KNOWLEDGE MANAGEMENT PROCESSES, TOOLS AND TECHNIQUES FOR COUNTERTERRORISM

Uffe Kock Wiil, Nasrullah Memon and Jolanta Gniadek
Counterterrorism Research Lab, The Maersk Mc-Kinney Moller Institute, University of Southern Denmark
Campusvej 55, 5230 Odense M, Denmark

Keywords: Knowledge management processes, Tools, and techniques, Counterterrorism domain, CrimeFighter toolbox.

Abstract: Knowledge about the structure and organization of terrorist networks is important for both terrorism investigation and the development of effective strategies to prevent terrorist attacks. Theory from the knowledge management field plays an important role in dealing with terrorist information. Knowledge management processes, tools, and techniques can help intelligence analysts in various ways when trying to make sense of the vast amount of data being collected. This paper presents the latest research on the CrimeFighter toolbox for counterterrorism. CrimeFighter provides advanced mathematical models and software tools to assist intelligence analysts in harvesting, filtering, storing, managing, analyzing, structuring, mining, interpreting, and visualizing terrorist information.

1 INTRODUCTION

Knowledge about the structure and organization of terrorist networks is important for both terrorism investigation and the development of effective strategies to prevent terrorist attacks. However, except for network visualization, terrorist network analysis remains primarily a manual process. Existing tools do not provide advanced structural analysis techniques that allow for the extraction of network knowledge from terrorist information.

Theory from the knowledge management field plays an important role in dealing with terrorist information (Chen, Reid, Sinai, Silke, and Ganor, 2008). Knowledge management processes, tools, and techniques can help intelligence analysts in various ways when trying to make sense of the vast amount of data being collected. Several manual knowledge management processes can either be semi-automated or supported by software tools.

This paper presents the latest research on the CrimeFighter toolbox for counterterrorism. CrimeFighter provides advanced mathematical models and software tools to assist intelligence analysts in harvesting, filtering, storing, managing, analyzing, structuring, mining, interpreting, and visualizing terrorist information.

CrimeFighter is based on previous work from several research projects performed in the areas of knowledge management, hypertext, investigative data mining, social network analysis, graph theory, visualization, and mathematical methods in counterterrorism. Work on *iMiner* was targeted at constructing a framework for automated terrorist network analysis, visualization, and destabilization (Memon, Wiil, Reda, Atzenbeck, and Harkiolakis, 2009). Work on ASAP (Advanced Support for Agile Planning) aimed at constructing a tool to assist software developers perform structural analysis of software planning data (Petersen and Wiil, 2008). Finally, several projects have been performed to harvest terrorist information from the Web (Henriksen and Sørensen, 2009; Knudsen, 2009; Dasho and Puszczewicz, 2009). The important results from the above work are now being incorporated into the CrimeFighter toolbox.

The paper is organized as follows. Section 2 describes the knowledge management processes, tools, and techniques used by CrimeFigther to support the counterterrorism domain. Section 3 describes the current status of the work on CrimeFighter, while Section 4 outlines open issues and future work. Finally, Section 5 concludes the paper.

Wiil U., Memon N. and Gniadek J. (2009).
KNOWLEDGE MANAGEMENT PROCESSES, TOOLS AND TECHNIQUES FOR COUNTERTERRORISM.
In *Proceedings of the International Conference on Knowledge Management and Information Sharing*, pages 29-36
DOI: 10.5220/0002291900290036

2 CRIMEFIGTHER PROCESSES, TOOLS AND TECHNIQUES

This section discusses how knowledge management processes, tools, and techniques can play an important role for counterterrorism exemplified by the presentation of the CrimeFighter toolbox.

2.1 Processes

Several knowledge management processes are involved in the attempt to provide a toolbox that can support intelligence analysts in their work with terrorist information as shown in Figure 1.

