proc. of the 4th Bayesian Modelling Applications Workshop (2006)
8. Pan, A., Raposo, J., Álvarez, M., Montoto, P., Orjales, V., Hidalgo, J., Ardao, L., Molano y Ángel Viña, A.: The DENODO Data Integration Platform. In: Proc. 28th Int. VLDB Conf., pp. 986–989. Morgan Kaufmann, San Francisco (2002)

9. Carley, K.M., Lee, J.-S., Krackhardt, D.: Destabilizing Networks. Connections 24(3), 79–92 (2002)
10. Carley, K.M.: Estimating Vulnerabilities in Large Covert Networks. In: Proc. of the 2004 International Symposium on Command and Control Research and Technology. Evidence Based Research, Vienna, VA, USA (2004)
11. Wasserman, S., Faust, K.: Social Network Analysis: Methods and Applications. Cambridge University Press, Cambridge (1994)
12. Redner, S.: Citation Statistics from 110 Years of Physical Review. Physics Today 58, 49 (2005)
13. Page, L., Brin, S.: The Anatomy of a Large-Scale Hypertextual Web Search Engine. In: Proceedings of the Seventh International World Wide Web Conference, vol. 30(1-7), pp. 107–117 (1998)
14. Newman, M.E.J.: A Measure of Betweenness Centrality Based on Random Walks. Social Networks 27, 39–54 (2005)
15. Svenson, P., Mårtenson, C., Carling, C.: Complex Networks: Models and Dynamics, Swedish Defence Research Agency Technical Report FOI-R—1766—SE, Stockholm, Sweden (2005)
16. Clauset, A., Newman, M.E.J., Moore, C.: Finding Community Structure in Very Large Networks. Physical Review E70, 066111 (2004)
17. Newman, M.E.J.: Modularity and Community Structure in Networks. Proc. Natl. Acad. Sci. USA 103, 8577–8582 (2006), http://arxiv.org/abs/physics/0602124
18. Klerks, P.: The Network Paradigm Applied to Criminal Organizations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands. Connections 24(3), 53–65 (2001)
19. Gottschalk, P.: Stages of Knowledge Management Systems in Police Investigations. Knowledge-Based Systems 19, 381–387 (2006)
20. Proceedings of the International Conferences on Information Fusion 1998-2005. International Society of Information Fusion, Mountain View, CA, USA
21. Bass, T.: Intrusion Detection Systems and Multi-sensor Data Fusion. Comm. ACM 43(4), 99–105 (2000)
22. Fredriksson, J., Svensson, P., Risch, T.: Mediator-Based Evolutionary Design and Development of Image Meta-Analysis Environments. J. Intell. Information Systems 17(2/3), 301–322 (2001)
23. Ackerman, M.S.: The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. Human-Computer Interaction 15, 179–203 (2000)
24. Jensen, D.: PROXIMITY 4.2 Tutorial. Knowledge Discovery Laboratory, Department of Computer Science, University of Massachusetts at Amherst (2006)
25. Manegold, S., Boncz, P.A., Kersten, M.L.: Optimizing Database Architecture for the New Bottleneck: Memory Access. VLDB Journal 9(9), 231–246 (2000)
26. Heer, J., Card, S.K., Landay, J.A.: Prefuse: a Toolkit for Interactive Information Visualization. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Portland, Oregon, USA (2005)
27. International Society of Information Fusion, http://www.isif.org (accessed 2008-03-27)
28. http://www.denodo.com (accessed 2008-03-27)
29. http://jung.sourceforge.net/ (accessed 2008-03-27)
30. http://www.hugin.com (accessed 2008-03-27)
31. http://tools.ietf.org/html/rfc3550 (accessed 2008-03-27)
32. http://www.hits-isac.eu/ (accessed 2008-03-2)