Nm2/Report

Aus VroniPlag Wiki

This report is based on the findings of an ongoing plagiarism analysis (date: 12-01-2014). It is therefore no conclusive report and it is recommended to visit the page http://de.vroniplag.wikia.com/wiki/Nm2 for newer findings and further information.

A critical discussion of the publication by Nasrullah Memon, David L. Hicks, and Henrik Legind Larsen: *How Investigative Data Mining Can Help Intelligence Agencies to Discover Dependence of Nodes in Terrorist Networks*

in: R. Alhajj et al. (Eds.): ADMA 2007, LNAI 4632, pp. 430–441, 2007. Springer Berlin Heidelberg →ISBN 978-3-540-73870-1 →Download (http://link.springer.com/chapter/10.1007%2F978-3-540-73871-8_40) →Erratum (http://link.springer.com/chapter/10.1007/978-3-540-73871-8_61)

Overview

The following chart illustrates the amount and the distribution of the findings of text parallels. The colours show the type of plagiarism diagnosed:

- grau="Komplettplagiat": the source of the text parallel is not given, the copy is verbatim.
- rot="Verschleierung": the source of the text parallel is not given, the copied text will be somewhat modified.
- gelb="Bauernopfer": the source of the text parallel is mentioned, but the extent and/or closeness of the copying is not made clear by the reference.

Prominent findings of plagiarism

- Fragment 430 28, Fragment 431 03: Three paragraphs of the introduction are taken from Katz et al. (2004), a publication that is not mentioned anywhere in the paper. The text is slightly adapted to give it a "terrorist feel", e.g. "Joe talks to Jane" in the source becomes "Atta talks with Khalid" in the paper.
- Fragment 432 31: 10 lines of text in Section 2 are taken verbatim without any attribution.
- Fragment 433 24: The authors cite themselves for a passage taken verbatim from Koschade (2005), who in fact quote another source for it.
- Fragment 434 01: A table is taken together with an eight-line explanation (Fragment 433 32) from a source not mentioned in the paper. The copied table is the one mentioned in an "Erratum" on SpringerLink.
- Fragment 434 04: Almost two paragraphs are taken from Koelle et al. (2006), a publication that is not mentioned anywhere in the paper. This includes all references to the literature (six in total).
- Fragment 440 16: More than half of the conclusions is taken verbatim from Stephenson & Zelen (1989), a publication not mentioned anywhere in the paper.

Statistics

- Currently there are 20 reviewed fragments documented, that are considered to be plagiarism. For 18 of them there is no reference given to the source used („Verschleierungen“ and „Komplettplagiate“). For 2 fragments the source is given, but the extent of the used text is not made clear („Bauernopfer“).
- The publication has 11 pages that have been analyzed. On a total of 10 of these pages plagiarism has been documented. This represents a percentage of **90.9%**. The 11 analyzed pages break down with respect to the amount of plagiarism encountered as follows:

Percentage plagiarism	Number of pages
No plagiarism documented	1
0%-50% Plagiarism	6
50%-75% Plagiarism	2
75%-100% Plagiarism	2

  From these statistics an extrapolation of the amount of text of the publication under investigation that has been documented as plagiarism can be estimated (conservatively) as **about 46%** of the main part of the publication.

- In all, text was taken from 12 sources.

Duplication

Most of the text of the paper has been recycled by the authors elsewhere:

- The entire Section 4 "Centrality Measures" as well as about half of Section 5 "Dependence Centrality" (i.e. p. 435:30-42, p. 436:all, p. 437:all, p. 438:1-30, p.439:5-10) are identical to the corresponding portions of Memon et al. (2007e) (retracted).
- A part of Section 4 "Centrality Measures" as well as about half of Section 5 "Dependence Centrality" (i.e. p. 435:30-42, p. 436:1-15, p. 437:26-35, p. 438:1-30) have also been published in Memon et al. (2008a)
- The entire Section 3 "Graph Theory" (p. 435:1-29) has also been published in Harkiolakis et al. (2008b)
- The entire Section 2 "Investigative Data Mining (IDM)" (p. 432:12-40, p. 433:all, p. 434:all) has also been published (in a slightly edited form) in Memon et al. (2010d) and in Memon et al. (2011a)

- Large parts of the paper (p. 430:17-36; p. 431: all; p. 432:12-40; p. 433:1-2,13-22,31-38; p. 434:19-45; p. 436:9-39; p. 437:all; p. 438:1-30) have also been published in Memon et al. (2008e) (retracted)
- Substantial parts of the paper (p. 430:17-36; p. 431:1-28; p. 436:9-36; p. 437:all; p. 438:1-30) have also been published in Memon & Hicks (2008f) (retracted)
- A large part of Section 2 "Investigative Data Mining (IDM)" (p. 432:12-40; p.433:1-30; 434:33-42) has also been published in Memon et al. (2009a) (retracted)
- Some parts of the paper (p. 430:27-36; p. 431:1-9; p. 437:26-35) have also been published in Memon et al. (2011c)
- Fragment 433 24 can be found in 9 other publications:
  - N. Memon's PhD thesis (2007)
  - Memon & Larsen (2006a)
  - Memon & Larsen (2007a)
  - Memon et al. (2007c) (retracted)
  - Memon et al. (2008d)
  - Memon et al. (2008e) (retracted)
  - Memon et al. (2009a) (retracted)
  - Memon et al. (2010d)
  - Memon et al. (2011a)

References

Memon, Larsen (2006a) (http://link.springer.com/chapter/10.1007%2F11811305_113) : Structural Analysis and Mathematical Methods for Destabilizing Terrorist Networks Using Investigative Data Mining in X. Li, O.R. Zaiane, and Z. Li (Eds.): ADMA 2006, LNAI 4093, pp. 1037 – 1048, 2006. Springer Berlin Heidelberg.

Memon, Larsen (2007a) (http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-IST-063///MP-IST-063-14.pdf) : Investigative Data Mining Toolkit: A Software Prototype for Visualizing, Analyzing and Destabilizing Terrorist Networks. Post-Workshop proc. NATO workshop on Information Visualization

Memon, Hicks, Larsen (2007c) (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4272050&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4272050) : Harvesting Terrorists Information from Web 11th International Conference Information Visualization (IV'07), 0-7695-2900-3/07 2007 IEEE (retracted)

Memon, Hicks, Hussain, Larsen (2007e) (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4455057&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F4454732%2F4454733%2F04455057.pdf) : Practical Algorithms and Mathematical models for destabilizing terrorist networks in Military Communications Conference, 1-7. MILCOM 2007. IEEE (retracted)

Memon. Larsen, Hicks, Harkiolakis (2008a) (http://link.springer.com/chapter/10.1007%2F978-3-540-69304-8_50?LI=true) : Detecting Hidden Hierarchy in Terrorist Networks: Some Case Studies, in C.C. Yang et al. (Eds.): ISI 2008 Workshops, LNCS 5075, pp. 477–489, 2008. Springer Berlin Heidelberg

Harkiolakis, Memon, Hicks, Atzenbeck (2008b) (http://vbn.aau.dk/en/publications/revealing-topological-properties-of-terrorist-networks(14f2d370-1ad4-11dd-8ae8-000ea68e967b).html) : Revealing Topological Properties of Terrorist Networks In: Hamid R. Arabnia and Youngsong Mun, editors, Proceedings of the 2008 International Conference on Artificial Intelligence (ICAI'08), pages 238–244, 2008.