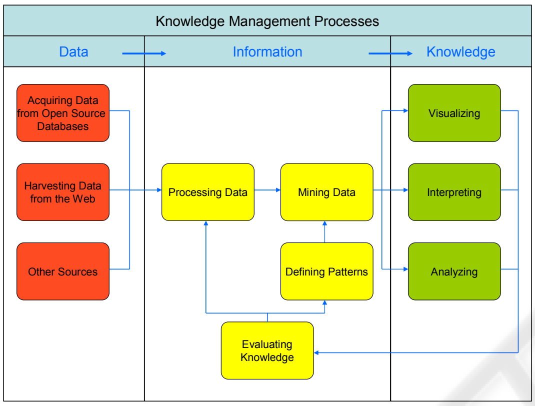


Figure 1: Knowledge management processes for counterterrorism.

Overall, the red processes involve acquiring data from various sources, the yellow processes involve processing data into relevant information, and the green processes involve further analysis and interpretation of the information into useful knowledge that the intelligence analysts can use to support their decision making.

Data Acquisition. Real intelligence data is hard to get due to its sensitive nature. In fact, very few researchers have been granted access to such data. Several options are available in the data acquisition processes:

- Data can be acquired from open source databases that contain authenticated information about terrorists and their activities. TrackingTheThreat.com is an example of a database that contains authenticated open source information about the Al Qaeda terrorist network. (www.trackingthethreat.com).
- Data can be harvested from the Web (including the dark Web – which is data not indexed by major search engines like Google, MSN, Yahoo, etc.). The Web contains many sources that potentially contain terrorist related information (i.e., regular Web pages, blogs, forums, search engines, RSS feeds, chat rooms, etc.).
- Data can be obtained from other sources such as databases maintained by intelligence agencies.

Our tools and techniques have so far only been tested with open source data (the first two items above).

Information Processing. The *Processing Data* step focuses on pre-processing of data. Data is cleaned from unnecessary elements and checked considering quality and completeness. The *Mining Data* step is concerned with processing of data using defined patterns (e.g., activities of people living or staying in the same city). Data mining algorithms are used in order to discover such hidden patterns and obtain relevant knowledge. The *Evaluating Knowledge* step is used to check whether the acquired knowledge is relevant. Errors are recognized and eliminated to improve the overall information processing. Possibly, new patterns are defined and old patterns are enhanced in the *Defining Patterns* step and the pre-processing of data in the *Processing Data* step is fine-tuned based on the feedback from the *Evaluating Knowledge* step.

Knowledge Management. The *Interpreting* knowledge step focuses on performing social network analysis in order to find new patterns and to gain deeper knowledge about the structure of terrorist networks. The *Analyzing* knowledge step focuses on supporting the work with emergent and evolving structure of terrorist networks to uncover new relationships between people, places, events, etc. The *Visualizing* knowledge step deals with the complex task of visualizing the structure of terrorist networks.

2.2 Tools

To support the knowledge management processes described in Section 2.1, CrimeFighter provides a number of tools. The toolbox philosophy is that the humans (intelligence analysts) are in charge of the knowledge management processes and the tools are there to assist the analysts. Thus, the purpose of the tools is to support as many of the knowledge management processes as possible to assist the intelligence analysts in performing their work more efficiently. In this context, efficient means that the analysts arrive at better analysis results much faster.

In general, the tools fall into two overall categories:

- Semi-automatic tools that need to be configured by the intelligence analysts to perform the dedicated task. After configuration, the tool will automatically perform the dedicated task.
- Manual tools that support the intelligence analysts in performing specific tasks by providing dedicated features that enhance the work efficiency when performing manual intelligence analysis work.

The tools of the CrimeFighter toolbox are shown is Figure 2.

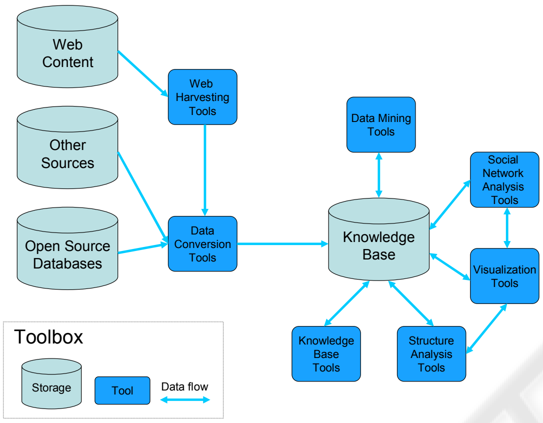


Figure 2: Tools in the CrimeFighter toolbox.

The heart of the toolkit is a knowledge base that contains data related to terrorism, which has been gathered and processed by dedicated tools. The content of the knowledge base is used by the various tools for further analysis and visualization.

The toolbox contains the following semi-automatic tools:

- Web harvesting tools make use of data acquisition agents (spiders) to harvest data from the Web. The spiders are controlled by the data conversion tools.
- Data conversion tools are responsible for both collecting (through spiders) and transforming data.
- Data mining tools provide selected data mining algorithms to discover new knowledge in data based on defined patterns.
- Social network analysis tools perform analysis to uncover new patterns and to gain deeper knowledge about the structure of terrorist networks.
- Visualization tools use graph layout algorithms to visualize discovered knowledge regarding terrorist networks. It can also be used as a graphics engine to support some of the tasks performed by the other tools in the toolbox.

The toolbox also contains the following manual tools:

- Knowledge base tools help maintain the knowledge base by allowing intelligence analysts to explore and revise the knowledge base content as well as to work with meta data.
- Structure analysis tools focuses on supporting the manual work with emergent and evolving structure of terrorist networks to uncover new relationships between people, places, events, etc.

Figure 3 shows how the different tools are related to the three overall knowledge management processes described in Section 2.1.

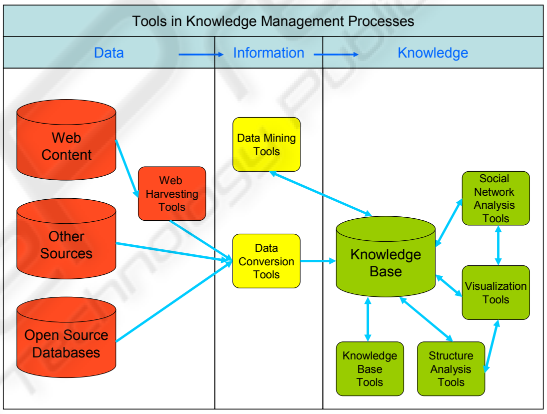


Figure 3: Tools supporting the knowledge management processes.

Some processes cannot be supported by tools and still have to be performed manually. The Evaluating knowledge step is an example of this. Intelligence analysts need to examine the quality of the knowledge and possibly alter the configuration of certain tools (i.e., data conversion, data mining, etc.) to obtain more relevant knowledge for their decision making.

2.3 Techniques

A number of advanced software techniques are used to develop the features of the tools (data mining, social network analysis, criminal geographic profiling, syndromic surveillance, hypertext, visualization, etc.). We will briefly describe these techniques to provide a better understanding of how they are deployed in our work.

Data Mining is a technique involving pattern-based queries, searches, or other analyses of one or more electronic databases, where a department or agency may conduct the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals (Mena, 2003). Among the more prominent methods and tools used in data mining are (Devlin and Lorden, 2007):

- Link analysis: looking for association and other forms of connecting among say, criminals or terrorists.
- Software agents: small, self-contained pieces of computer code that can monitor, retrieve, analyze, and act on information.
- Machine learning: algorithms that can extract profiles of criminals and graphical maps of crime.
- Neural network: special kind of computer programs that can predict the probability of crimes and terrorist attacks.

Social Network Analysis. The events of 9/11 instantly altered the perceptions of the words "terrorist" and "network" (Alam, 2003), and the United States and other countries rapidly started to gear up to fight a new kind of enemy. In conventional warfare, conducted in specific locations, it is important to understand the terrain in which the battles will be fought. In the war against terror, there is no specific location. As 9/11 showed only too well, the battleground can be anywhere. The terrorists' power base is not geographic; rather, they operate in networks, with members distributed across the globe (Carpenter, and Stajkovic, 2006). To fight such an enemy, we need to understand the new "terrain": networks – how they are constructed and how they operate. Using techniques of graph theory and network analysis to analyze social networks, such as terrorist networks, a specialized sub-discipline known as social network analysis rapidly developed in the years leading up to 9/11 and has been a hotter topic since. The applicability of social network analysis to fight crime and terrorism had been known to specialists for many years, but it was only after 9/11 that the general public realized the critical importance of "connecting dots" in investigations and surveillance of terrorists (Devlin and Lorden, 2007).