Memon, Hicks, Harkiolakis (2008d) (http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=837145) : A Data Mining Approach to Intelligence Operations In: Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008, edited by Belur V.

Dasarathy, Proc. of SPIE Vol. 6973, 697309, (2008), 0277-786X/08, doi: 10.1117/12.780835

Memon, Harkiolakis, Hicks (2008e) (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4493536&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F4488216%2F4493499%2F04493536.pdf%3Farnumber%3D4493536) : Detecting High-Value Individuals in Covert Networks: 7/7 London Bombing Case Study aiccsa, pp.206-215, 2008 IEEE/ACS International Conference on Computer Systems and Applications, 2008 (retracted)

Memon, Hicks (2008f) (http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=4529487) : Detecting Key Players in 11-M Terrorist Network: A Case Study ares, pp.1254-1259, 2008 Third International Conference on Availability, Reliability and Security, 2008, 0-7695-3102-4/08 IEEE Computer Society DOI 10.1109/ARES.2008.173 (retracted)

Memon, Qureshi, Wiil, Hicks (2009a) (http://ieeexplore.ieee.org/xpl/login.jsp?reload=true&tp=&arnumber=5066528&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5066528) : Novel Algorithms for Subgroup Detection in Terrorist Networks 2009 International Conference on Availability, Reliability and Security, 978-0-7695-3564-7/09 IEEE, Computer Society, DOI 10.1109/ARES.2009.168 (retracted)

Memon et al. (2008d) (http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=837145) as well as in Memon, Wiil,Qureshi (2010d) (http://www.inderscience.com/info/inarticle.php?artid=31284) : Practical algorithms for subgroup detection in covert networks Int. J. Business Intelligence and Data Mining, Vol. 5, No. 2, 2010, 134-155, Inderscience

Memon, Wiil, Alhajj, Atzenbeck, Harkiolakis (2011a) (http://www.inderscience.com/info/inarticle.php?artid=37161) : Harvesting covert networks: a case study of the iMiner database in Int. J. Networking and Virtual Organisations, Vol. 8, Nos. 1/2, 2011, Inderscience

Memon, Wiil, Qureshi, Karampelas (2011c) (http://link.springer.com/chapter/10.1007%2F978-3-7091-0388-3_20) : Exploring the Evolution of Terrorist Networks U.K. Wiil (ed.), Counterterrorism and Open Source Intelligence, Lecture Notes in Social Networks 2, 413-427, DOI 10.1007/978-3-7091-0388-3 20, Springer-Verlag/Wien 2011

Appendix 1: Fragments

Remark on the colouring

The colouring is automatically generated and shows text parallels. Its purpose is to facilitate the orientation of the reader, it does not, however, automatically diagnose plagiarism of any kind. In order to form a judgement about a certain text parallel one should consult the text itself.

Remark on the line numbering

When identifying a fragment with line numbers everything that contains text (except for the page header and/or footer) is counted, including headings. Usually charts, tables etc. including their captions are not counted, however.

20 gesichtete, geschützte Fragmente

[1.] Nm2/Fragment 430 17

Verschleierung

Untersuchte Arbeit: **Seite: 430, Zeilen: 17-27**	**Quelle: Xu and Chen 2003** **Seite(n): 232, Zeilen: 21ff**
1 Introduction	1 Introduction
Terrorists seldom operate in a vacuum but interact with one another to carry out terrorist activities. To perform terrorist activities requires collaboration among terrorists. Relationships between individual terrorists are essential for the smooth operation of a terrorist organization, which can be viewed as a network consisting of nodes (for example terrorists, terrorist camps, supporting countries, *etc*.) and links (for example, communicates with, or trained at, *etc*.). In terrorist networks, there may exist some group or cell, within which members have close relationships. One group may also interact with other groups. For example, some key nodes (key players) may act as leaders to control activities of a group, while others may serve as gatekeepers to ensure smooth flow of information or illicit goods.	Criminals seldom operate in a vacuum but interact with one another to carry out various illegal activities. In particular, organized crimes such as terrorism, drug trafficking, gang-related offenses, frauds, and armed robberies require collaboration among offenders. Relationships between individual offenders form the basis for organized crimes [18] and are essential for smooth operation of a criminal enterprise, which can be viewed as a network consisting of nodes (individual offenders) and links (relationships). In criminal networks, there may exist groups or teams, within which members have close relationships. One group also may interact with other groups to obtain or transfer illicit goods. Moreover, individuals play different roles in their groups. For example, some key members may act as leaders to control activities of a group. Some others may serve as gatekeepers to ensure smooth flow of information or illicit goods.

Farbig

Anmerkungen

The source is not mentioned, although the beginning of the introduction of the paper is only a version of the introduction of the source, adapted from criminal networks to terrorist networks.

[2.] Nm2/Fragment 430 28

Verschleierung

Untersuchte Arbeit: Seite: 430, Zeilen: 28-36	**Quelle: Katz et al 2004 Seite(n): 308, 309, Zeilen: 308: 23ff; 309: 1ff** Farbig
In social network literature, researchers have examined a broad range of types of ties [1]. These include communication ties (such as who talks to whom or who gives information or advice to whom), formal ties (such as who reports to whom), affective ties (such as who likes whom, or who trust whom), material or work flow ties (such as who gives bomb making material or other resources to whom), proximity ties (who is spatially or electronically close to whom). Networks are typically multiplex, that is, actors share more than one type of tie. For example, two terrorists might have a formal tie (one is a foot-soldier or a newly recruited person in the terrorist cell and reports to the other, who is the cell leader) and an affective tie (they are friends); and [may also have a proximity tie (they are residing in the same apartment and their flats are two doors away on the same floor).]	Network researchers have examined a broad range of types of ties. These include communication ties (such as who talks to whom, or who gives information or advice to whom), formal ties (such as who reports to whom), affective ties (such as who likes whom, or who trusts whom), material or work flow ties (such as who gives money or other resources to whom), proximity ties (who is spatially or electronically close to whom), and cognitive ties (such as who knows who knows whom). Networks are typically mutiplex [sic], that is, actors share more than one type of tie. For example, two academic colleagues might have a formal tie (one is an assistant professor and reports to the other, who is the department chairperson) [page 309] and an affective tie (they are friends) and a proximity tie (their offices are two doors away).