Criminal Geographic Profiling is a technique originally designed to help police forces to prioritize large lists of suspects typically generated in cases involving serial crime (Raine, Rossmo, and Comber, 2009), for instance, murder and rape (Rossmo and Velarde, 2008). The technique uses the location of related crime sites to make inferences about the most likely area in which the offender might live (or visit regularly), and has been extremely successful in this field (Bennell and Corey 2007; Canter and Hammond 2007). The need for such a technique arises because investigations of serial crimes frequently generate too many, rather than too few, suspects.

Syndromic Surveillance is an innovative electronic surveillance system (automated extraction and analysis of routinely collected data) which use data based on disease symptoms, rather than disease diagnosis (Maciejewski, Hafen, Rudolph, Tebbetts, Cleveland, Grannis, and Ebert, 2009). It involves collecting and analyzing statistical data on health trends (such as symptoms reported by people seeking care in emergency rooms or other health care settings) or even sales of flu medicines. Because bioterrorist agents such as anthrax, plague, and smallpox initially present "flu-like" symptoms, a sudden increase of individuals with fever, headache, or muscle pain could be evidence of a bioterrorist attack (Yan, Chen, and Zeng, 2007). By focusing on symptoms rather than confirmed diagnoses, syndromic surveillance aims to detect bioterror events earlier than would be possible with traditional disease surveillance systems.

Hypertext. Organizing and making sense of information is an important task for intelligence analysts and has been the main focus of hypertext research from its very beginning. Hypertext systems aim at augmenting human intellect – that is "increasing the capability of a man to approach a complex problem situation, to gain comprehension to suit his particular needs, and to derive solutions to problems" (Engelbart, 1962). The most widely used structure abstractions in hypertext are nodes and links. Nodes are informational units that can be connected through links. Users can traverse links and thereby navigate through a hypertext (graph). Nodes and links, however, have been criticised for a lack of support for emergent and evolving structures. Spatial hypertext was designed for and is well suited for dealing with emergent and evolving structures (Shipman, Hsieh, Maloor, and Moore, 2001). Thus, hypertext theory (in particular spatial hypertext theory) plays an important role for the structure analysis tools.

Visualization. Information synthesis and analysis can be facilitated by a visual interface designed to support analytical processing and reasoning. Such an interactive visualization approach is also known as visual analytics (Thomas and Cook, 2006). Visually analyzing social networks has been receiving growing attention and several visualization tools have been developed for this purpose. *Vizster* (Heer and Boyd, 2005) provides an environment to explore and analyze online social network, supporting automatically identification and visualization of connections and community structures. *SocialAction* (Adam and Shneiderman, 2006) allows users to explore different social network analysis measures to gain insights into the network properties, to filter nodes (representing entities), and to find outliers. Users can interactively aggregate nodes to reduce complexity, find cohesive subgroups, and focus on communities of interest. However, the measures used in these systems are topological-oriented. Xu and Chen (2005) proposed a framework for automatic network analysis and visualization. Their *CrimeNet Explorer* identifies relationships between persons based on frequency of co-occurrence in crime incident summaries. Hierarchy clustering algorithm is then applied to partition the network based on relational strength. A visual analytic system *Jigsaw* (Stasko, Gorg, Liu, and Singhal, 2007) represents documents and their entities visually in multiple views to illustrate connections between entities across the different documents. It takes an incremental approach to suggest relevant reports to examine next by inspecting the co-occurred entities.

3 CURRENT STATUS

This section describes the current status of our research by briefly presenting our existing tools for counterterrorism. Additional detail can be found in the provided references.