1. Monge, P.R., Contractor, N.: Theories of Communication Networks. Oxford University Press, New York (2003)

Anmerkungen

The copied text continues on the next page: Nm2/Fragment 431 03

The source is not mentioned anywhere in this paper, although the text has been taken from the source and adapted to terrorist networks. One of the authors of reference 1 is, however, co-author in Katz, et al. But this exact wording is not to be found in Monge & Contractor, only in Katz, et al.

[3.] Nm2/Fragment 431 03

Verschleierung

Untersuchte Arbeit: Seite: 431, Zeilen: 3-17	**Quelle: Katz et al 2004 Seite(n): 309, Zeilen: 3ff** Farbig
Network researchers have distinguished between strong ties (such as family and friends) and weak ties such as acquaintances [2, 3]. This distinction will involve a multitude of facets, including affect, mutual obligations, reciprocity, and intensity. Strong ties are particularly valuable when an individual seeks socio-emotional support and often entail a high level of trust. Weak ties are more valuable when individuals are seeking diverse or unique information from someone outside their regular frequent contacts.	Network researchers have distinguished between strong ties (such as family and friends) and weak ties (such as acquaintances) (Granovetter, 1973, 1982). This distinction can involve a multitude of facets, including affect, mutual obligations, reciprocity, and intensity. Strong ties are particularly valuable when an individual seeks socioemotional support and often entail a high level of trust. Weak ties are more valuable when individuals are seeking diverse or unique information from someone outside their regular frequent contacts. This information could include new job or market opportunities.
Ties may be non directional (for example, Atta attends a meeting with Nawaf Alhazmi) or vary in direction (for instance, Bin Laden gives advice to Atta vs. Atta gets advice from Bin Laden). They may vary in content (Atta talks with Khalid about the trust of his friends in using them as human bombs and his recent meeting with Bin Laden), frequency (daily, weekly, monthly, *etc*.), and medium (face-to-face conversation, written memos, email, fax, instant messages, *etc*.). Finally ties may vary in sign, ranging from positive (Iraqis like Zarqawi) to negative (Jordanians dislike Zarqawi).	Ties may be nondirectional (Joe attends a meeting with Jane) or vary in direction (Joe gives advice to Jane vs. Joe gets advice from Jane). They may also vary in content (Joe talks to Jack about the weather and to Jane about sports), frequency (daily, weekly, monthly, etc.), and medium (face-to-face conversation, written memos, e-mail, instant messaging, etc.). Finally, ties may vary in sign, ranging from positive (Joe likes Jane) to negative (Joe dislikes Jane).
2. Granovetter, M.: The Strength of Weak Ties. American Journal of Sociology 81, 1287– 1303 (1973)	Granovetter,M. (1973). The strength of weak ties. *American Journal of Sociology*, 81, 1287-1303.
3. Granovetter, M.: The Strength of Weak Ties: A Network Theory Revisited. In: Collins, R. (ed.) Sociological Theory, pp. 105–130 (1982)	Granovetter,M. (1982). The strength of weak ties: A network theory revisited. In R. Collins (Ed.), *Sociological theory 1983* (pp. 105-130). San Francisco: Jossey-Bass.

Anmerkungen

The source is mentioned nowhere in the paper, although the text has been taken from it after adapting it to terrorist networks: e.g. "Joe talks to Jane" becomes "Atta talks with Khalid"

The two references to Granovetter are also taken from the source.

The copied text begins on the previous page: Nm2/Fragment 430 28

[4.] Nm2/Fragment 431 20

Verschleierung

Farbig

Untersuchte Arbeit:
Seite: 431, Zeilen: 20-27

Structural network patterns in terms of subgroups and individual roles are important in understanding the organization and operation of terrorist networks. Such knowledge can help law enforcement and intelligence agencies to disrupt terrorist networks and develop effective control strategies to combat terrorism. For example, capture of central members in a network may effectively upset the operational network and put a terrorist organization out of action [4, 5, 6]. Subgroups and interaction patterns between groups are helpful in finding a network's overall structure, which often reveals points of vulnerability [7, 8].

4. Baker, W.E., Faulkner, R.R.: The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. American Sociological Review 58(6), 837–860 (1993)

5. McAndrew, D.: The Structural Analysis of Criminal Networks. In: Canter, D., Alison, L. (eds.) The Social Psychology of Crime: Groups, Teams, and Networks, Aldershot, Dartmouth. Offender Profiling Series, III, pp. 53–94 (1999)

6. Sparrow, M.: The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects. Social Networks 13, 251–274 (1991)

7. Evan, W.M.: An Organization-set Model of Inter-organizational Relations. In: Tuite, M., Chisholm, R., Radnor, M. (eds.) Inter-organizational Decision-making, Aldine, Chicago, pp. 181–200 (1972)

8. Ronfeldt, D., Arquilla, J.: What Next for Networks and Netwars? In: Arquilla, J., Ronfeldt, D. (eds.) Networks and Netwars: The Future of Terror, Crime, and Militancy, Rand Press (2001)

Quelle: Xu and Chen 2003
Seite(n): 232, 233, Zeilen: 232: 32ff; 233: 1ff

Structural network patterns in terms of subgroups, between-group interactions, and individual roles thus are important to understanding the organization, structure, and operation of criminal enterprises. Such knowledge can help law enforcement and intelligence agencies disrupt criminal networks and develop effective control strategies to combat organized crimes such as narcotic trafficking and terrorism. For exam-

[page 233]

ple, removal of central members in a network may effectively upset the operational network and put a criminal enterprise out of action [3, 17, 21]. Subgroups and interaction patterns between groups are helpful for finding a network's overall structure, which often reveals points of vulnerability [9, 19].

3. Baker, W. E., Faulkner R. R.: The social organization of conspiracy: illegal networks in the heavy electrical equipment industry. American Sociological Review, Vol. 58, No. 12. (1993) 837–860.

9. Evan, W. M.: An organization-set model of interorganizational relations. In: M. Tuite, R. Chisholm, M. Radnor (eds.): Interorganizational Decision-making. Aldine, Chicago (1972) 181–200.

17. McAndrew, D.: The structural analysis of criminal networks. In: Canter, D., Alison, L. (eds.): The Social Psychology of Crime: Groups, Teams, and Networks, Offender Profiling Series, III, Aldershot, Dartmouth (1999) 53–94.

19. Ronfeldt, D., Arquilla, J.: What next for networks and netwars? In: Arquilla, J., Ronfeldt, D. (eds.): Networks and Netwars: The Future of Terror, Crime, and Militancy. Rand Press, (2001).

21. Sparrow, M. K.: The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, Vol. 13. (1991) 251–274.

Anmerkungen

The source is not mentioned anywhere in the paper.

The text has been adapted from criminal networks to terrorist networks and also five references to the literature have been copied.