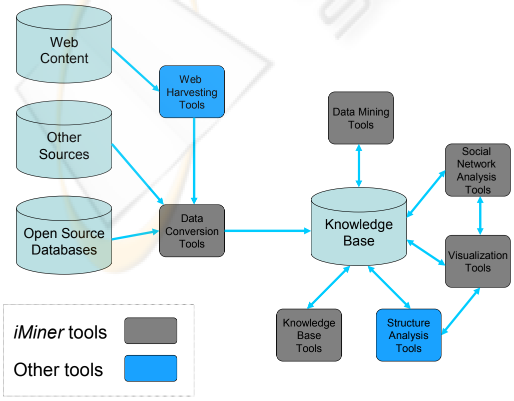


Figure 4: Previous research on counterterrorism.

Currently, many of the identified knowledge management processes for counterterrorism are supported by our tools. Figure 4 shows the current status of our work.

The *iMiner* prototype includes tools for data conversion, data mining, social network analysis, visualization, and for the knowledge base. *iMiner* incorporates several advanced and novel models and techniques useful for counterterrorism like subgroup detection, network efficiency estimation, and destabilization strategies for terrorist networks including detection of hidden hierarchies (Memon, Wiil, Reda, Atzenbeck, and Harkiolakis, 2009).

In relation to *iMiner*, several collections of authenticated datasets of terrorist events that have occurred or were planned have been harvested from open source databases (i.e., TrackingTheTreat.com). Figure 5 shows the dataset on Al Qaeda.

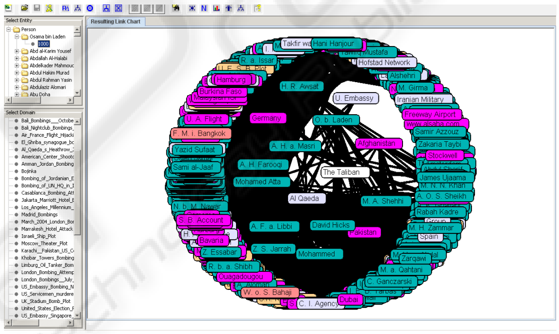
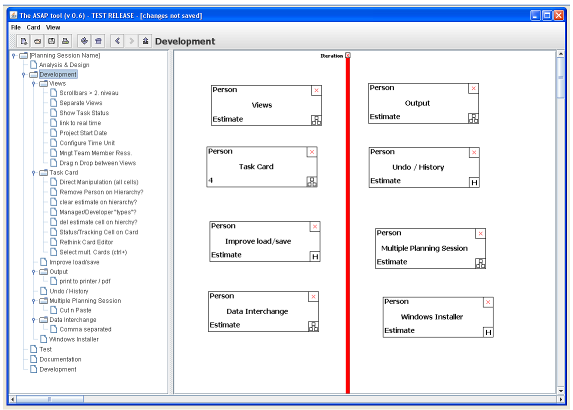


Figure 5: *iMiner* screenshot.

Work has also been conducted on the ASAP tool (Figure 6) to assist software developers to perform structural analysis of software planning data (Petersen and Wiil, 2008).

Many of the spatial hypertext concepts and techniques that supports working with emergent and evolving structures (Shipman, Hsieh, Maloor, and


The ASAP tool (v 0.6) - TEST RELEASE - [changes not saved]

File Card View

Development

- [Planning Session Name]
  - Analysis & Design
  - Development
    - Views
      - Scrollbars > 2. niveau
      - Separate Views
      - Show Task Status
      - link to real time
      - Project Start Date
      - Configure Time Unit
      - Mngt Team Member Ress.
      - Drag n Drop between Views
    - Task Card
      - Direct Manipulation (all cells)
      - Remove Person on Hierarchy?
      - clear estimate on hierarchy?
      - Manager/Developer "types"?
      - del estimate cell on hierchy?
      - Status/Tracking Cell on Card
      - Rethink Card Editor
      - Select mult. Cards (ctrl+)
    - Improve load/save
    - Output
      - print to printer / pdf
    - Undo / History
    - Multiple Planning Session
      - Cut n Paste
    - Data Interchange
      - Comma separated
    - Windows Installer
  - Test
  - Documentation
  - Development

Iteration

Person
Views
Estimate

Person
Task Card
4

Person
Improve load/save
Estimate

Person
Data Interchange
Estimate

Person
Output
Estimate

Person
Undo / History
Estimate

Person
Multiple Planning Session
Estimate

Person
Windows Installer
Estimate

Figure 6: ASAP screenshot.