[5.] Nm2/Fragment 431 27

BauernOpfer

Untersuchte Arbeit:
Seite: 431, Zeilen: 27-44

Networks come in basically three types [9]:

(1) The chain network, as in a smuggling chain, where people, goods, or information move along a line of separated contacts and where end-to-end communication must travel through the intermediate nodes. (2) The star, hub, or wheel network, as in a terrorist syndicate or a cartel structure, where a set of actors is tied to a central node or actor and all must go through that node to communicate and coordinate with each other. (3) The all-channel network, as in a collaborative network of small militant groups, in which every group or node is connected to every other node.

Each type of network may be suited to different conditions and purposes, and there may be any number of hybrids. The all-channel network has historically been the most difficult to organize and sustain, partly because of the dense communications required. Yet the all-channel network is the type that is gaining strength from the information revolution. The design is flat. Ideally, there is no single, central leadership or command or headquarters—-no precise heart or head that can be targeted. Decision-making and operations are decentralized, allowing for local initiative and autonomy [10].

---

9. Arquilla, J., Ronfeldt, D.: Swarming and a Future of Conflict. RAND National Defense Institute (2001)

10. Hoffman, B.: Terrorism evolves Toward Netwar. RAND Review 22(2) (1999)

Quelle: Arquilla Ronfeldt 2001
Seite(n): 7, 8, 9, Zeilen: 7: 24ff; 8: 1ff; 9: 4ff

Farbig

[page 7]

networks come in basically three types or topologies (see Figure 1.1):

- The *chain* or line network, as in a smuggling chain where people, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes.
- The *hub*, star, or wheel network, as in a franchise or a cartel where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.

[page 8]

[FIGURE]

- The *all-channel* or full-matrix network, as in a collaborative network of militant peace groups where everybody is connected to everybody else.

[...]

Each type may be suited to different conditions and purposes, [...] There may also be hybrids of the three types,[...]

[page 9]

Of the three network types, the all-channel has been the most difficult to organize and sustain, partly because it may require dense communications. But it is the type that gives the network form its new, high potential for collaborative undertakings and that is gaining new strength from the information revolution. [...] The organizational design is flat. Ideally, there is no single, central leadership, command, or headquarters—-no precise heart or head that can be targeted. [...] Decisionmaking and operations are decentralized, allowing for local initiative and autonomy.

Anmerkungen

The source is given at the beginning, but it is not clear to the reader that the source is being followed verbatim at times and also in one paragraph further down.

[6.] Nm2/Fragment 432 24

BauernOpfer

Untersuchte Arbeit: **Seite: 432, Zeilen: 24-30**	**Quelle: DeRosa 2004** **Seite(n): v, Zeilen: 32ff**
Although these techniques are powerful, it is a mistake to view investigative data mining techniques as a complete solution to security problems. The strength of IDM is to assist analysts and investigators. IDM can automate some functions that analysts would otherwise have to perform manually. It can help to prioritize attention and focus an inquiry, and can even do some early analysis and sorting of masses of data. Nevertheless, in the complex world of counterterrorism, it is not likely to be useful as the only source for a conclusion or decision.	Although these techniques are powerful, it is a mistake to view data mining and automated data analysis as complete solutions to security problems. Their strength is as tools to assist analysts and investigators. They can automate some functions that analysts would otherwise have to perform manually, they can help prioritize attention and focus an inquiry, and they can even do some early analysis and sorting of masses of data. But in the complex world of counterterrorism, they are not likely to be useful as the only source for a conclusion or decision.

Farbig

Anmerkungen

The source in mentioned one paragraph above, which is also very much inspired from it. However, there is no indication, implicit or explicit, that this paragraph is also taken from De Rosa (2004).

[7.] Nm2/Fragment 432 31

Verschleierung

Untersuchte Arbeit: Seite: 432, Zeilen: 31-40	**Quelle: Thuraisingham_2003 Seite(n): 213, 214, Zeilen: 213: 41-44; 214: 1-8** Farbig
In the counterterrorism domain, much of the data could be classified. If we are to truly get the benefits of the techniques we need to test with actual data. But not all researchers have the clearances to work on classified data. The challenge is to find unclassified data that is, representative of the classified data. It is not straightforward to do this, as one has to make sure that all classified information, even through implications, is removed. Another alternative is to find as good data as possible in an unclassified setting for researchers to work on. However, the researchers have to work not only with counterterrorism experts but also with data mining specialists who have the clearances to work in classified environments. That is, the research carried out in an unclassified setting has to be transferred to a classified setting later to test the [applicability of data mining algorithms. Only then do we get the true benefit of investigative data mining.]	[page 213] However for the domain that we are considering much of the data could be classified. If we are to truly get the benefits of the techniques we need to test with actual data. But not all of the researchers have the clearances to work on classified data. The challenge is to find unclassified data that is a representative sample of the classified [page 214] data. It is not straightforward to do this, as one has to make sure that all classified information, even through implications, is removed. Another alternative is to find as good data as possible in an unclassified setting for the researchers to work on. However, the researchers have to work not only with counter-terrorism experts but also with data mining specialists who have the clearances to work in classified environments. That is, the research carried out in an unclassified setting has to be transferred to a classified setting later to test the applicability of the data mining algorithms. Only then can we get the true benefits of data mining.

Anmerkungen

The source is mentioned nowhere in the paper.

[8.] Nm2/Fragment 433 14

Verschleierung

Farbig

Untersuchte Arbeit: **Seite: 433, Zeilen: 14-19**	**Quelle: Koschade 2005** **Seite(n): 2, 3, Zeilen: 2: 6ff; 3: 31ff**
IDM offers the ability to map a covert cell, and to measure the specific structural and interactional criteria of such a cell. This framework aims to connect the dots between individuals and to map and measure complex, covert, human groups and organizations [13]. The method focuses on uncovering the patterning of people's interaction, and correctly interpreting these networks assists in predicting behaviour and decision-making within the network [13].	Social network analysis offers the ability to firstly map a covert cell, and to secondly measure the specific structural and interactional criteria of such a cell. [page 3] This framework aims to connect the dots between individuals and "map and measure complex, sometimes covert, human groups and organisations".[8] The method focuses on uncovering the patterning of people's interaction,[9] and correctly interpreting these networks assists "in predicting behaviour and decision-making within the network".[10]
13. Memon, N., Larsen, H.L.: Structural Analysis and Mathematical Methods for Destabilizing Terrorist Networks. In: Li, X., Zaïane, O.R., Li, Z. (eds.) ADMA 2006. LNCS (LNAI), vol. 4093, pp. 1037–1048. Springer, Heidelberg (2006)	[8] Krebs, V. (2002) "Mapping Networks of Terrorist Cells", *Connections*, Vol. 24, 3, pp. 43-52. [9] Freeman, L. (nd) 'The Study of Social Networks', *The International Network for Social Network Analysis*, Retrieved May 17, 2004, from http://www.sfu.ca/~insna/INSNA/na_inf.html. [10] Renfro, R. & Deckro, R. (2001). "A Social Network Analysis of the Iranian Government", paper presented at *69th MORS Symposium*, 12-14 June, 2001, p. 4.

Anmerkungen

The authors refer to one of their own earlier papers (see SpringerLink (http://link.springer.com/chapter/10.1007%2F11811305_113)). There the passage can indeed be found, but Koschade (2005) was published even before the Memon/Larson paper. Thus, the Memon/Larson paper cannot be the original source.

The authors also removed three citations.

[9.] Nm2/Fragment 433 24

Verschleierung

Untersuchte Arbeit: Seite: 433, Zeilen: 24-31	**Quelle: Koschade 2005 Seite(n): 2, 3, Zeilen: 2: 8-14; 3: 38ff** Farbig
IDM also endows the analyst with the ability to measure the level of covertness and efficiency of the cell as a whole, and the level of activity, ability to access others, and the level of control over a network each individual possesses. The measurement of these criteria allows specific counter-terrorism applications to be drawn, and assists in the assessment of the most effective methods of disrupting and neutralising a terrorist cell [13]. In short, IDM provides a useful way of structuring knowledge and framing further research. Ideally it can also enhance an analyst's predictive capability [13].	The method also endows the analyst the ability to measure the level of covertness and efficiency of the cell as a whole, and also the level of activity, ability to access others, and the level of control over a network each individual possesses. The measurement of these criteria allows specific counter-terrorism applications to be drawn, and assists in the assessment of the most effective methods of disrupting and neutralising a terrorist cell. [page 3] In short, social network analysis "provides a useful way of structuring knowledge and framing further research. Ideally it can also enhance an analyst's predictive capability".[12]
13. Memon, N., Larsen, H.L.: Structural Analysis and Mathematical Methods for Destabilizing Terrorist Networks. In: Li, X., Zaïane, O.R., Li, Z. (eds.) ADMA 2006. LNCS (LNAI), vol. 4093, pp. 1037–1048. Springer, Heidelberg (2006)	[12] Aftergood, S. (2004) 'Secrecy News: Social Network Analysis and Intelligence' [online], *Federation of American Scientists Project on Government Secrecy*, Vol. 2004, 15. Retrieved May 17, 2004, from http://www.fas.org/sgp/news /secrecy/2004/02 /020904.html.

Anmerkungen

The authors refer to one of their own earlier papers (see SpringerLink (http://link.springer.com/chapter /10.1007%2F11811305_113)). There the passage can indeed be found, but Koschade (2005) was published even before the Memon/Larson paper. Thus, it cannot be the original source.

The authors also removed a citation and attribute the quote to themselves.

[10.] Nm2/Fragment 433 32

Verschleierung

Untersuchte Arbeit: Seite: 433, Zeilen: 32-39	**Quelle: Popp and Poindexter 2006 Seite(n): 23, Zeilen: left col. 5ff**
On the other hand, traditional data mining commonly refers to using techniques rooted in statistics, rule-based logic, or artificial intelligence to comb through large amounts of data to discover previously unknown but statistically significant patterns. However, in the application of IDM in the counterterrorism domain, the problem is much harder, because unlike traditional data mining applications, we must, find an extremely wide variety of activities and hidden relationships among individuals. Table 1 gives a series of reasons for why traditional data mining isn't the same as investigative data mining.	Data mining commonly refers to using techniques rooted in statistics, rule-based logic, or artificial intelligence to comb through large amounts of data to discover previously unknown but statistically significant patterns. However, the general counterterrorism problem is much harder because unlike commercial data mining applications, we must find extremely rare instances of patterns across an extremely wide variety of activities and hidden relationships among individuals. Table 2 gives a series of reasons for why commercial data mining isn't the same as terrorism detection in this context.

Farbig

Anmerkungen

The source is not mentioned anywhere in the paper.

[11.] Nm2/Fragment 434 01

Verschleierung

Untersuchte Arbeit: Seite: 434, Zeilen: 1

Table 1. Traditional data mining vs. investigative data mining

TRADITIONAL DATA MINING	INVESTIGATIVE DATA MINING
Discover comprehensive models of databases to develop statistically valid patterns	Detect connected instances of rare patterns
No starting points	Known starting points or matches with patterns estimated by analysts
Apply models over entire data	Reduce search space; results are starting points for human analysts
Independent instances (records)	Relational instances (networked data)
No correlation between instances	Significance autocorrelation
Minimal consolidation needed	Consolidation is key
Dense attributes	Sparse attributes
Sampling is used	Sampling destroys connections
Homogeneous data	Heterogeneous data
Uniform privacy policy	Non-uniform privacy policy

Quelle: Popp and Poindexter 2006 Seite(n): 23, Zeilen: Table 2

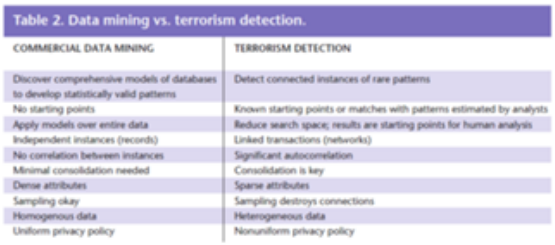

Table 2. Data mining vs. terrorism detection.

COMMERCIAL DATA MINING	TERRORISM DETECTION
Discover comprehensive models of databases to develop statistically valid patterns	Detect connected instances of rare patterns
No starting points	Known starting points or matches with patterns estimated by analysts
Apply models over entire data	Reduce search space; results are starting points for human analysis
Independent instances (records)	Linked transactions (networks)
No correlation between instances	Significant autocorrelation
Minimal consolidation needed	Consolidation is key
Dense attributes	Sparse attributes
Sampling okay	Sampling destroys connections
Homogenous data	Heterogeneous data
Uniform privacy policy	Nonuniform privacy policy

Farbig

Anmerkungen

The tables are almost identical, but the source is not mentioned anywhere in the thesis.