Moore, 2001) used in ASAP are domain independent and can be re-used in a tool that supports intelligence analysts working with terrorist information.

Finally, several prototypes have been constructed to harvest terrorist information from the Web. Henriksen and Sørensen (2009) have developed a focused web crawler for regular web pages. Knudsen (2009) has developed a tool to harvest information from RSS feeds. Dasho and Puszczewicz (2009) have developed a tool to harvest information from blogs.

4 OPEN ISSUES AND FUTURE WORK

As described in Section 3, we provide support for many of the processes based on novel models and advanced software tools. However, we have identified some open issues in relation to our work.

Structure Analysis. As mentioned, we have experiences from developing a structural analysis tool for the software planning domain. While some of the concepts from spatial hypertext can be re-used for the counterterrorism domain, it is still wide open how this should be done. Atzenbeck, Hicks, and Memon (2009) provide an analysis of the counterterrorism domain and lists requirements in relation to developing a structure analysis tool:

- Supporting the emergent and fragile nature of the created structure and fostering its communication among analysts.
- Integrating with the information sources used by the analyst, permitting them to be represented and structured in a common information space.
- Supporting awareness of, and notification based on, linked information across information source boundaries.
- Permitting multiple directions of thought through versioning support.

Thus, supporting emergent and evolving structure as a means for knowledge representation, communication, integration, versioning, awareness, and notification is central to this tool.

Web Harvesting. The three independent prototypes mentioned above form a good starting point for developing web harvesting tools that can support the data acquisition process in relation to the Web. The challenge is to combine the individual prototypes into an overall configurable, semi-automatic web harvesting tool. Related work regarding design and implementation of web crawlers (Shkapenyuk and Suel, 2002), information gathering in a dynamic world (Hornung, Simon, and Lausen, 2006), and studies of cyber communities in blogs (Chau and Xu, 2008) provides important pointers for this work.

Knowledge Base. The knowledge base used by *iMiner* stores terrorist information in the form of triples:

<subject, object, relationship>

where "subject" and "object" are entities of interest and "relationship" is a link between exactly two entities (Memon, Wiil, Reda, Atzenbeck, and Harkiolakis, 2009). This domain model with nodes (entities) and links (binary relations) supports development of advanced software tools to assist intelligence analysts. Figure 7 shows how this type of domain model can be used to model a complex terrorist networks – example from (Krebs, 2002).

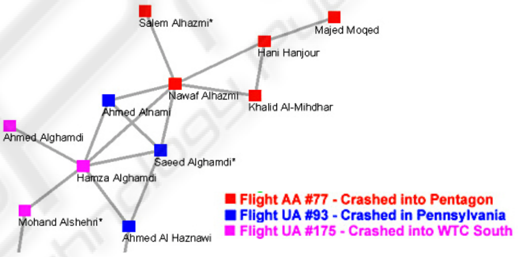


Figure 7: Part of 9/11 terrorist network (Krebs, 2002).

Nodes are entities with attributes allowing relevant information to be stored about the entities. Social network analysis techniques can be used to identify key nodes in the network. This type of information can be used for network destabilization purposes. Taking out key nodes will decrease the ability of the network to function normally.

However, the above domain model also poses limitations. Links only exist as a text string describing the nature of the relation between two nodes (e.g., person A "met with" person B). Links are not first class entities with the same properties as nodes. This is in contrast to the fact that the links between the nodes provides at least as much relevant information about terrorist networks as the nodes themselves (Gloor and Zhao, 2006).

A domain model with links as first class entities (like nodes) will allow additional features to be built into the social network analysis and visualization tools:

- **Using Links Weights.** Currently, all links have the weight "1". Having links as first class entities allows individual weights to be added to links. Weights can be based on information such as the reliability of the information and the level of the relation. Thus, links can be treated differently based on weights allowing more accurate information to be deducted from the terrorist network.