(click on the images to enlarge them)

[12.] Nm2/Fragment 434 04

KomplettPlagiat

Untersuchte Arbeit: Seite: 434, Zeilen: 4-14	**Quelle: Koelle et al 2006 Seite(n): 1, Zeilen: left col.: 19ff** Farbig
SNA primarily focuses on applying analytic techniques to the relationships between individuals and groups, and investigating how those relationships can be used to infer additional information about the individuals and groups [14]. There are a number of mathematical and algorithmic approaches that can be used in SNA to infer such information, including connectedness and centrality [15]. Law enforcement personnel have used social networks to analyze terrorist networks [16, 17] and criminal networks [6]. The capture of Saddam Hussein was facilitated by social network analysis: military officials constructed a network containing Hussein's tribal and family links, allowing them to focus on individuals who had close ties to Hussein [19].	Social network analysis (SNA) primarily focuses on applying analytic techniques to the relationships between individuals and groups, and investigating how those relationships can be used to infer additional information about the individuals and groups (Degenne & Forse, 1999). There are a number of mathematical and algorithmic approaches that can be used in SNA to infer such information, including connectedness and centrality (Wasserman & Faust, 1994). [...] Law enforcement personnel have used social networks to analyze terrorist networks (Krebs, 2006; Stewart, 2001) and criminal networks (Sparrow, 1991). The capture of Saddam Hussein was facilitated by social network analysis: military officials constructed a network containing Hussein's tribal and family links, allowing them to focus on individuals who had close ties to Hussein (Hougham, 2005).
6. Sparrow, M.: The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects. Social Networks 13, 251–274 (1991) 14. Degenne, A., Forse, M.: Introducing Social Networks. Sage Publications, London (1999) 15. Wasserman, S., Faust, K.: Social Network Analysis: Methods and Applications. Cambridge University Press, Cambridge (1994) 16. Krebs, V.E.: Uncloaking Terrorist Networks (2002), Accessed on 23/3/2005 http:// www.firstmonday.org/ issues/issue7_4/krebs 17. Stewart, T.: Six Degrees of Mohamed Atta (2001), Accessed on 24/1/2006 http://money.cnn.com/ magazines/business2 19. Hougham, V.: Sociological Skills Used in the Capture of Saddam Hussein (2005), Accessed on 22/2/2005 http://www.asanet.org/ footnotes/julyaugust05/fn3.html	Degenne, A. & Forse, M. (1999). *Introducing Social Networks*. London: Sage Publications. Hougham, V. (2005). *Sociological Skills Used in the Capture of Saddam Hussein*. *http://www.asanet.org /footnotes/* julyaugust05/fn3.html. Krebs, V. E. (2006). *Uncloaking Terrorist Networks*. *http://www.firstmonday.org/ issues/issue7_4/krebs* Sparrow, M. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks 13, 251-274. Stewart, T. (2001). *Six Degrees of Mohamed Atta*. *http://money.cnn.com/magazines/business2* Wasserman, S. & Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

Anmerkungen

The source is not mentioned, although the text and six references to the literature are taken verbatim from it.

[13.] Nm2/Fragment 435 34

Verschleierung

Untersuchte Arbeit: Seite: 435, Zeilen: 34-40	Quelle: Stephenson and Zelen 1989 Seite(n): 2, 3, Zeilen: 2: 31ff; 3: 1ff	Farbig
A review of key centrality concepts can be found in the papers by Freeman *et al*. [23]. Their work has significantly contributed to the conceptual clarification and theoretical application of centrality. He provides three general measures of centrality termed “degree”, “closeness”, and “betweenness”. His development was partially motivated by the structural properties of the center of a star graph. The most basic idea of degree centrality in a graph is the adjacency count of its constituent nodes.	A review of key centrality concepts can be found in the papers by Freeman (1979a,b). His work has significantly contributed to the conceptual clarification and theoretical application of centrality. Motivated by the work of Nieminen (1974), Sabidussi (1966), and Bavelas (1948) he provides three general measures of centrality termed [page 3] “degree”, “closeness”, and “betweenness”. His development is partially motivated by the structural properties of the center of a star graph. The most basic idea of point centrality in a graph is the adjacency count of its constituent points. “	
23. Freeman, L.C., Freeman, S.C., Michaelson, A.G.: On Human Social Intelligence. Journal of Social and Biological Structures 11, 415–425 (1988)	Freeman, L.C. 1979 a “Centrality in Social Networks: Conceptual Clarification.” Social Networks I: 215-239.	

Anmerkungen

The reference to Freeman *et al*. is to a different paper, a group work that does not deal with centrality concepts. Interestingly, referring to the authors the next sentence speaks of "Their", the one after that of "He", and then "His", which parallels the sentences in Stephenson & Zelen. The word "point" has been replaced by "node". Stephenson & Zelen 1989 are not mentioned anywhere in the paper.

[14.] Nm2/Fragment 436 05

KomplettPlagiat

Untersuchte Arbeit: Seite: 436, Zeilen: 5-11	Quelle: Koschuetzki et al 2005 Seite(n): 20, Zeilen: 8-16	Farbig
The degree centrality $C_d(v)$ of a vertex v is simply defined as the degree $d(v)$ of v if the considered graph is undirected. The degree centrality is, e.g., applicable whenever the graph represents something like a voting result. These networks represent a static situation and we are interested in the vertex that has the most direct votes or that can reach most other vertices directly. The degree centrality is a local measure, because the centrality value of a vertex is only determined by the number of its neighbors.	The most simple centrality is the degree centrality $c_D(v)$ of a vertex v that is simply defined as the degree $d(v)$ of v if the considered graph is undirected. [...] The degree centrality is, e.g., applicable whenever the graph represents something like a voting result. These networks represent a static situation and we are interested in the vertex that has the most direct votes or that can reach most other vertices directly. The degree centrality is a local measure, because the centrality value of a vertex is only determined by the number of its neighbors.	

Anmerkungen

The source is not mentioned anywhere in the paper.

[15.] Nm2/Fragment 436 28

Verschleierung

Untersuchte Arbeit: Seite: 436, Zeilen: 28-39	**Quelle: Koschuetzki et al 2005 Seite(n): 22, 23, Zeilen: 22: 12ff; 23: 1-3** Farbig
We denote the sum of the distances from a vertex $u \in V$ to any other vertex in a graph $G = (V,E)$ as the total distance $\sum_{u \in V} d(u,v)$, where $d(u,v)$ is shortest [sic] distance between the nodes u and v The problem of finding an appropriate location can be solved by computing the set of vertices with minimum total distance.	We denote the sum of the distances from a vertex $u \in V$ to any other vertex in a graph $G = (V,E)$ as the total distance[2] $\sum_{v \in V} d(u,v)$. The problem of finding an appropriate location can be solved by computing the set of vertices with minimum total distance. [...]
In SNA literature, a centrality measure based on this concept is called closeness. The focus lies here, for example, on measuring the closeness of a person to all other people in the network. People with a small total distance are considered as most important as those with high total distance. The most commonly employed definition of closeness is the reciprocal of the total distance:	In social network analysis a centrality index based on this concept is called closeness. The focus lies here, for example, on measuring the closeness of a person to all other people in the network. People with a small total distance are considered as more important as those with a high total distance. [...] The most commonly employed definition of closeness is the reciprocal of the total distance
$$C_C(u) = \frac{1}{\sum_{v \in V} d(u,v)} \qquad (2)$$	[page 23] $$C_C(u) = \frac{1}{\sum_{v \in V} d(u,v)} \qquad (3.2)$$
$C_C(u)$ grows with decreasing total distance of u, therefore it is also known as a structural index.	In our sense this definition is a vertex centrality, since ' $C_C(u)$ grows with decreasing total distance of u and it is clearly a structural index.

[2] In [273], Harary used the term status to describe a status of a person in an organization or a group. In the context of communication networks this sum is also called transmission number.

Anmerkungen

The source is not mentioned anywhere in the paper.

[16.] Nm2/Fragment 437 01

Verschleierung

Untersuchte Arbeit: Seite: 437, Zeilen: 1-5	Quelle: Stephenson and Zelen 1989 Seite(n): 3, Zeilen: 10-16 Farbig
The third measure is *betweenness* which is defined as the frequency at which a node occurs on geodesics that connect pairs of nodes. Thus, any node that falls on the shortest path between other nodes can potentially control the transmission of information or effect exchange by being an intermediary; it is the potential for control that defines the centrality of these nodes [23].	The third measure is called betweenness and is the frequency at which a point occurs on the geodesic that connects pairs of points. Thus, any point that falls on the shortest path between other points can potentially control the transmission of information or effect exchange by being an intermediary. “It is this potential for control that defines the centrality of these points” (Freeman 1979a: 221).
23. Freeman, L.C., Freeman, S.C., Michaelson, A.G.: On Human Social Intelligence. Journal of Social and Biological Structures 11, 415–425 (1988)	Freeman, L.C. 1979 a “Centrality in Social Networks: Conceptual Clarification.” *Social Networks* I: 215-239.

Anmerkungen

The authors replace "point" with "node" and remove the quotation marks of the Freeman quote, although a different Freeman paper is cited that does not actually discuss "betweenness" at all. Stephenson & Zelen (1989) are not mentioned.

[17.] Nm2/Fragment 437 09

Verschleierung

Farbig

Untersuchte Arbeit:
Seite: 437, Zeilen: 9-19

Let $\delta_{uw}(v)$ denotes the fraction of shortest paths between *u* and *w* that contain vertex *v*:

$$\delta_{uw}(v) = \frac{\sigma_{uw}(v)}{\sigma_{uw}} \quad (3)$$

where σ_{uw} denotes the number of all shortest-paths between *u* and *w*. The ratio $\delta_{uw}(v)$ can be interpreted as the probability that vertex *v* is involved into any communication between *u* and *w*. Note, that the measure implicitly assumes that all communication is conducted along shortest paths. Then the betweenness centrality $C_B(v)$ of a vertex *v* is given by:

$$C_B(v) = \sum_{u \neq v \in V} \sum_{w \neq v \in V} \delta_{uw}(v) \quad (4)$$

Any pair of vertices *u* and *w* without any shortest path from *u* to *w* will add zero to the betweenness centrality of every other vertex in the network.

Quelle: Koschuetzki et al 2005
Seite(n): 29-30, Zeilen: 29: 26ff; 30: 1, 13-15

Let $\delta_{st}(v)$ denote the fraction of shortest paths between *s* and *t* that contain vertex *v*:

$$\delta_{st}(v) = \frac{\sigma_{st}(v)}{\sigma_{st}} \quad (3.12)$$

where σ_{st} denotes the number of all shortest-path [sic] between *s* and *t*. Ratios $\delta_{st}(v)$ can be interpreted as the probability that vertex v is involved into any communication between *s* and *t*. Note, that the index implicitly assumes that all communication is conducted along shortest paths. Then the betweenness centrality $c_B(v)$ of a vertex *v* is given by:

[page 30]

$$c_B(v) = \sum_{s \neq v \in V} \sum_{t \neq v \in V} \delta_{st}(v) \quad (3.13)$$

[...]

Any pair of vertices *s* and *t* without any shortest path from *s* to *t* just will add zero to the betweenness centrality of every other vertex in the network.

Anmerkungen

The definitions given here are, of course, standard and don't require a citation. However, the interpreting and explaining text is taken from the source word for word. The source is not mentioned in the paper anywhere.

[18.] Nm2/Fragment 438 12

Verschleierung

Untersuchte Arbeit: Seite: 438, Zeilen: 12-14, 19-20	**Quelle: Freeman 1980 Seite(n): 588, Zeilen: 1ff**
Now we define dependence centrality as the degree to which a node, *u*, must depend upon another, *v*, to relay its messages along geodesics to and from all other reachable nodes in the network. Thus, for a network containing *n* nodes, the dependence centrality of *u* on *v* can be found by using: [...]	Now we can define pair-dependency as the degree to which a point, p_i, *must depend upon another,* p_j, *to relay its messages along geodesics to and from all other reachable points in the network. Thus, for a network containing* n *points, [...]*
We can calculate the dependence centrality of each vertex on every other vertex in the network and arrange the results in a matrix [...]	We can calculate the pair-dependencies of each point on every other point in the network and arrange the results in a matrix,

Farbig

Anmerkungen

The notion of pair-dependency, which has been known for some time, is called "dependence centrality" in this paper (the used formula is a slight adaptation of the original formula). A source is not mentioned, although some text appears to have been taken from this paper.

[19.] Nm2/Fragment 438 23

Verschleierung

Untersuchte Arbeit: Seite: 438, Zeilen: 23-26	**Quelle: Freeman 1980 Seite(n): 588, Zeilen: 10ff**
Each entry in D is an index of the degree to which the node designated by the row of the matrix must depend on the vertex designated by the column to relay messages to and from others. Thus *D* captures the importance of each node as a gatekeeper with respect to each other node — facilating [sic] or perhaps inhibiting its communication.	Each entry in **D** is an index of the degree to which the point designated by the row of the matrix must depend on the point designated by the column to relay messages to and from others. Thus **D** captures the importance of each point as a gatekeeper with respect to each other point — facilitating or perhaps inhibiting its communication.

Farbig

Anmerkungen

Apart from the substitution "node"/"vertex" <--> "point" the text is identical. The source is not mentioned anywhere in the paper.

[20.] Nm2/Fragment 440 16

KomplettPlagiat

Untersuchte Arbeit: Seite: 440, Zeilen: 16-22	**Quelle: Stephenson and Zelen 1989 Seite(n): 3, 27, Zeilen: 3: 28ff; 27: 34ff** Farbig
We have attempted to illustrate the calculation of centralities to these prototypical situations. However we regard our efforts in this direction as only a beginning. We only considered shortest distances in this paper. It is quite possible that information will take a more circuitous route either by random communication or may be intentionally channeled through many intermediaries in order to “hide” or “shield” information in a way not captured by geodesic paths. These considerations raise questions as to how to include all possible paths in a centrality measure.	It is quite possible that information will take a more circuitous route either by random communication or may be intentionally channeled through many intermediaries in order to “hide” or “shield” information in a way not captured by geodesic paths. These considerations raise questions as to how to include all possible paths in a centrality measure. [page 27] We have attempted to illustrate the calculation of centralities to these prototypical situations. However we regard our efforts in this direction as only a beginning.