- **Finding Missing Links.** Investigative data mining techniques (Memon, 2007) could be used to suggest (predict) missing links in the terrorist network revealing relations that were previously unknown to the intelligence analysts.
- **Identifying Key Links.** Just like social network analysis techniques can be used to identify key nodes, they can also be used to identify key links in the terrorist network. A key link could for instance be "the flow of finances" between two persons. Taking out key links can also be used to destabilize terrorist networks.

These are just a few examples of how a more powerful domain model inspired by the basic hypertext node link model (Engelbart, 1962) can provide additional features for intelligence analysts. Future research is likely to reveal many additional features made possible by the new domain model.

The above open issues are currently being addressed in various projects to further strengthen our toolbox approach to counterterrorism.

5 RELATED WORK

The CrimeFighter approach towards a toolbox for counterterrorism is inter-disciplinary involving many different research topics as described in the previous sections. To our knowledge, no other approach provides a similar comprehensive coverage of tools and techniques to support the involved knowledge management processes.

The individual tools are based on theory from various research fields. Theory and related work from these fields are discussed throughout the paper – especially in Section 2.3 on techniques.

6 CONCLUSIONS

This paper described the latest research on the CrimeFighter toolbox for counterterrorism. The work reported in this paper has primarily made the following contributions:

- We have identified and described knowledge management processes, tools, and techniques that are central to the counterterrorism domain.
- We have developed and implemented advanced mathematical models and software tools that help automate and support knowledge processes for counterterrorism to assist intelligence analysts in their work.
- We have presented past, ongoing, and future work on CrimeFighter – a novel toolbox for counterterrorism that provides advanced support for the counterterrorism domain.

So far our tools and techniques have only been tested with open source data from authenticated terrorist databases and the Web. We have not had access to real intelligence data. We are currently in the process of making a Memorandum of Understanding with an intelligence agency from Asia. We expect that this will allow us to test our tools and techniques in the future with real intelligence data and with intelligence analysts as end users. This will take the research to the next level. Testing the tools and techniques with real data and real end users is the ultimate test that will validate the value of our approach.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the support from the Faculty of Engineering and the Maersk Mc-Kinney Moller Institute (both University of Southern Denmark) to establish the Counterterrorism Research Lab.

REFERENCES

Adam, P., and Shneiderman, B. 2006. Balancing Systematic and Flexible Exploration of Social Networks. IEEE Transactions on Visualization and Computer Graphics, 12(5), 693–700.

Alam, M. B. 2003: Perceptions of Japanese Students on Terrorism. Strategic Analysis, Vol. 27, No. 2, 279-291

Atzenbeck, C., Hicks, D. L., and Memon, N. 2009. Supporting Reasoning and Communication for Intelligence Officers. Accepted for the International Journal of Networking and Virtual Organizations (IJNVO). Inderscience Publishers.

Bennell, C., and Corey, S. 2007. Geographic profiling of terrorist attacks. In Criminal profiling: international theory, research and practice, pp. 189–203. Humana Press.

Canter, D. V., and Hammond, L. 2007. Prioritizing burglars: Comparing the Effectiveness of Geographic profiling methods. Police Pract. Res. 8, 371–384.

Carpenter, M. A., and Stajkovic, A. D. 2006. Social network theory and methods as tools for helping business confront global terrorism: Capturing the case and contingencies presented by dark social networks. Corporate strategies under international terrorism and adversity. Edward Elgar Publishing.

Chau, M., and Xu, J. 2008. Using Web Mining and Social Network Analysis to Study the Emergence of Cyber Communities in Blogs. In Terrorism Informatics. Knowledge Management and Data Mining for Homeland Security, pp. 473-494. Springer.

Chen, H., Reid, E., Sinai, J., Silke, A., and Ganor, B. (eds.). 2008. Terrorism Informatics. Knowledge Management and Data Mining for Homeland Security. Springer.