Anmerkungen

The source is not mentioned anywhere in the paper.

Appendix 2: Sources

[1.] Quelle:Nm2/Arquilla Ronfeldt 2001

Autor	John Arquilla, David Ronfeldt
Titel	Networks and Netwars: The future of crime, terror, and militancy
Ort	Santa Monica
Verlag	RAND
Jahr	2001
ISBN	0-8330-3030-2
URL	Google Books (http://books.google.de/books?id=cL_3CsUvxMMC&printsec=frontcover&hl=de#v=onepage&q&f=false) , also: chapter 3 (http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch3.pdf) and complete (http://www.911investigations.net/IMG/pdf/doc-392.pdf?)
Literaturverz.	yes
Fußnoten	yes

[2.] Quelle:Nm2/Brandes Erlebach 2005

Autor	Ulrik Brandes, Thomas Erlebach
Titel	Chapter 2 Fundamentals
Sammlung	Network Analysis: Methodological Foundations
Herausgeber	Ulrik Brandes, Thomas Erlebach
Ort	Berlin Heidelberg
Verlag	Springer
Jahr	2005
ISBN	978-3-540-24979-5
ISSN	0302-9743
URL	http://www.inf.uni-konstanz.de/algo/publications/be-f-05.pdf
Literaturverz.	no
Fußnoten	no

[3.] Quelle:Nm2/DeRosa 2004

Autor	Mary DeRosa
Titel	Data Mining and Data Analysis for Counterterrorism
Herausgeber	Center for Strategic and International Studies
Ort	New York
Verlag	The CSIS Press
Jahr	2004
ISBN	0-89206-443-9
URL	http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf
Literaturverz.	yes
Fußnoten	yes

[4.] Quelle:Nm2/Freeman 1980

Autor	Linton C. Freeman
Titel	The gatekeeper, Pair-dependency and Structural Centrality
Zeitschrift	Quality and Quantity
Ort	Amsterdam
Verlag	Elsevier
Jahr	1980
Nummer	14
Seiten	585-592
DOI	10.1007/BF00184720
URL	http://moreno.ss.uci.edu/31.pdf
Literaturverz.	no
Fußnoten	no

[5.] Quelle:Nm2/Katz et al 2004

Autor	Nancy Katz, David Lazer, Holly Arrow, Noshir Contractor
Titel	Network Theory and Small Groups
Zeitschrift	Small Group Research
Datum	June 2004
Nummer	35 (3)
Seiten	307-332
DOI	10.1177/1046496404264941
URL	[1] (http://sgr.sagepub.com/content/35/3/307) , [2] (http://www.hks.harvard.edu/davidlazer/files/papers/Lazer_Katz_Small_Group.pdf)
Literaturverz.	no
Fußnoten	no

[6.] Quelle:Nm2/Koelle et al 2006

Autor	David Koelle, Jonathan Pfautz, Michael Farry, Zach Cox, Geoffrey Catto, Joseph Campolongo
Titel	Applications of Bayesian Belief Networks in Social Network Analysis
Sammlung	Proc. of the 4th Bayesian Modeling Applications Workshop during the 22nd Annual Conference on Uncertainty in Artificial Intelligence: UAI '06, July 13th, Cambridge, Massachusetts, 2006
Jahr	2006
Seiten	6
URL	http://www.cs.uu.nl/groups/DSS/UAI-workshop/Koelle.pdf
Literaturverz.	no
Fußnoten	no

[7.] Quelle:Nm2/Koschade 2005

Autor	Stuart A. Koschade
Titel	A Social Network Analysis of Aum Shinrikyo: Understanding Terrorism in Australia
Sammlung	Social Change in the 21st Century Conference, 28 October 2005, Queensland University of Technology
Herausgeber	C. Bailey, Laurie R. Buys
Ort	Brisbane
Datum	28. October 2005
ISBN	1-7410-7108-9
URL	http://eprints.qut.edu.au/3496/
Literaturverz.	no
Fußnoten	no

[8.] Quelle:Nm2/Koschuetzki et al 2005

Autor	D. Koschützki, K.A. Lehmann, L. Peeters, S. Richter, D. Tenfelde- Podehl, O. Zlotowski
Titel	Chapter 3 Centrality Indices
Sammlung	Network Analysis: Methodological Foundations
Herausgeber	Ulrik Brandes, Thomas Erlebach
Ort	Berlin Heidelberg
Verlag	Springer
Jahr	2005
Seiten	16-61
ISBN	978-3-540-24979-5
ISSN	0302-9743
URL	http://books.google.de/books?id=TTNhSm7HYrIC
Literaturverz.	no
Fußnoten	no

[9.] Quelle:Nm2/Popp and Poindexter 2006

Autor	Robert Popp, John Poindexter
Titel	Countering Terrorism through Information and Privacy Protection Technologies
Zeitschrift	IEEE Security and Privacy
Herausgeber	IEEE Computer Society
Datum	November 2006
Nummer	4 (6)
Seiten	18-27
DOI	10.1109/MSP.2006.147
URL	http://dl.acm.org/citation.cfm?id=1191682; http://www.eecs.harvard.edu/cs199r/readings/popp-sp2006.pdf
Literaturverz.	no
Fußnoten	no

[10.] Quelle:Nm2/Stephenson and Zelen 1989

Autor	Karen Stephenson, Marvin Zelen
Titel	Rethinking Centrality: Methods and Examples
Zeitschrift	Social Networks
Ausgabe	11
Jahr	1989
Seiten	1-37
URL	http://www.sciencedirect.com/science/article/pii/0378873389900166
Literaturverz.	no
Fußnoten	no

[11.] Quelle:Nm2/Thuraisingham 2003

Autor	Bhavani Thuraisingham
Titel	Chapter 3: Data Mining for Counter-Terrorism
Jahr	2003
Anmerkung	Year has been taken from PDF file properties: "Created: 20/10/2003 17:08:18"
URL	http://www.utdallas.edu/~jxr061100/paper-for-website/%5b18%5dMining-Terrorism-NGDM04.pdf
Literaturverz.	no
Fußnoten	no

[12.] Quelle:Nm2/Xu and Chen 2003

Autor	Jennifer Xu, Hsinchun Chen
Titel	Untangling Criminal Networks: A Case Study
Sammlung	Intelligence and Security Informatics First NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA, June 2–3, 2003 Proceedings
Herausgeber	Chen, H et al.
Ort	Berlin, Heidelberg
Verlag	Springer
Jahr	2003
Nummer	2665
Seiten	232-248
Reihe	Lecture Notes in Computer Science
DOI	10.1007/3-540-44853-5_18
URL	http://www.springerlink.com/content/4rn8l185w0rvl931/
Literaturverz.	no
Fußnoten	no