Dasho, E., and Puszczewicz, R. 2009. Tools and Techniques for Counterterrorism: Web Mining and Social Network Analysis in Blogs. Project report. University of Southern Denmark.

Devlin, K., and Lorden, G. 2007. The Numbers Behind NUMB3RS: Solving Crime with Mathematics. Plume.

Engelbart, D. C. 1962. Augmenting human intellect: A conceptual framework, Summary Report AFOSR-3233, Standford Research Institute.

Gloor, P. A., and Zhao, Y. 2006. Analyzing Actors and Their Discussion Topics by Semantic Social Network Analysis. Information Visualization. IV 2006, pp. 130-135

Henriksen, K., and Sørensen, M. 2009. Design and Implementation of a Focused Web Crawler for use in Web Harvesting for Counterterrorism Planning Purposes. Project report. University of Southern Denmark.

Heer, J., and Boyd, D. 2005. Vizster: Visualizing Online Social Networks. In Proc. of the IEEE Symposium on Information Visualization (InfoVis 2005).

Hornung, T., Simon, K., and Lausen, G. 2006. Information Gathering in a Dynamic World. Principles and Practice of Semantic Web Reasoning. LNCS 4187, pp. 237–241. Springer.

Knudsen, M. 2009. Dynamic Web Harvesting Using RSS Feeds. Project report. University of Southern Denmark.

Krebs, V. 2002. Mapping networks of terrorist cells. Connections, 24, 45–52.

Maciejewski R., Hafen, R., Rudolph, S., Tebbetts, G., Cleveland, W.S., Grannis, S. J., Ebert, D. S., 2009. Generating Synthetic Syndromic-Surveillance Data for Evaluating Visual - Analytics Techniques, IEEE Computer Graphics and Applications, 29, 3, 18-28.

Memon N. 2007. Investigative Data Mining: Mathematical Models of Analyzing, Visualizing and Destabilizing Terrorist Networks. Ph.D. Dissertation, Aalborg University, Denmark.

Memon, N., Wiil, U. K., Alhajj, R., Atzenbeck, C., and Harkiolakis, N. 2009. Harvesting Covert Networks: The Case Study of the iMiner Database. Accepted for the International Journal of Networking and Virtual Organizations (IJNVO). Inderscience Publishers.

Mena, J. 2003. Investigative Data Mining for Security and Criminal Detection. Butterworth-Heinemann.

Petersen, R. R., and Wiil, U. K. 2008. ASAP: A Planning Tool for Agile Software Development. In Proc. of the ACM Hypertext Conference, pp. 27-32. ACM Press.

Raine, N. E., Rossmo, D. K., and Comber, S. C. 2009. Geographic profiling applied to testing models of bumble-bee foraging. In J. R. Soc. Interface 6, 307-319.

Rossmo, D. K., and Velarde, L. 2008. Geographic profiling analysis: principles, methods, and applications. In Crime mapping case studies: practice and research, pp. 35–43. Wiley.

Shipman, F. M., Hsieh, H, Maloor, P., and Moore, J. M. 2001. The Visual Knowledge Builder: A Second Generation Spatial Hypertext, In Proc. of the ACM Hypertext Conference, pp. 113-122. ACM Press.

Shkapenyuk,V., and Suel, T. 2002. Design and Implementation of a High-Performance Distributed Web Crawler. In Proceedings of .18th International Conference on Data Engineering, (San Jose, CA, February), pp. 357-368. IEEE Computer Society.

Stasko, J., Gorg, C., Liu, Z., and Singhal, K. 2007. Jigsaw: Supporting Investigative Analysis through Interactive Visualization. In Proc. of the IEEE Symposium on Visual Analytics Science and Technology, pp. 131–138.

Thomas, J., and Cook, K. 2006. A Visual Analytics Agenda. IEEE Computer Graphics and Applications 26(1), 10–13.

Xu, J., and Chen, H. 2005. CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery. ACM Transactions on Information Systems 23(2), 201–226

Yan, P., Chen, H., and Zeng, D. 2007. Syndromic Surveillance Systems: Public Health and Bio-defence. Annual Review of Information Science and Technology (ARIST), 41, 425-495